CYBER SECURITY IN THE NATIONAL MARKET SYSTEM

Supriya Sarnikar and D. Bruce Johnsen[†]

A secure financial market system is critical to our national economy. Yet, we show that over the past thirty years, financial market regulations have actually increased the vulnerability of U.S. financial trading systems to cyber terrorism by mandating a "national market system" in which otherwise separate trading centers are electronically linked into a single integrated network and the market data generated in each center is subject to mandatory sharing. Our conclusion is that the SEC's policy of communalizing the rights to market data, though very appealing as egalitarian politics, is contrary to the public interest and the protection of investors.

I. INTRODUCTION

A secure financial market system is critical to our national economy. Much of our industrial, technological, agricultural, and even national defense activity relies heavily on investment capital raised within, or intermediated through, the U.S. financial system. What is more, the prices generated by our financial trading systems serve as invaluable signals for efficient investment and resource allocation decisions by countless operating entities. Any breach of security that interrupts or hinders these financial systems could easily paralyze our national economy, at least for a time.

Following the terrorist attacks of September 11, 2001, most of the attention directed to securing our financial system focused on the physical threat

[†] Supriya Sarnikar is Assistant Professor at Westfield State College. Ph.D. Economics, 2002, University of Arizona; J.D. 2005, George Mason University. D. Bruce Johnsen is Professor of Law, George Mason University School of Law. J.D. 1985, Emory University; Ph.D. Economics 1987, University of Washington. For helpful comments, we thank Mark Grady, workshop participants in the *Robert A. Levy Fellows Workshop* at George Mason School of Law, and participants at the 2003 University of Maryland School of Business and the *Corporate and Securities I* panel during the 2004 annual meetings of the American Law and Economics Association. We also thank the Critical Infrastructure Protection Project at George Mason University for generous funding.

to infrastructure in real space. The response by many financial market centers, such as the New York Stock Exchange (NYSE) and the National Association of Securities Dealers Automatic Quotation (NASDAQ) system, was to create redundant back-up capacity at remote locations that would allow them to reopen their markets quickly in the event of a physical attack on their primary systems.[1]

The terrorist threat to cyber security in our financial system has received far less attention, with the Securities and Exchange Commission (SEC) increasing its focus on the physical threat following 9/11 while all but ignoring the cyber threat. We have strong reason to believe that the cyber threat to the U.S. financial trading network is substantial specifically because it is a network. The most obvious reason for concern is that the U.S. financial system is both the beacon of Western capitalism and the central nervous system of the U.S. economy. It is an all-too-tempting target. Also, the statistics on incident reports collected and disseminated by the Computer Emergency Response Team (CERT) show that a disproportionate number of security incidents occur in the financial industry.[2] A successful attack would dramatically weaken the system and at the same time signal its vulnerability to the rest of the world. A less obvious but equally important reason for concern is that U.S. financial market regulations over the past thirty years have actually increased the vulnerability of our trading systems to cyber terrorism.

Our conclusion is that the SEC's policy of communalizing the rights to market data – most importantly the right to real-time price quotes generated by various market centers – though very appealing as egalitarian politics, is contrary to our national interest in market security. By attenuating various market centers'

[1] The NYSE-owned Securities Industry Automation Corporation (SIAC) unveiled a highly redundant, geographically and physically diverse routing system called SFTI (Secure Financial Transaction Infrastructure) in 2002. *See* NYSE, New York Stock Exchange > Technologies, http://www.nysetransacttools.com/sfti/*; see also* U.S. Securities and Exchange Commission, *Policy Statement: Business Continuity Planning for Trading Markets*, SEC Policy Statement No. 34-485445 (October 1, 2003), *available at* http:/www.sec.gov/rules/ policy/34-48545.htm.

[2] *See* Thomas Glaessner, Tom Kellermann & Valerie McNevin, The World Bank, *Electronic Security: Risk Mitigation in Financial Transactions* 6 (2002); *see* Cert Statistics, http://www.cert.org/stats.

exclusive rights to market data and the price discovery system that generates it, SEC regulations dramatically reduced the incentive of these market centers to invest in cyber-security. As a result, the National Market System (NMS) is under far greater threat than need be.

Our analysis proceeds as follows. In section II, we outline the basic structure of the NMS. In section III, we show how the SEC's mandate for sharing market data leads to under-investment in price discovery. In section IV, we show how the networked nature of cyber-security and the associated economic incentives make the NMS highly vulnerable to attack owing to systematic under-investment in security by the various market centers. Finally, in section V, we show that the SEC has done little to protect the NMS from cyber threat and argue that restoring market centers' rights to market data and the price discovery infrastructure that generates it is an essential first step in protecting our nation's critical infrastructure.

II. THE STRUCTURE OF THE NATIONAL MARKET SYSTEM

As part of the 1975 Securities Acts Amendments to the Securities Exchange Act of 1934, Congress mandated that the SEC develop a National Market System (NMS) for equity securities trading to achieve the following five goals:[3] 1) economically efficient execution of securities transactions; 2) fair competition among brokers and dealers, among exchange markets, and between exchange markets and markets other than exchange markets; 3) availability to brokers, dealers, and investors of information with respect to quotations for and transactions in securities; 4) the practicability of brokers executing investors' orders in the best market; and, 5) an opportunity, consistent with the provisions of clauses (1) and (4) of this subparagraph, for investors' orders to be executed without the participation of a dealer. The NMS amendments envisioned that "linking all markets for qualified securities through communication and data processing facilities will foster efficiency, enhance competition, increase the

[3] *See generally*, Securities Exchange Act §11A (a)(1)(C).

information available to brokers, dealers, and investors, facilitate the offsetting of investors' orders, and contribute to best execution of such orders."[4]

Pursuant to the Congressional mandate, the SEC facilitated the creation of three electronic communications linkage systems that formed the core of the NMS for trading equity securities in the United States:[5] the Consolidated Tape System (CTS), the Consolidated Quotation System (CQS) and the Intermarket Trading System (ITS).[6] The CTS is an electronic linkage system that consolidates the last sale prices of all stocks listed on all exchanges and disseminates this information to all market centers in real time.[7] The CTS is supplemented by a number of NASDAQ-operated trading systems that disseminate the last sale information for Over-The-Counter (OTC) securities.[8] The CQS collects and disseminates current bid and ask quotations from and to all market centers. In contrast to the CTS, the CQS reveals pre-transaction information; that is, standing orders to buy and sell.[9] This system in some ways is the core of the NMS. The ITS is a computer system that allows participants to route orders among the participating markets to execute trades with the best price quotes, as displayed by the CQS.[10] The Computer-Assisted Execution System (CAES) is a companion system operated by NASDAQ that automates order routing and execution for securities listed on domestic exchanges in the ITS.

[4] Securities Exchange Act §11A (a)(1)(D).

[5] Laura Nyantung Beny, U.S. *Secondary Stock Markets: A Survey of Current Regulatory and Structural Issues and a Reform Proposal To Enhance Competition*, 2002 Colum.Bus. L.Rev. 399, 415 [hereafter Beny (2002)].

[6] The stock exchanges that are linked by the ITS plan are the American Stock Exchange LLC (Amex), Boston Stock Exchange, Inc. (BSE), Chicago Board Options Exchange, Inc. ("CBOE"), Chicago Stock Exchange, (CHX), Cincinnati Stock Exchange (CSE), NASD, New York Stock Exchange, Inc. (NYSE), Pacific Exchange, Inc. (PCX), and Philadelphia Stock Exchange, Inc. (PHLX).

[7] Beny (2002), *supra* note 5 at 415.

[8] Beny (2002), *supra* note 5 at 415.

[9] Beny (2002), *supra* note 5 at 416.

[10] *Report of the Advisory Committee on Market Information: A Blueprint for Responsible Change, available at* http://www.sec.gov/divisions/marketreg/marketinfo/finalreport.htm#joint (last accessed August 1, 2009).

When linked to ITS, market makers on NASDAQ can execute trades in securities listed on the NYSE and other exchanges through CAES with specialists on the associated exchange floor.

The CTS is operated by the Consolidated Tape Association (CTA) Plan, the CQS is operated under the Consolidated Quote (CQ) Plan, and the ITS is operated under the ITS Plan.[11] Each of these plans was jointly developed through agreement of the various market participants and governs not only the operation of the linkage systems but also the division of market information revenues.[12] Each market participant in the CTA Plan names one representative to the CTA committee. The CQ Plan is also administered by an operating committee that is substantially the same as the CTA committee.[13] Each of these plans is administered by a network administrator, who contracts with vendors and subscribers to provide commercial access to network data. For administering and processing data generated in exchange-listed stocks, including supplying market data to various intermediate vendors such as Bloomberg and Quotron, the NYSE and AMEX jointly created the Securities Information Automation Corporation (SIAC).[14] In November 2006, the NYSE acquired AMEX's one-third stake and assumed full ownership of the SIAC.[15]

Until recently, the NMS plans allowed market participants to jointly set fees for access to market information and also jointly determine the way market data revenues were allocated among the participants in the plans. After subtracting operating expenses, each Network's revenues generally were distributed to its participants in proportion to their share of total transaction volume in the Network.[16] The exchanges submit their data to a central processor (the SIAC for exchange-listed stocks) through the communications linkages

[11] *Id*.
[12] *Id*.
[13] *Id*.
[14] Joel Seligman, *Rethinking Securities Markets: The Sec Advisory Committee On Market Information And The Future Of The National Market System*, 57 BUS. LAW. 637, 643. (Feb.2002) [hereafter Seligman (2002)].
[15] NYSE news release dated November 1, 2006. *Available at* http://www.nyse.com/press/1162379705276.html. Last accessed August 1, 2009.
[16] Seligman (2002), *supra* note 14 at 645.

outlined above. The central information processor consolidates the data and disseminates it to vendors and subscribers and charges access fees. For many years, the SEC shied away from directly regulating the market data fees that can be charged. Instead, the NMS plan participants were required to decide these fees and any changes were made through majority (2/3) voting.[17] Each participant in the NMS plan gets one vote; *i.e.*, the votes are not weighted according to market share of trading volume generated. The revenues received from selling the market information were distributed among the participants according to their proportional share of total transactional volume.[18] While there were problems associated with even this hands-off approach to market data fees and revenue allocation, the SEC has recently taken steps that worsen the situation. In its recent Regulation NMS ruling, the SEC has purported to regulate the market access fees and allocation of market data fees. To understand why the SEC's approach is problematic, we need to understand the economic incentives created by the National Market System.

III. ECONOMIC INCENTIVE EFFECTS IN THE NATIONAL MARKET SYSTEM

Perhaps the most important function of a securities trading network is price discovery. Mulherin, Netter, and Overdahl (1991) argue that the central function of financial exchanges is to create markets in standardized contracts and to exclusively assign rights to price quotes.[19] By mandating that exchanges share this information through the CQS, the NMS essentially denies the exchanges proprietary rights to the price quotes they generate.[20] The denial of exclusive

[17] SEC concept release No. 34-42208; File No. S7-28-99 on Regulation of Market Information Fees and Revenues.

[18] Seligman (2002), *supra* note 14 at 647.

[19] Mulherin, Harold J., Jeffry M. Netter, and James A. Overdahl, *Prices are Property: The Organization of Financial Exchanges from a Transaction Cost Perspective*, 34 J. Law & Econ. 591 (1991) [hereafter Mulherin, Netter, Overdahl].

[20] "The (NMS) plans also govern two of the most important rights of ownership of the information – the fees that can be charged and the distribution of revenues derived from those fees. As a consequence, no single market can be said to fully "own" the stream of consolidated information that is made available to the public. Although markets and others may assert a

rights to market information results in free-riding and erodes the incentives of market centers – the self-regulatory organizations (SROs) such as the NYSE and electronic communication networks (ECNs) such as NASD (the SRO for NASDAQ) – to protect the integrity of market data and the price discovery mechanisms that generate it. This situation is analogous to that created by the Telecommunications Act of 1996, which mandated that the incumbent telecommunications provider share its network with entrants. This essentially was a denial of property rights to the incumbent in its capital investment.[21]

By denying property rights to market information, the NMS discourages investment in the price discovery function. Other scholars claim the SEC has gone about implementing the 1975 Congressional mandate to establish a NMS in the wrong way. Macey and Haddock (1985) argue that when it charged the SEC with responsibility for establishing a true NMS, Congress expected the SEC to deregulate the market by removing off-board trading restrictions and other rules (most importantly the off-board trading restrictions the NYSE imposed on its member firms) the exchanges or the SEC had in place at the time to suppress competition.[22] In their view, the right way to establish a NMS would have been to remove these restrictions and allow "the market to dictate the evolution of the appropriate communication systems."[23]

The current NMS structure instead encourages competition for order flow (trading volume) rather than competition in price discovery and the quality of the resulting price quotes. This is because the SEC's actual policy has been to encourage trading in NYSE- or NASDAQ-listed stocks by nonmembers on

proprietary interest in the information that they contribute to this stream, the practical effect of comprehensive federal regulation of market information is that proprietary interests in this information are subordinated to the Exchange Act's objectives for a national market system." SEC Concept Release No. 34-42208.

[21] *See* Robert S. Pindyck, *Mandatory Unbundling and Irreversible Investment in Telecom Networks*, NBER Working Paper 10287, Feb. 2004, (arguing that network sharing regulations reduce incentives to build new networks or upgrade existing ones).

[22] *See* Jonathan R. Macey & David D. Haddock, *Shirking at the SEC: The Failure of the National Market System*, 1985 U. ILL. L. REV. 315, 323-324 (1985) (hereafter Macey and Haddock).

[23] Macey & Haddock *supra* note 22 at 324.

regional exchanges and proprietary ECNs. This policy is based on the assumption that the NYSE would otherwise dominate stock trading, much along the lines of a garden-variety monopolist in the standard "structure-conduct-performance" paradigm, in which market concentration is purely a reflection of inefficiency in allocation (monopolization) with no consideration to offsetting productive efficiencies (economies of scale or scope or network effects). Anyone with even a modest understanding of competition policy understands that this is a completely stale and discredited notion.[24] Nevertheless, to mold competition along the lines envisioned by the model of perfect competition, which assumes a large number of buyers and sellers and low concentration, the SEC mandated creation of the CQS to allow the regional exchanges to compete with the NYSE for trading volume using its own price quotes. The effect of this policy has been to encourage the practice of payment for order flow, whereby secondary market centers pay brokers to route their order to their venue for execution. These side payments encourage brokers to route orders to market centers that do not necessarily provide the best price quote, and as a result the diverted orders never contribute to the price discovery function or the depth of the market; order flow is fragmented, while price discovery is centralized but much thinner than it otherwise would be.[25]

The ITS trade-through rules require brokers to execute orders at prices no worse than the National Best Bid/Offer (NBBO), as displayed by the CQS. The ITS is the limb of the NMS that allows brokers to transmit orders between markets. If a specialist or floor broker sees a better price in the CQS available on another exchange, the ITS system requires transmission of a "commitment to trade" to the appropriate participating market. The market maker in the other market must either accept or decline the commitment. ITS, however, relies on specialists and floor brokers to examine quotations displayed on screens above the specialists' posts, insert orders for electronic transmission to another market center, and make timely responses to commitments to trade from other market centers. Ferrell (2001) argues that NYSE specialists deliberately withhold their

[24] *See* Robert Bork, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF (1978).
[25] Beny (2002), *supra* note 5 at 431-433.

best quotes from the CQS to raise their competitors' costs,[26] and that they routinely provide floor brokers with better quotes and lower execution costs by matching or improving upon the NBBO as displayed by the CQS. Moreover, block transactions (orders of 10,000 shares or more), as well as posted price quotations of 100 or more shares, were exempt from the ITS trade-through rule. As a consequence, the ITS's share of trade volume remained very low. In 1999, 5.4 billion shares traded through the ITS, which was approximately two percent of aggregate consolidated tape volume.[27] This should not be surprising since the ITS trade-through rules essentially required market makers to either provide better prices or surrender trades to a competitor in another market resulting in a loss of fees to the market maker.

These practices, and the attendant inefficiencies, are the result of denying market centers that provide price discovery exclusive rights to their price quotes. The dominant market, which is forced to subsidize secondary markets, then either attempts to circumvent the integrated system or strategically under-invests in price discovery. Secondary markets, on the other hand, over-invest in reliance on the availability of price quotes from the dominant market and consequently also under-invest in the price discovery function. The overall result is fragmentation and reduced liquidity, which is contrary to Congress's stated goals of fostering competitive, thickly-traded, and efficient capital markets. The SEC's new order protection rules under Regulation NMS purport to close the gaps in the ITS plan and possibly eliminate the ITS linkages entirely. Instead, they allow private linkages to take the place of the ITS.[28] Allowing private linkages to develop and take the place of the ITS seems to be a step in the right direction, but the details of how the private linkages will work are unclear at this time. On the other hand, the SEC's newfound enthusiasm to impose limits on access fees, and more importantly to regulate market data fees, could worsen the problem.[29]

---

[26] Allen Ferrell, *A Proposal for Solving the "Payment for Order Flow" Problem*, 74 S. CAL. L. REV. 1027 (2001).

[27] Joel Seligman, *Rethinking Securities Markets: The SEC Advisory Committee On Market Information And The Future Of The National Market System*, 57 BUS. LAW. 637, 670 (2002).

[28] *See* Rule 610 of Regulation NMS, SEC Final Rule on Regulation NMS.

[29] *See* Rule 610 of Regulation NMS, SEC Final Rule on Regulation NMS.

To understand why the SEC's approach to ensuring better competition in the NMS is suboptimal, it is useful to digress to explain the economics of financial trading. Financial trading is a network industry that exhibits network effects[30] and a tendency toward a market structure with one dominant player. Network effects are said to exist when individual benefits or costs of being a part of the network increase or decrease, respectively, with the number of other participants in the network. The network may be either physical, such as the telecommunications network, or virtual, such as the "network" of users of particular software. The following section explains why network effects might efficiently lead to a highly concentrated market structure and why mandating network sharing by participants, rather than enforcing negotiated rights to the network, is an ill-advised way to approach the problem.

The Economics of Networks

Some well-known examples of network effects occur in computer software markets and telecommunications, although the QWERTY typewriter keyboard is perhaps the most notorious example.[31] These settings exhibit both the demand-side and supply-side economies of scale that are characteristic of most network industries.

Supply-side economies of scale exist when increasing the scale of production (increasing total volume holding the rate for production constant) reduces long-run average cost.[32] When supply-side economies of scale exist ─ classic scale economies in production ─ market structure usually tends toward a natural monopoly.[33] Most public utilities, such as electricity, water, cable

[30] For definitions and a discussion of network effects see Nicholas Economides, *The Economics of Networks*, 14 Int'l J. of Ind. Org. 673 (1996). *See also* Supriya Sarnikar, *Empirical Essays on Network Effects in Markets* (University of Arizona, Ph.D Dissertation, 2002) for a survey of the literature in this area and for an analysis of the impact of network effects on market outcomes.

[31] S.J. Liebowitz & Stephen E. Margolis, *The Fable of the Keys*, 33 J. Law & Econ 1 (1990).

[32] Robert S. Pindyck & Daniel S. Rubinfeld, *Microeconomics*, Sixth ed. P. 237 (hereinafter Pindyck and Rubinfeld).

[33] Pindyck & Rubinfeld at 362.

television, local telephone, etc., exhibit supply-side economies of scale.[34] While technological changes may have eliminated economies of scale in electricity generation, electricity distribution still exhibits economies of scale.[35] Forcing the entry of new firms into electricity distribution in the presence of significant economies of scale will have undesirable consequences for electricity consumers because, by dividing output between more firms, each firm's average cost of production increases and leads to higher prices for end users.[36]

Demand-side economies of scale are said to exist when the benefit derived by consumers from a product or service increases as the number of users increases.[37] The benefit from buying a phone, setting up an e-mail account, or installing instant-messaging software on your computer, for example, is greater when there are others who also have compatible phones, e-mail accounts, or instant-messaging software. One need only recall the television ad for a popular cell phone service provider, in which the size of the army of users is shown to reflect the quality of service. Without other users, the full benefit of the product or service cannot be realized because benefits increase with the number of users. Such demand-side benefits-of-scale are variously called "network externalities" or "network effects" in the economics literature.[38] Just as supply-side economies of scale lead to concentration, the presence of network benefits leads to the

[34] Pindyck & Rubinfeld at 362.

[35] *See* Paul L. Joskow, *Restructuring, Competition and Regulatory Reform in the U.S. Electricity Sector*, 11 J. ECON. PERS. 119 (1997).

[36] When a monopolistic industry with strong supply side economies of scale "is broken up into two competing firms, each supplying half the market, the average cost for each would be higher than the cost incurred by the original monopoly." Pindyck & Rubinfeld at 362, ¶6.

[37] *See* Michael L. Katz and Carl Shapiro, *Network Externalities, Competition and Compatibility*, 75 AM. ECON. REV. 424, 425 (1985) (first using the term "demand-side economies of scale" to describe a network externality); *see also* Neil M. Gandal, *Hedonic Price Indexes for Spreadsheets and an Empirical Test for Network Externalities*, 25 RAND. J. ECON. 160 (1994) (defining a network externality).

[38] Pindyck and Rubinfeld describe network externalities as the phenomenon "when each individual's demand depends on the purchases of other individuals." *Supra* note 32, at 132 ¶2. *See also* S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 J. ECON. PERS 133, 135 (1994) (preferring the use of the term 'network effects' over 'network externalities' to describe such phenomena)

standardization of product attributes, which may be most economically supplied either by a single firm, or by multiple firms adhering to a common standard, depending on the presence or absence of supply-side scale economies.

Network Effects in Financial Trading

A major function of financial markets is to provide liquidity, which is generally defined as the ability of investors to buy or sell assets such as financial securities in a short period of time without causing a significant change in the price of the asset being traded.[39] Thickly-traded markets that attract a lot of buy and sell orders are, in general, more liquid than thinly-traded markets that attract fewer orders. Thus, securities investors who route their trades to a central market generate positive network effects in financial trading,[40] and those who prefer high liquidity will naturally prefer to trade in a centralized market (all else being equal).

If the central market is operated by a for-profit firm and is prevented from engaging in price discrimination across traders, complete centralization may produce less liquidity than is socially optimal because of the monopolist's incentive to restrict access to its facilities so as to appropriate the rents accruing to the network ─ the classic natural monopoly problem.[41] Instead of combating this problem by encouraging investments in creation of greater liquidity, the SEC has mandated electronic linkages that communalize the benefits of price discovery created by the network. Even in its latest attempt to foster competition

[39] Nicholas Economides & Aloysius Siow, *The Division of Markets is Limited by the Extent of Liquidity: Spatial Competition with Externalities,* 78 AM. ECON. REV. 108 (1988)

[40] *See* Craig Pirong, *Securities Market Macrostructure: Property Rights And The Efficiency Of Securities Trading*, 18 J.L. Econ. & Org. 385 (October 2002). *See also* Economides and Siow, *supra* note 39 at 108.

[41] *See* Economides & Siow, *supra* note 39 at 108-109. Note that a highly centralized market such as the NYSE may be limited in its ability to capture the rents accruing to the network owing to the threat of potential competition. From its inception in 1792 until passage of the Securities Act (1933) and Securities Exchange Act (1934), the NYSE faced repeated competition from upstart markets. In every case it met competition from rival exchanges. *See* Mulherin, Netter, & Overdahl *supra* note 19.

through NMS, the SEC fails to recognize the role of economic incentives that encourage investments in price discovery.

Moreover, the SEC continues to resist appeals from the exchanges to be allowed to independently set the prices for the market data they create. As part of the NMS plans, and as outlined in the previous section, the exchanges sell consolidated market data at prices agreed upon by all plan participants. The revenues from the market data are then allocated proportionately according to trading volume generated by each exchange. This revenue allocation scheme allows smaller exchanges to "free ride" on the price discovery benefits created by the dominant NYSE.

Evidence relating to comparative revenue shares of the exchanges suggests that the smaller exchanges are subsidized by the larger exchanges as a result of the mandated sharing of price information. The NYSE ends up bearing a larger share of the costs of operating the NMS because of the way the costs and revenues from the sale of price information are allocated. The central NMS data processor for NYSE listed securities, the SIAC, is compensated at cost. The collective market data revenues received by selling the transaction data generated by all the market centers together are reduced by the operating costs of the linkage system, which include the costs incurred by information processors but do not include the costs incurred by the market centers in creating that data. The remaining net revenues are then allocated to each market center according to the fraction of the total transactions. The fraction of total transactions is calculated by taking the total number of last-sale transactions reported by the market center and dividing it by the total number of last-sale transactions reported by all market centers. This method of allocating revenues has encouraged the market centers to break each trade into several smaller transactions so as to inflate their share of market data revenue. According to data presented in the Regulation NMS ruling, in 2004, the total market data revenue collected was $434.1 million, out of which the dominant NYSE received only $141.9 million (roughly 33%). The NYSE's share of the market data revenues pales when compared to other exchanges worldwide. The London Stock Exchange, which in 2003 handled a trading volume of $3.6 trillion compared to the NYSE's $9.7 trillion, received about $180 million in market data revenues. By comparison, the NYSE handled

trading volume of $9.7 trillion but received only about $172 million in market data revenues. Given that price discovery and liquidity are the two main outputs of an exchange, by denying the exchanges the right to some measure of exclusivity over their market data is counter-productive in ways that regulators have thus far failed to recognize. The SEC's approach under the new regulation NMS is to treat the exchanges as public utilities with common-carrier status and to regulate the market access and market data fees. While it may be true that the financial trading markets will tend to be natural monopolies for reasons outlined earlier, rate regulation in the style of public utility regulation can have even more undesirable consequences because of complications arising out of the nature of the threat to cyber security.

IV. THE CYBER-THREAT TO THE NATIONAL MARKET SYSTEM

The incentive problems created by NMS regulation not only affect the efficient functioning of financial markets but also create incentive problems that lead to under-investment in cyber-security. The cyber-security industry itself suffers from under-investment due to network effects that are only partially internalized. Since cyber-security and financial trading both exhibit network effects, the incentive problems experienced in securing cyber-networks in the financial trading industry are compounded. The following subsection describes important incentive problems in the provision of cyber security.

Network Effects in Cyber Security

It is often said that a cyber network is only as strong as its weakest virtual link,[42] implying that investments by individual participants in a network to secure their own systems will be inadequate unless all other participants in the

[42] "Internet sites have become so interconnected and intruder tools so effective that the security of any site depends, in part, on the security of all other sites on the Internet." - Testimony of Stephen E. Cross, Director, Software Engineering Institute, Carnegie Mellon University before the Joint Economic Committee, US Congress dated February 23, 2000. *Available at* http://www.sei.org/.

network also secure their systems. Stated another way, a cyber network is secure if, and only to the extent that, all participants in the network secure their parts of the network.

Economists have shown, in general, that the presence of network effects often leads to socially sub-optimal choices by individual owners of network capital.[43] To ensure the socially efficient outcome, network participants are likely to coordinate their actions. But often-misaligned incentives and imperfect information in the face of positive transaction costs prevent coordination. Securing the cyber network requires that each participant invest the socially optimal amount in the security of its particular network capital. While individual participants bear the cost of such investment in security, the benefits of the investment are enjoyed by all participants in the network (though not necessarily equally). To see why network effects may lead to under-investment in cyber security, consider the following model originally proposed by Varian (2002)[44] and modified slightly here for simplicity.

Imagine in an industry of two firms, A and B, each invests effort, I_a and I_b, to secure its part of the cyber-network. The cost of each unit of effort by Firm A is C_a and that by Firm B is C_b. Each firm receives private benefits of V_a and V_b, respectively, if its network is secure and free of security-compromising incidents. Assume that the probability, P, that a firm's network is fully secure depends not only on its own efforts but also on the investments made by the other firm. Further assume that the probability of successfully warding off a cyber attack is a function of the minimum of the effort investment made by either firm. This is true in the case of at least some kinds of threats to cyber security, such as the threat of a distributed denial of service (DDOS) attack. Weak computers anywhere on the network can be used as zombies to launch a DDOS on otherwise secure systems. Unless all participants on a given network invest in

[43] *See* Sarnikar, *supra* note 28 (for a review of the economics literature on network externalities).

[44] Hal Varian, *System Reliability and Free Riding*, Conference proceedings of the 'Workshop on Economics and Information Security at University of California Berkeley, May 16-17, 2002', *Available at* http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity (last accessed August 1, 2009).

securing their systems, the security of the network as a whole can be jeopardized. The payoff to each individual firm is, therefore:

The payoff to Firm A is: $P(\min(I_a, I_b))\, V_a - C_a$

Similarly, the payoff to Firm B is: $P(\min(I_a, I_b))\, V_b - C_b$

Whereas, the social payoff is : $P(I_a + I_b)\,(V_a + V_b) - C_a - C_b$

If the firms choose the level of effort to invest in cyber security to maximize their private payoffs, in equilibrium they will each invest an equal amount, which is a function of the lowest cost-benefit ratio. i.e., $I_a^* = I_b^* = (C/V)_{min}$. The socially optimal level of investment is given by $(C_a + C_b)/(V_a + V_b)$, which is always higher than the individually rational outcome in the private equilibrium. To see why, imagine that Firm A has the minimum cost-benefit ratio so that both firms will invest an effort equal to C_a/V_a.

$(C_a + C_b)/(V_a + V_b) > C_a/V_a$ because $C_b > C_a$ and $V_b > V_a$.

This result remains even when the security of the network depends on the amount of information available about the type and level of threats. Gordon, Loeb and Lucyshin (2003) show that if appropriate incentives to share information on types of threats are not present, firms will tend to "free ride" on other firms' investment in security and tend to under-invest in information sharing mechanisms.[45] This is another statement of the coordination problem that is generally identified in the literature when significant network effects are present. When each network participant invests in the security of its own systems, it confers benefit on other participants. It is well established in the economics literature that the presence of positive external benefits often leads to under-provision of the good.[46] The good in this case is investment in the security

[45] Lawrence A.Gordon, Martin P. Loeb & William Lucyshyn, *Sharing Information on Computer Systems Security: An Economic Analysis*, 22 J. of Acct. & Pub. Pol. 461 (2003).

[46] *See* Pindyck & Rubinfeld at 644.

of the cyber-network. Gordon and Loeb (2002) develop an economic model of risk assessment from an individual firm's point of view to arrive at the privately optimal level of investment in cyber-security.[47] They conclude that a firm should focus on medium-level threats and that insuring security against high-level threats is sub-optimal for the firm because the costs exceed the firm's private benefits. This phenomenon presents a major problem in ensuring the security of most core infrastructures owing to their pervasive use and reliance on cyber networks, but it presents special problems in the security of financial trading systems because financial trading itself exhibits network effects as well.

All cyber networks are excessively vulnerable to hacking, but the financial sector's cyber networks are the most targeted by hackers for obvious reasons – to paraphrase Dillinger, "that's where the money is". Statistics on cyber-security incident reports provided by the Computer Emergency Response Team (CERT) show that the security of our financial networks has been consistently compromised and that both the number of incidents and the losses from each incident are steadily rising.[48] There are many reasons for this. First, the current state of the technology makes it impossible to prevent all attacks.[49] Second, ensuring security of the network requires constant monitoring because the internet security industry still engages primarily in a reactive process (i.e., a vulnerability is identified by a hacking incident or a virus/worm attack, and then a patch is developed and released) rather than a preventive process where the software security issues would be researched and addressed at the product

[47] Lawrence A. Gordon & Martin P. Loeb, *The Economics of Information Security Investment*, 5 ACM Transactions on Information and System Security, 438 (2002) [hereafter, Gordon and Loeb (2002)].

[48] CERT data (*See* Tom Kellermann, *Mobile Risk Management: E-finance in the Wireless Environment*, World Bank Discussion Paper, May 2002).

[49] "Current design and implementation of information infrastructure is flawed ….technology is too complex and confusing for users to make good decisions, (i.e., this will take time to fix)." CERT/CC Overview on Incident and Vulnerability Trends at 10. *Available at* http://www.cert.org/present/cert-overview-trends/module-4.pdf (Last accessed on May 1, 2004).

development stage.[50] The nature of software development implies that even the best software will be flawed and that system administrators are often overwhelmed with the number of patches that need to be applied to software already installed.[51] An increasing number of attacks are based on known vulnerabilities for which imperfect patches have already been issued.[52] Third, adding to these problems is that the number of well-qualified security professionals is still very low and, consequently, ill-qualified people oftentimes perform this critical function.[53] Fourth, most cyber-attacks are invisible to the ultimate customer. The quality of the service (of security provided) is not observable by the ultimate user. In fact, most damages caused by hack attacks

[50] David Alderson & Kevin Soo-Hoo, *The Role of Economic Incentives in Securing Cyberspace*, CISAC Report, Stanford University, Nov. 2004 (market conditions encourage commercial software companies to bring the product to the market before it is completely ready).

[51] "When vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may be too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term – system maintenance is never-ending. Because managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply." – quote from testimony of Stephen E. Cross, Director, Software Engineering Institute, Carnegie Mellon University before the Joint Economic Committee, US Congress dated February 23, 2000.

[52] David Alderson & Kevin Soo-Hoo, *The Role of Economic Incentives in Securing Cyberspace*, CISAC report, Stanford University, Nov. 2004 (documenting an interesting incident in 2003 when the Slammer worm attacked more than 90% of the Internet in under ten minutes by exploiting a known vulnerability in the Microsoft SQL server software for which a patch had been developed more than six months earlier. Among the compromised machines were several at Microsoft Corporation itself!) at 9.

[53] CERT/CC reports that it receives a substantial number of calls on its hotline from system administrators who do not know what a software patch is. As a result, most of the compromises that occur are as a result of hackers exploiting well-known vulnerabilities for which security patches were available but the system administrator simply failed to apply the patch. Also, the increasing number of vulnerabilities found each day also makes it difficult for a system administrator to ensure that all required patches are installed. Very often, a system administrator may not know all the different software that has been installed on his or her network by individual users. *See* CERT/CC Overview, *supra* note 48.

remain hidden[54] for long periods, suggesting that system administrators responsible for ensuring network security have little incentive to report incidents to upper management or to the popular press. All of this illustrates the poor incentives for investment in cyber security many firms' organizational structures provide.

Last, but by no means least, is the problem presented by the effects of reputation. Financial institutions realize the importance of maintaining a good reputation among their customers for asset security within the broader financial system. Partly owing to the flawed nature of current software products, however, they find themselves vulnerable to cyber attacks.[55] The general public expects its financial institutions to be secure; any hacking incident that might harm a financial firm's reputation very likely will be kept hidden from the public when it is possible to do so. The following quote attributed to Cornelius Tate, Special Agent, CERT, poignantly illustrates the problem.

> I think the dollar loss is actually higher than what is being reported. In my experience, I see companies not reporting or downplaying their compromises or losses. I think a lot of the reduced reporting comes down to the company attempting to reduce the 'shock' to the stockholders and the public. I think you will see noticeable increase in the dollar

[54] After a successful computer system intrusion, it can be very difficult or impossible to determine precisely what subtle damage, if any, was left by the intruder. - quote from testimony of Stephen E. Cross, Director, Software Engineering Institute, Carnegie Mellon University before the Joint Economic Committee, US Congress dated February 23, 2000. *Available at* http://www.cert.org.

[55] *See* Table 2 (pg.9) of Tom Kellermann, *Mobile Risk Management, E-finance in the Wireless Environment*, The World Bank Discussion paper, May 2002. The table lists a number of security incidents at financial institutions including Citibank, Bloomberg, etc. and the amount of damages from each incident where available. In September 1995, for example, Citibank suffered over $10 million in losses from a single hacking incident and was able to recover only about $400,000. In 2001, hackers broke into Bloomberg's system and maintained access for six months before the intrusion was detected. Similar incidents disrupted trading on the NASDAQ in March 2000 after a denial-of-service attack perpetrated by a compromised computer system of Internet Trading Technologies company.

> amount from year to year (although the number of respondents remain consistent) because companies are more aware of the fact that everyone is susceptible to being a victim, and to be a victim has become acceptable and does not equate to a loss of 'public confidence'.[56]

Admittedly, most of the problems with securing cyber networks arise from the open nature of the Internet and the security loopholes in mass-produced commercial software. Dedicated proprietary networks,[57] such as those found in the NMS, are presumably easier to secure than the Internet itself. The NMS networks are for the most part isolated from the Internet. Third parties who intend to connect to the SIAC's networks must either use direct dedicated connections that cannot be used for any other purpose or they can use so-called extranet providers. The only contact the SIAC's network might have with the insecure Internet would be when it allows third parties to access its network through Virtual Private Network (VPN)[58] connections obtained from a regular Internet Service Provider. Even dedicated networks suffer from the same general flaws as the Internet. However, they are only as secure as the participants that connect to it. Their software can still have security holes even if it is custom-made. So far, hacking incidents in the financial trading sector have been motivated by financial gain[59] and have originated at the broker/vendor end of the

[56] Cornelius Tate, quoted in Tom Kellermann, *Mobile Risk Management: E-finance in the Wireless Environment*, Financial Sector Discussion Paper (World Bank), p. 10 (May 2002).

[57] The SIAC has moved to TCP/IP based network connections to provide access to the trading, clearing, and settlement systems as well as the market data distribution systems. The Secure Financial Transaction Infrastructure (SFTI) has built in high levels of physical and geographic redundancy. The SFTI offers vendors and brokers the option of connecting to at least two of the nine access centers that are geographically dispersed within and outside of Manhattan. The access centers are interconnected to each other and to the SIAC data centers with a highly redundant physical network. *See* NYSE Euronnext, Section on NYSE Technologies, *available at* http://www.nysetransacttools.com/sfti/ (last accessed July 22, 2007).

[58] Virtual Private Networks (VPNs) are a means of sending and receiving information securely over public networks such as the Internet.

[59] The most recent hacker stock scam involved an Eastern European cyber-crime gang that hacked into seven U.S. brokerage firms, sold the securities held by those firms, and used the

network, but the risk of compromise to trading networks is real and has the potential for creating catastrophic losses. The highest risk to the trading networks, as for all private company intra-networks, is from insiders. CERT survey data and reports show that insider risk is a rising threat for every cyber network.[60]

All the above problems are compounded when network participants not only have an incentive to under-invest in security because of the network effects but are also experiencing a mandate to share data and other system features under NMS regulation.

V. HOW TO PROTECT THE NATIONAL MARKET SYSTEM

The SEC has done very little to ensure the security of the cyber networks that facilitate financial trading. Its draft interagency white paper issued in the aftermath of 9/11[61] focuses on creating physical and geographic redundancy that is largely irrelevant to ensuring security of the cyber-network. Physical and geographic redundancy is a strategy that addresses potential problems of connectivity, i.e., problems with the electrical and telecommunication networks underlying the cyber-network. But this does nothing to combat the potential threats from cyber-terrorism. The issue of cyber-security is conspicuously absent from the report. Given the proprietary nature of the software and the dedicated nature of financial trading networks, the biggest threat to the NMS comes from

funds to buy millions of shares of a lightly traded penny stock to drive up its price. This was the third such scam the SEC has uncovered but only after it had been in operation for at least a year. Gregg Keizer, *SEC Freezes $3M Made in Hacker Stock Scam*, Computer World, March 9, 2007,, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=standards_and_legal_issues&articleId=9012699&taxonomyId=146.

[60] The CERT® Program, *Survey Shows E-Crime Incidents are Declining Yet Impact is Increasing*, *available at* http://www.cert.org/archive/pdf/ecrimesurvey06.pdf.

[61] SEC, Release No. 34-46432, File No. 57-32-02, Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Sept. 5, 2002).

insiders. One industry comment to the white paper[62] emphasized the insider threat to the cyber-networks, the threat from the weakest virtual link in the chain, and others.[63] The 2006 E-crime survey conducted by CSO magazine in conjunction with US-CERT[64] found that the insider threat is getting worse, with 55% of those surveyed reporting insider events, compared to 39% in 2005. The U.S. Secret Service, in conjunction with the CERT/CC, examined 23 incidents carried out by 26 insiders in the Banking and Finance sectors and found that most of the insider attacks were perpetrated by "non-technical personnel with little computer knowledge or training."[65] Some commentators have suggested that appropriate liability rules might combat the incentive problems in cyber security[66] under some circumstances. But these measures alone are insufficient if the underlying industry incentive structure is severely flawed, as in the case of the National Market System. As shown in Gordon and Loeb (2002) and in our adaptation of the Varian (2002) model in section IV, when network effects are present, private parties will under-invest in protecting against low-probability, high-impact incidents. In protecting critical infrastructure against the threat of cyber-terrorism, large investments that are privately sub-optimal but socially

[62] McNevin, Valerie, Esq., Office of Innovation, Comment on Draft Agency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (October 22, 2002), *available at* http://www.sec.gov/rules/concept/s73202/vmcnevin1.htm.

[63] For similar arguments that industry structures provide very weak incentives for cyber security investments in general, *see* Bruce Schneier, *No, we don't spend enough!*, Conference proceedings of the 'Workshop on Economics and Information Security at University of California Berkeley, May 16-17, 2002, *available at* http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity (last accessed August 1, 2009).

[64] *See* The CERT® Program, *supra* note 60, *available at* http://www.cert.org/archive/pdf/ecrimesurvey06.pdf.

[65] Randazzo, M., Keeny, M., Kowalski, E., Capelli, D., and Moore, A.P., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, Joint SEI and U.S. Secret Service Report, August 2004, http://www.cert.org/archive/pdf/bankfin040820.pdf.

[66] *See* Hal Varian, *System Reliability and Free Riding*, Conference proceedings of the 'Workshop on Economics and Information Security at University of California Berkeley, May 16-17, 2002', *available at* http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity. (last accessed August 1, 2009).

optimal should be taken as well. Given the positive external benefits and the potential for coordination failures, a role for a regulator is to facilitate natural inclinations to coordinate by network participants. In its rush to communalize financial trading, however, the SEC is destined to fail.

The only supervisory role the SEC plays in monitoring the automated linkage systems of the NMS is that it requests voluntary quarterly reports from network participants on (1) whether or not they have conducted stress tests of their automated systems, (2) current and future capacity estimates and (3) contracts with independent reviewers to assess annually whether their systems can perform adequately at current and future estimated capacity levels.[67]

Moreover, it appears the SEC has little in the way of immediate plans to protect cyber security in the NMS. The 2001 *Report of the SEC's Advisory Committee on Market Information* highlights a number of concerns regarding the integrity of market information and provides several recommendations for salutary reform,[68] none of which even purport to address cyber security. Given that the Committee issued its report in September 2001, this may be forgivable, but in the years since then the SEC has yet to show any inclination to address the issue. Most instructive is the *Report's* disclaimer that providing property rights to market data by those who generate it is contrary to Congress's policy that the SEC regulate financial markets to create a national market system. This appears to be incorrect. One of the most important things regulators can do to ensure the efficient functioning of any market is to enforce private property rights to discovered opportunities that would otherwise be beyond the ability of market participants to uncover owing to free rider or collective action problems. Nowhere is this truer than with regard to financial market cyber security. Rather than being contrary to effective regulation, the enforcement of private property rights to market data is absolutely essential because it gives market participants a greater stake in protecting their systems than does the current regime of communalized rights to market data and other network features.

[67] SEC Policy Statement: Automated Systems of Self-Regulatory Organizations, Release No. 34-27445 (Nov. 16, 1989); *see also* SEC Policy Statement: Automated Systems of Self-Regulatory Organizations (II), Release No. 34-29185 (May 9, 1991).

[68] *Available at* http://www.sec.gov/divisions/marketreg/marketinfo/finalreport.htm#joint.

VI. CONCLUSION

The most important objective of national cyber security is to ensure that those in a position to protect our national market system have the incentive to do so. By mandating the communalization of price data, the SEC has put the NYSE and other market centers on a financial razor's edge, and they will have too little to lose from lapses of security and the inevitable cyber-breach. On such an occasion, they can simply redeploy their assets to an alternative pursuit with little private loss. The key to maintaining national cyber security in financial trading is to ensure that the participants who can make a difference – the men and women "on the spot" – have something substantial to lose in the event of a breach: so-called "economic rents."

Our nation's regulators and politicians must come to grips with the concept of economic rents. It is essential that economic rents accrue to the many personal relationships necessary to establish the trust that allows our financial markets to operate efficiently. Atomizing financial markets in the face of clear supply-side scale economics and demand-side network effects is a prescription for injury to investors and the national economy more generally. Antitrust regulators learned roughly this lesson after repeated failures of attempts to force American industry to conform to the assumptions of the model of perfect competition. Similarly, the SEC must avoid the deterministic fallacy of forcing the NMS to conform to these same assumptions.

REFERENCES

Alderson, David and Kevin Soo-Hoo. "The Role of Economic Incentives in Securing Cyberspace." CISAC Report, Stanford University, Nov. 2004.

Beny, Laura Nyantung. "U.S. Secondary Stock Markets: A Survey of Current Regulatory and Structural Issues and a Reform Proposal To Enhance Competition." *Columbia Business Law Review* 2002: 399-473.

Bork, Robert. *The Antitrust Paradox: A Policy At War With Itself* (1978).

Computer Emergency Response Team. "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector." Available at http://www.cert.org/archive/pdf/bankfin040820.pdf.

Economides, Nicholas. "The Economics of Networks." *International Journal of Industria Organization* 55 (1996): 673- 699.

Economides, Nicholas and Aloysius Siow. "The Division of Markets is Limited by the Extent of Liquidity: Spatial Competition with Externalities." *American Economic Review* 78 (1988):108- 121.

Ferrell, Allen. "A Proposal for Solving the 'Payment for Order Flow' Problem." *S. CAL. L. REV.* 74(2001): 1027- (2001).

Gandal, Neil M. "Hedonic Price Indexes for Spreadsheets and an Empirical Test for Network Externalities." *RAND Journal of Economics* 25(1994): 160- 170.

Glaessner, Thomas; Tom Kellermann; Valerie McNevin. "Electronic Security: Risk Mitigation in Financial Transactions." A World Bank Report (2002).

Gordon, Lawrence A. and Martin P. Loeb. "The Economics of Information Security Investment." *ACM Transactions on Information and System Security* 5(2002): 438-457.

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

Joskow, Paul L. "Restructuring, Competition and Regulatory Reform in the U.S. Electricity Sector." *Journal of Economic Perspectives* 11(1997): 119-138.

Katz, Michael L. and Carl Shapiro. "Network Externalities, Competition and Compatibility." *American Economic Review* 75(1985): 424-440.

Kellermann, Tom. "Mobile Risk Management: E-finance in the Wireless Environment." World Bank Discussion Paper, May 2002.

Keizer, Gregg. "SEC Freezes $3M Made in Hacker Stock Scam," *Computer World*, March 9, 2007.

Liebowitz, S.J. and Stephen E. Margolis. "The Fable of the Keys." *Journal of Law and Economics* 33(1990): 1-25.

Liebowitz, S.J. and Stephen E. Margolis. "Network Externality: An Uncommon Tragedy." *Journal of Economic Perspectives* 8(1994): 133-150.

Macey, Jonathan R. and David D. Haddock. "Shirking at the SEC: Failure of the National Market System." *University of Illinois Law Review* 1985: 315-362.

McNevin, Valerie, Esq., Office of Innovation, Comment on Draft Agency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.

Mulherin, Harold J., Jeffry M. Netter, and James A. Overdahl. "Prices are Property: The Organization of Financial Exchanges from a Transaction Cost Perspective." *Journal of Law and Economics* 34 (1991): 591.

Pindyck, Robert S. "Mandatory Unbundling and Irreversible Investment in Telecom Networks." NBER working paper 10287, February 2004.

Pirong, Craig. "Securities Market Macrostructure: Property Rights and the Efficiency of Securities Trading." *Journal of Law Economics and Organization* 18(2002): 385 -410.

Robert S. Pindyck and Daniel S. Rubinfeld. *Microeconomics.* 6th ed.

Sarnikar, Supriya. *Empirical Essays on Network Effects in Markets*. Ph.D. diss., University of Arizona, 2002.

Schnieier, Bruce. "No, we don't spend enough!" Conference proceedings of the 'Workshop on Economics and Information Security at University of California Berkeley, May 16-17, 2002'. Available at http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity. Last accessed 8/1/2009.

Securities Exchange Commission. *Report of the Advisory Committee on Market Information: A Blueprint for Responsible Change* available at http://www.sec.gov/divisions/marketreg/marketinfo/finalreport.htm#joint.

Securities Exchange Commission, Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Sept 5, 2002).

Securities Exchange Commission. *Business Continuity Planning for Trading Markets*, SEC Policy Statement No. 34-485445 (October 1, 2003).

SEC Concept Release No. 34-42208

Seligman, Joel. "Rethinking Securities Markets: The SEC Advisory Committee on Market Information and the Future of the National Market System." *Business Lawyer* 57(2002): 637 – 680.

Automated Review Policy I, SEC Policy Statement on Automated Systems of Self-Regulatory Organizations, SEC Release No. 34-27445.

Automated Review Policy II, SEC Policy Statement on Automated Systems of Self-Regulatory Organizations, SEC Release No. 34-29185.

Varian, Hal. *System Reliability and Free Riding*, Conference proceedings of the 'Workshop on Economics and Information Security at University of California Berkeley, May 16-17, 2002'. Available at http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity. Last accessed 3/15/2007.