CISAC
STANFORD
IIS

CENTER FOR INTERNATIONAL SECURITY AND COOPERATION

The Role of Economic Incentives in Securing Cyberspace

David Alderson
Kevin Soo Hoo

November 2004

Stanford University's Center for International Security and Cooperation, part of Stanford Institute for International Studies, is a multidisciplinary community dedicated to research and training in the field of international security. The Center brings together scholars, policymakers, scientists, area specialists, members of the business community, and other experts to examine a wide range of international security issues. The Center's mission has remained largely the same since its founding in 1983: To produce outstanding policy-relevant research on international security problems; to teach and train the next generation of international security specialists; and to influence public policy through public outreach, track-two diplomacy, and policy advising.

The Role of Economic Incentives in Securing Cyberspace

David Alderson
alderd@cds.caltech.edu

Kevin Soo Hoo
ksoohoo@packetmotion.com

Abstract

In the last eight years, every significant public policy initiative to address the safety and security of the U.S. national information infrastructure has recommended a significant, largely voluntary, role for the private sector, owing in large part to the dominant ownership stake of private entities in the infrastructure. Notably absent from much of the policy discourse and underlying research has been a careful examination of the stakeholder incentives to adopt and to spur the development of security technologies and processes. We believe that the lack of progress to date in achieving a secure and robust cyber infrastructure is in large part the direct result of a failure by public policy to recognize and to address those incentives and the technological, economic, social and legal factors underlying them.

We advocate a new approach for the analysis and development of coherent policy in which the interaction of economic incentives among stakeholders is explicitly considered. By economic incentives, we mean the full array of economic and technological factors that shape infrastructure decision-making, not merely government subsidies or tax credits. We provide an initial framework for understanding the technology dependencies and economic incentives associated with cyber security, along with illustrative examples of the key players and their motivations. We argue that the successful development of a secure cyber infrastructure will require more than improved technology and that it could be accelerated by careful consideration of the evolving economic and legal issues that shape stakeholder incentives.

Dr. David Alderson is currently a postdoctoral scholar in the Engineering and Applied Sciences Division of the California Institute of Technology. He is also a Senior Research Associate with the Preventive Defense Project at CISAC. Dr. Alderson received his PhD from the Department of Management Science and Engineering at Stanford University in 2003. His research addresses the technological, economic, and policy issues related to the management of the Internet and other large-scale infrastructure networks.

Dr. Kevin Soo Hoo is currently a security architect at PacketMotion, Inc., a network security appliance startup based in San Mateo, California. His research interests include quantitative metrics of information security, economic incentives and infrastructure vulnerability, and information security risk management. He graduated from Stanford University's Department of Management Science and Engineering with a PhD in Engineering-Economic Systems in June 2000, and the title of his dissertation was “How Much is Enough? A Risk Management Approach to Computer Security.”

1. The Rise of the Internet as a Critical Infrastructure

During the 1990s the Internet evolved from a platform on which government and university scientists exchanged research information to a core component of the national economic and social fabric. As the computer and networking technologies underlying the Internet became faster and more reliable, internets and intranets proliferated, connecting government, businesses, and citizens. With the decommissioning of the NSFNet in 1995, the ongoing development and maintenance of this national cyber infrastructure moved officially from the hands of the government to commercial and non-profit entities. Since that time, the drivers of Internet development and deployment have been largely commercial, and the agenda of the Internet has been that of entrepreneurs, investors, and corporations looking to achieve a revolution in business affairs.

The government's hands-off approach was a tremendous success, and during the late 1990s the Internet vaulted to prominence as a national infrastructure. The development of new technologies enabled tremendous breakthroughs in efficiency and productivity. These gains accelerated the drive to connect business, social, and even government processes, for example, billing, accounting, order management, banking, media distribution, retail shopping, income tax filing, social security, and voting, just to name a few. All of these processes were made faster, more accessible, and more cost-effective by embracing the Internet. However, this rise in productivity brought with it a growing dependence upon the cyber infrastructure. In many cases, the integration of Internet technology has become so extensive and pervasive that a return to the pre-network era is infeasible. As the complexity of the infrastructure increases, the potential for large-scale disruptions from system failures also grows. The occasional occurrence of significant failures has prompted many, both inside and outside of government, to question whether the government's "hands-off" approach is sufficient to protect the national interest in this ad hoc, yet now critically important infrastructure.

We believe that the fundamental problem behind the current infrastructure vulnerability is that the economic incentives for both makers and users of Internet technology are not aligned to compel the vigilant development, deployment, and application of secure technology. Government, as the defender of the public interest, is accorded both the responsibility and the power to reshape the market to foster a more secure infrastructure. However, government action to date has been restrained, falling short of active interference in the marketplace, preferring instead to study and publicize the problems of infrastructure vulnerability and, in so doing, call upon the private sector to take the initiative to solve them.

Government Efforts to Secure Cyberspace

From the time of its initial involvement in public debate on the problem of critical infrastructure vulnerability, the U.S. federal government has actively sought to understand the implications of the nation's growing dependence on this infrastructure (Table 1). However, in all discussions and policy initiatives the government has rejected direct regulation as an instrument for achieving this objective. The argument is that since the Internet and its associated infrastructures are neither owned nor operated by the federal government, it is neither appropriate nor feasible for the government to manage direct control of it. Instead, the government has espoused an approach in which *public-private partnership* would form the organizational basis for mitigating these vulnerabilities. The idea is that the mutual need for a robust cyber infrastructure with appropriate government oversight will naturally foster cooperation among key players. In this scenario, the role of government is simply to reduce any legal barriers to this cooperation and to encourage industry participants to set aside competitive concerns that might restrain their involvement. For example, in cases where a lack of trusted relationships among key players prevents the required cooperation, the government, as a trusted third party, could act in an information gathering and sharing capacity. In cases where a rapid and coordinated response is needed (for example, in the case of a

new computer virus or worm), the government could act in an information dissemination capacity to broadcast appropriate early warning messages.

Date	Initiative	Description	Result
July 1996	President's Commission on Critical Infrastructure Protection (PCCIP)	A cross-section of industry leaders, policy experts, and academics examined infrastructure vulnerabilities and their social, economic, and national security effects.	*Critical Foundations*, published in October 1997, concluded that the vulnerabilities were real, the risks were growing, and remedial action in the form of public-private partnership should be taken sooner rather than later
May 1998	Presidential Decision Directive 63	Created two new offices: National Infrastructure Protection Center (NIPC) & Critical Infrastructure Assurance Office (CIAO).	NIPC operated within the FBI to serve as a national analysis and warning center and to lead efforts within law enforcement. CIAO operated within the Department of Commerce to coordinate policy.
Jan 2000	*National Plan for Information Systems Protection V1.0*	Released through the CIAO, this plan was the first government plan for dealing with the problems outlined by the PCCIP.	This plan called for 3 federal initiatives: (1) establish public-private information sharing partnerships for each infrastructure industry; (2) perform vulnerability assessments and establish remediation plans for each infrastructure; (3) implement education and awareness programs.
Sept 2001	*Combating Terrorism: Selected Challenges and Related Recommendations*	General Accounting Office Report on National Plan implementation.	The report found that progress on the initiatives had been slow.
Oct 2001	Executive Order 13231	Created President's Critical Infrastructure Protection Board (PCIPB).	Board was assigned responsibility for coordinating all information system security within the Executive Branch and nationally as well.
Sept 2002	*Draft National Strategy to Secure Cyberspace*	Second government plan to address vulnerabilities within the national cyber infrastructures.	The plan echoed the recommendations of the previous plan and went further to specify detailed recommendations for both private and government initiatives.
Nov 2002	Department of Homeland Security (DHS)	NIPC, CIAO, and PCIPB were all reorganized under DHS	Significant personnel turn-over during reorganization slowed efforts to finalize and implement the national plan.
Feb 2003	*National Strategy to Secure Cyberspace*	Revised national plan released by DHS.	National Strategy was revised to eliminate all private-sector mandates.
July 2004	Audit by DHS Office of Inspector General	Assessment of progress DHS has made in implementing the National Strategy.	Limited progress in implementing major initiatives. Report provides specific recommendations that were accepted by DHS as future work.

Table 1. Policy initiatives of the federal government to promote a secure cyber infrastructure.

These policy initiatives have relied almost exclusively on "market forces" to create a robust and secure infrastructure. Generally speaking, these policies rarely specify in detail how such forces would or could work. To date, the current market forces have resulted in relatively little progress toward a secure cyber infrastructure. Consider the following examples.

1. Most widespread computer exploits to date have been based on vulnerabilities that were known, documented, and for which patches already existed [13].
2. Individual users and even corporations are slow to adopt and maintain best security practices when using the Internet. As noted in the 2004 Ernst & Young Global Information Security Survey [6],

   > "[T]here is little visible change in how security is practiced in many organizations. In 1994, a respondent told us, '*It is apparently going to take a major breach of security before this organization gets its act together*.' Some 10 years later, that sentiment is still quite evident and still typifies organizations' reluctance to deal with the significant threats and to invoke well-accepted controls. What we found in 2004 is that too many organizations feel that information security has no value when there is no visible attack.."

3. Developers of software and hardware often do not implement well-established best practices for building security into their products. [2][13].

As of this writing, security is perceived by most information technology developers and users as inconvenient and expensive. The result has been a general reluctance among individuals, corporations, and even government agencies to adopt the necessary measures that would make and keep the infrastructure secure. Yet, the approach of the government remains fundamentally unchanged. Government policy makers continue to shy away from traditional regulation as a solution, preferring instead to rely on non-coercive measures to encourage and entice stakeholders into securing the infrastructure, including:

1. *Lead by example*: Using the government's vast procurement budget, security requirements have been instituted for government purchases of information technology.
2. *Fund research*: DHS, DoD, NIST, DoE, and other government agencies have funded basic and developmental research into better security technologies.
3. *Establish standards*: NIST in cooperation with the NSA have been drafting standards for secure information technology, from hardware to software design and performance.
4. *Encourage information sharing*: Lead government agencies in every major infrastructure industry sector have helped establish vehicles by which industry participants can, without fear of prosecution, exchange information about information security threats, vulnerabilities, and incidents.
5. *Evangelize*: Through various venues government officials have used the bully pulpit to call for the general public's assistance in securing the cyber infrastructure.

The most recent National Plan attempts to use a "call to arms" to motivate the American public to adopt better security practices. Given recent history, the current National Plan seems unlikely to achieve any significant results with this approach.[1]

Why have the same market forces that yielded such incredible innovation and gains in productivity during the 1990s failed to achieve a robust and reliable infrastructure for the 21st Century? Why are the current government initiatives for public-private partnership unlikely to achieve the desired results? To answer these and related questions, we must consider the role of economic incentives in the context of cyber infrastructures.

2. The Reality of Economic Incentives

A principal reason for the failure of current policy to effect a more secure infrastructure may be a poor appreciation of the economic incentives at work in the marketplace. Because the private sector owns and operates such an overwhelming majority of the cyber infrastructure, an understanding of the economic realities that shape its decision processes can help to explain why government efforts to secure the infrastructure have been stymied. Furthermore, an examination of these incentives can also point to possible policy solutions for reshaping the marketplace to encourage better security without coercive regulation.

Economic incentives encompass a wider set of consumer preferences than simple dollars and cents. The hypothesis that the free market will, on the basis of competition, arrive at a secure infrastructure is itself rooted in assumptions about the economic utility of a secure infrastructure versus an insecure one. The argument goes something akin to this: "Secure products will have a lower cost of ownership and therefore should beat out products that are riddled with security vulnerabilities." And yet, in spite of this

[1] In October 2004, the Director of the National Cyber Security Division at DHS resigned—the third resignation by a cybersecurity chief in 18 months—raising concerns about the efficacy of DHS efforts on cybersecurity.

eminently reasonable heuristic argument, the problem of infrastructure security seems to have worsened rather than lessened. What went wrong?

Many of the potential pitfalls associated with relying on the market to provide computer security products have been known for more than 15 years [16]. Most recently in the context of the modern Internet, scholars have presented several candidates to explain the lack of adequate cyber infrastructure security, involving moral hazard and perverse incentives. Examples include Varian's free riders in information infrastructure security [17], Gordon's asymmetric information between the chief security and chief financial officers of a corporation [9], and Anderson's general survey of perverse incentives in information insecurity [1]. These market failures all may be, to some degree, at work. However, even if the general thrust of the argument in favor of market forces is correct, it may take decades for truly secure products to triumph in the marketplace. In the mean time, the day-to-day business imperatives such as pricing, product features, and vendor market power will continue to dominate. Recent history seems to suggest that the power of security to convey decisive competitive advantage is much overstated. Most germane to our purpose, the security of critical infrastructures that rely on the privately-owned, international, and poorly understood cyber infrastructure is not assured, and certainly not transparently assured, by the decisions of actors in the marketplace.

If government policy is to depend upon the free market to secure the information infrastructure, then its policy should be informed by an understanding of the market forces upon which it is relying. If those forces do not adequately provide for critical infrastructure security, as the above failures would seem to suggest, then policy changes are needed to correct them. Appropriate economic incentives are a necessary condition for a secure and robust cyber infrastructure, regardless of whether they come at the request of the federal government or from the market at large. In other words, ultimately:

1. Stakeholders (owners, operators, users) of the Internet must have clearly defined responsibilities for securing their own systems and (economic, legal) liabilities for contributing to overall vulnerability that are commensurate with their level of involvement, criticality, and capability; and
2. The impact and consequences of stakeholder behavior must be readily measurable.

Current policy initiatives, particularly the National Strategy, do not address directly this issue of assigning responsibility, relying instead on a general principle of *everyone* being held accountable for *everything.* In practice, this approach results in a situation where nobody can be held immediately and legitimately accountable for failure. In this regard, the government, as the *only* party that can advocate on behalf of national security interests, has the role and responsibility to manage the interactions among stakeholders. To do this, the government must understand the needs and constraints of software vendors, ISPs, and other infrastructure providers. Though the collaborative approach of a public-private partnership is necessary, it may be insufficient to solve the problem.

3. Understanding Vulnerabilities in Cyber Infrastructure

Recognizing the economic aspects of this multidisciplinary problem is not enough, however, to identify and pursue a remedial course of action. Cybersecurity is an inherently difficult problem, due largely to the complexity of the technical components and their dependencies, and to the complexity of the economic relationships among stakeholders. Here, we outline some of the fundamental technological dependencies along with basic stakeholder roles and relationships that contribute to the overall security of the Internet and related cyber infrastructures.

The robustness, interoperability, and adaptability of the Internet can be attributed to a set of fundamental network design principles (e.g., layering, end-to-end, transparency) adopted by the early builders that has yielded a layered architecture consisting of a suite of protocols (i.e., the "TCP/IP protocol stack"). Most simply, consider a framework in which the underlying ***network infrastructure*** supports the provisioning of ***network services*** (Table 2). Here, network infrastructure denotes the hardware/software required to enable the movement of data across the network, including the physical hardware (e.g., routers, switches, servers) and the protocols (e.g., TCP, IP, DNS, BGP) used to encode and transmit data. In contrast, network services are the end-to-end services that provide basic functionality to users of the network. These services depend on the network infrastructure and are themselves the building blocks of more sophisticated applications. Examples include the worldwide web (WWW), electronic mail, and peer-to-peer (P2P) file transfer.

This *vertical decomposition* of functional layers is complemented by a *horizontal decomposition* of decentralized technical components that implement these protocol layers and provide robust performance in the presence of individual component loss [18]. In the horizontal dimension, individual network components can be differentiated as being part of the ***network core*** (internal to the network) or at the ***network edge*** (an end host). Core components include physical hardware, such as routers, switches and cables, as well as the software required to operate them. In contrast, edge components are the systems at the network endpoints, such as desktop computers or servers, including all of the software required to operate them.

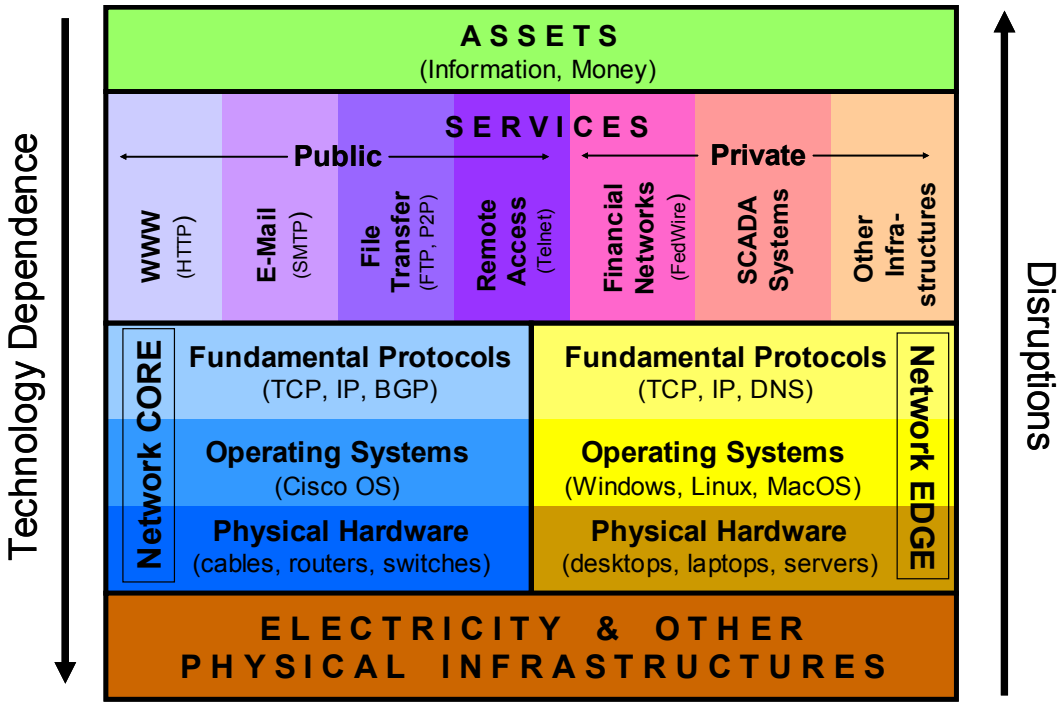

Table 2. Overall schematic representation of cyber infrastructure. Dependencies are shown from the top down. Since the purpose of the network is to provide access to information assets, they sit at the top of the diagram. Public and private network services are dependent on a network infrastructure that is implemented in vertical functional layers and distributed among machines at the network edge and in the network core. The most fundamental layer is the physical hardware, which is itself dependent on the electricity infrastructure.

Network services depend on the end-to-end delivery of data across the network infrastructure. Often, these end-to-end services themselves are the building blocks of more sophisticated applications. We differentiate two basic types of network services. ***Public services*** are defined by openly available protocols, and anyone wanting to implement the service on the network need only to conform to the

associated protocol specification. Examples (and their underlying protocols) include the worldwide web (HTTP), electronic mail (SMTP), file transfer (FTP), and remote access (Telnet). ***Private services*** have restricted access and may be implemented using proprietary applications and protocols. Examples include financial networks (e.g., FedWire), virtual private networks (VPNs), and supervisory control and data acquisition (SCADA) systems used to control other systems or infrastructures. Private services are often run over common public network infrastructure; although, if the service is important enough, they may be operated over a separate, dedicated network that is connected to the public Internet in only a few places (e.g., DoD applications). The ultimate purpose of a network service is to provide access to assets (usually information or money). For example, online banking services enable the remote management and transfer of funds, while commercial web sites offer information services that may be general (e.g., Yahoo or Google) or specific (e.g. CNN.com or Weather.com).

The adaptability of this architecture has allowed the Internet to surpass its originally intended design, and its role as a critical infrastructure has emerged with the increasing functionality and convenience of network services. However, an implicit assumption underlying the network's construction is that of *trusted end hosts* so that ensuring security and its many aspects (e.g., authentication, authorization, repudiation) is not part of the design. Since the highly structured nature of the fundamental network architecture is not easily changed (e.g. consider the recent difficulty in deploying IPv6), recent efforts to retrofit security have been hampered by the rapidity with which new challenges to security have emerged.

By mapping the dependencies between technology components and layers, this framework highlights the propagation of vulnerabilities through the overall infrastructure. For example, in order for computers at the network edge to interoperate across the network, they must implement the same fundamental protocols. Each implementation of a particular protocol is a potential source of flaws that could be exploited during an accident, failure, or attack. The client-server architecture of most systems today implies that any network service has at least two classes of potential targets. In the current environment, most large-scale attacks are directed at the Windows operating system, in large part because Microsoft products are run on more than 90% of all computers at the network edge. Although Microsoft is an attractive target for this reason alone, this framework shows that other targets could potentially result in greater consequences. For example, an attack on the Cisco IOS that disables routers could disrupt functionality within the network core, thereby affecting all computers at the network edge. Other incidents (e.g. IP spoofing, DNS attacks, BGP misconfigurations, virus/worm infection, accidental cuts in fiber cables, hacker penetration) can also be analyzed in the context of this framework.

As a result of the many ways in which this architecture can be compromised, the general consensus seems to be that the current Internet is inadequate as a critical infrastructure. Why this is the case and, more importantly, what to do about it remain open questions. Much effort to date has been centered on how to secure the current infrastructure, with specific emphasis on the types of new technologies that are required to do so. Others have recently started to rethink the fundamental network design [4] by asking "If one could start over and build an information infrastructure from scratch, how would one do it?" And yet, both of these primarily technological approaches may be overlooking an essential point: that security problems arise at the human interface with technology. The lack of security in the Internet today may be due in large part to economic, legal, and social reasons with technological challenges accounting for only a small portion of the problem.

3. Stakeholders and their Incentives

Mapping the roles that individual corporations, standards bodies, consumer groups, and government agencies play in the infrastructure tends to be quite complicated, since individual players often have multiple roles. For example, Amazon.com is a provider of a network service, an owner and operator of a

significant internal network infrastructure, a steward of personal information for its customers, and a consumer itself of network services. However, a detailed articulation of the various incentives motivating different stakeholders usually is possible in the context of specific portions of the overall infrastructure.

In the network core, the primary stakeholders are the owners and operators of the network infrastructure, namely the Internet Service Providers (ISPs). They are responsible for the procurement and the provisioning of physical hardware, as well as configuration and maintenance of any operating systems. They interact closely with another group of stakeholders: the vendors of networking equipment (e.g., Cisco, Juniper, Nortel) who are responsible for the design, manufacture, and distribution of physical devices and associated operating systems that implement fundamental networking protocols. Finally, standards organizations, such as the Internet Engineering Taskforce (IETF), are responsible for the specification of fundamental protocols that are implemented by the network equipment vendors and used by the ISPs.

At the network edge, the primary stakeholders are the consumers of network services and the stewards of information assets, including corporations, government agencies, non-profit organizations, individual users, and others. Unlike the core network infrastructure vendors, the vendors of network edge computer hardware (e.g., Dell) are typically different from the vendors of network edge operating systems (e.g., Microsoft, RedHat). Exceptions to this rule include Apple, IBM, Sun Microsystems, Hewlett Packard, and others who produce their own variants of the Unix operating system to run on their hardware. To make use of the core network infrastructure, the network edge must implement the same fundamental protocols defined by the standards organizations, e.g. the IETF, and used in the network core. Thus, standards organizations have a role that spans the network infrastructure layer.

Given this framework for determining stakeholders and component dependence, we can now view and analyze vulnerabilities and their attendant exploits from a perspective based on consequences, incentives, and precautions. Furthermore, policy initiatives can be crafted to alter the environment and to correct any misalignment of incentives in the market. To illustrate the power of this approach, we examine several important issues from the current policy debate over how to promote and ensure a secure cyber infrastructure.

The role and responsibility of (software) vendors

The original design of the Internet (i.e., its protocols and deployment) was based on the premise of open access amongst participants who already shared a high level of interpersonal trust. Retrofitting the Internet to facilitate common security requirements, such as authentication, authorization, and non-repudiation, presents a significant technical challenge. Additionally, market forces today seem to favor rapid time to market and feature development over security. Indeed, the current maxim among software companies appears to be “ship now, patch later”—a policy that has produced a software infrastructure riddled with security holes.

The lack of security in most software products should not be surprising. Since the use of best practices for the development of secure software is costly in terms of time and resources, security “features” become a natural victim of the vendor's need to minimize costs. The exceptions to this rule are security-focused software products, such as virus protection software, firewalls, etc., where the functionality desired by users is security itself. Over the last several years, the market for these products has grown dramatically. Yet, the fact that these products remain a part of a specialized market demonstrates that most consumers remain unwilling to bear the cost of incorporating security in software.

Most Internet stakeholders agree that software vendors must do more to reduce the security vulnerabilities of their products. The question for policy makers is how to affect the mechanisms and motivation for such a change. One suggestion is to make software vendors liable for damages incurred as a result of insecure software. Currently, vendors have avoided general liability for the use or misuse of their products with their *end-user license agreements (EULAs)*. Because the product use is contingent upon accepting the agreement and is strictly voluntary, vendors are able to shield themselves from liability. However, the problem with this line of reasoning is that the market for software is far from perfect and the incentives of individual users may preclude the possibility of rejecting a EULA. In cases where a dominant market product is incompatible with its competitors, no viable alternative may exist and the consumer may have no choice but to accept the EULA. Not surprisingly, yet another ongoing debate has spawned around the question of whether a computing monoculture poses a significant threat to national security because it creates a single point of failure for the infrastructure as a whole [8][10].

At present, when a vendor discovers a software security issue in one of its released products, it addresses the problem by releasing a security patch to fix the flaw. The increasing complexity of software products has fueled an incredible rise in the number of security vulnerabilities needing patches. The sheer volume of patches being released every month is straining the abilities of even the most diligent end-users to keep pace. Due to the complexity and inconvenience of installing these numerous patches, many systems remain vulnerable until an attack occurs. Furthermore, as noted in a recent *Economist* article, the announcement of a patch for a security flaw is sometimes an invitation to hackers to exploit the flaw before the patch becomes widely applied [5]. Every widespread security incident in 2003 exploited a vulnerability for which a security patch had already been developed by the time of the incident, meaning that these incidents were, in a strict sense, avoidable, assuming the end-users kept pace with the patch releases. Consider as an example the Sapphire/Slammer Worm, which targeted computers running Microsoft SQL Server in January 2003 and attacked more than 90% of the Internet in under ten minutes [15]. This worm exploited a software flaw that had been discovered and for which a patch had been developed more than six months earlier, yet more than 100,000 unpatched hosts remained and became infected, including several machines at Microsoft itself [11][12]. If appropriate incentives do not exist for Microsoft to patch its flaws on its own computers, what chance is there that the rest of the general Internet-using public will be any different?

The open source movement presents a rather unique challenge to the analysis of stakeholders and incentives. Since open source software is built in collaboration by many individual developers, there is no single vendor who has responsibility for it. In practice, users of open source software must take responsibility for the correct installation and operation of its code. If a bug is discovered, the user must either fix the bug herself or look to the open source community for a solution. If the risks or burden of running open source become too great, then users may turn away from its products. As the competitive landscape shifts, the open source movement will be challenged to demonstrate that it can provide trustworthy software at or above the standard required of proprietary software vendors.

The role and responsibility of ISPs

Internet Service Providers (ISPs) are the owners and operators of the current public network infrastructure. ISPs provide two basic types of service: “retail” access and “commercial” network transport. In the current landscape, national providers, such as America Online (AOL) and Microsoft Network (MSN) dominate the market for retail services, though some local access providers can still be found, particularly in the market for broadband services. Providers who maintain their own network backbone, such as Sprint and Level3, provide commercial transport services to corporations as well as other ISPs.

To become an ISP, a company must make considerable investments to procure, install, and maintain the facilities and equipment necessary to provide network services. In spite of this significant capital requirement, competition among ISPs has been sufficient to keep pricing for such services relatively low. As a result, ISPs are challenged with balancing infrastructure expenditures with limited revenues. The financial failure of large providers, such as WorldCom and Qwest, demonstrates the treacherous economic waters many ISPs must navigate. To keep operating costs as low as possible, vendors whose products may offer low cost functionality at the expense of security are likely to be preferred.

ISPs have a critical role to play in the promotion and achievement of a secure cyber infrastructure. They have direct relationships with vast tracts of the Internet-using population and as a result, some leverage over their security practices. At the network edge, they are uniquely positioned as the gatekeepers of the Internet to exert great control over the traffic allowed to enter and to exit the information superhighway. ISPs wield tremendous power because they operate the network infrastructure both at the edge as well as at the core, and they therefore have the means and influence to enforce security standards across large portions of the infrastructure. Whether and how they should exert that power remain open questions. The traditional tradeoff for a public communications infrastructure is either to enjoy the content immunity of a "common carrier" while accepting regulation with respect to "carrier grade service", or to escape the regulation of carrier grade service but accept responsibility for transmitted content. ISPs currently have responsibility for neither content nor carrier grade service, simultaneously arguing that, like the telephone company, they are not responsible for the content of communications traveling through their wires and that, unlike the telephone, Internet service is not so critical to society to warrant carrier grade service regulation. This position, however, is starting to change. Distributed denial of service attacks against important customers, the marriage of spam and virus propagation, lawsuits over the distribution of defamatory material, the Recording Industry Association of America's pending lawsuits to block copyright-violating music distribution web sites, and parental demands for adult content filters are thrusting ISPs into the reluctant role of policing traffic.

The role and responsibility of consumers

To date, consumers have sought the greatest functionality at the lowest possible price. Indeed, the advent of the open source movement has engendered its own subculture of users who expect services to be free. Thus, consumers have been reluctant to pay for features that do not provide significant and measurable benefit to them. Since security features have not, generally, met this standard, consumers have been unlikely to adopt them, and even less likely to pay for them. This attitude, however, is beginning to change, due in part to efforts by the government and other security-minded organizations to evangelize about the potential risks of running insecure software and also due to the validation of those warnings by an increase in the incident rate of network worms, viruses, and Trojan horses. In addition, recent developments in the legal landscape suggest that the courts may make users increasingly responsible for the software that they operate [3].

4. A New Premise for Cybersecurity Policy

The vulnerabilities and issues outlined in the previous sections involve a complex array of technology, economic, and legal issues, which have thus far made a simple solution elusive. The perspective offered by the federal government in its approach since 1996 is that information deficit remains a key obstacle to addressing the challenges of infrastructure vulnerability. For example, the ongoing government initiatives (outlined in Section 2) imply, in essence, that the primary reasons software patches are not applied in a timely manner are one or more of the following.

- Users do not know that vulnerability exists.

- Users do not understand the potential dangers that arise from this vulnerability.
- Users do not have sufficient knowledge or encouragement to eliminate the vulnerability.

Yet, even this rationale does not explain why Microsoft would fail to patch its own systems and, as a result, suffer at the hand of the Sapphire/Slammer worm.

Again, we believe that the fundamental problem behind the current infrastructure vulnerability is that economic incentives for both software vendors and software users are not aligned to compel the vigilant development, deployment, and application of software patches. Accordingly, one approach to correcting this misalignment might be to assign explicit responsibility for the consequences resulting from the operation of insecure software. A few admittedly extreme examples might serve to illustrate the point. What if a company, such as Microsoft, were held financially liable for all damages suffered as a result of its customers' unpatched software? What if CIOs were held responsible for corporate losses resulting from unpatched software? What if ISPs were held responsible for damages caused by virus traffic that travels over their networks? What if individual users could be fined for contributing to the spread of a computer virus or worm? We do not necessarily advocate any of these measures, but if market forces are to be relied upon for infrastructure security, then carefully constructed changes to the current market structure will be needed.

We believe that effective policy for cybersecurity must directly address the economic incentives of the infrastructure stakeholders. By assigning specific responsibilities and liabilities, commensurate with stakeholders' interests and capabilities, government can instill in stakeholders sufficient motivation to secure the infrastructure without resorting to overbearing regulation or nationalization of assets. The self-interested behavior of each stakeholder can then be expected to yield a secure cyber infrastructure.

The Challenge of Measurability

The current inability of infrastructure participants to measure the quality of security in a standardized and repeatable manner prevents the easy assignment of responsibilities for cyber security. Without standard metrics and the means for measuring progress, improvements in infrastructure security cannot be credibly achieved, regardless of how thoroughly responsibility is assigned. In fact, the very mechanism by which responsibility is assigned would likely depend heavily upon an appropriate measurement of security.

Security cannot be measured directly in any strict sense. Good security means that an organization will not suffer the consequences of a security breach. Measuring the absence of future security incidents is tricky, especially when human factors are involved. There are two primary strategies for measuring or validating security.

1. Examine the results of security efforts, including red-teaming exercises, penetration testing, vulnerability scanning, and other means of probing defenses for weaknesses in security.
2. Examine the building blocks and processes of security efforts to infer the prevalence of vulnerabilities. Activities include auditing business processes and procedures for security policy compliance, assessing the quality of security in infrastructure components, and reviewing system development and administration processes for security best practices.

In the current environment, measurement of security is conducted by separate organizations that sporadically define, collect, and analyze technical metrics in isolation. These metrics often include the number of vulnerabilities found in network scans, known incidents reported, estimated losses from security events, security bug discovery rate in a new software application, intrusion detection system alerts, number of virus-infected e-mails intercepted, etc. Some organizations, such the Computer Security Institute, conduct computer security surveys and publish the results, but the voluntary nature of reporting and the lack of concise definitions open these survey reports to criticism. To date, standardized metrics

have not emerged. Several factors may be contributing to this failure, including a lack of consensus definitions for basic security terms, poor incentives for data collection and analysis and sharing, legal obstacles to collective action, and cultural bias within the information security community against quantification and measurement [7].

The need for metrics, however, is real and growing more acute. A number of industry consortia and trade groups are putting forward candidates for IT security metrics. TechNet, the American Security Consortium, and others are advocating new approaches to metrics. The hope is that formal benchmarks will soon emerge. The Department of Homeland Security in a recent Cybersecurity Summit, December 2-3, in Santa Clara, CA, put the industry on notice that solutions to these and other obstacles must be found soon, or the government will intervene. What shape that intervention might take is uncertain, but the threat alone is motivating many to begin addressing the problem of metrics.

Accountability for infrastructure security has not yet emerged from the laissez faire regulatory environment of today's Internet. The pace with which the market appears to be moving to address security gives little hope that clear lines of responsibility will be drawn without explicit government intervention. We are not advocating that government mandate specific solutions and compel owners, operators, and users of the Internet to employ them. Rather, we are suggesting that government policy could reshape the market to correct for apparent incentive failures and in doing so, leverage for infrastructure security the same technological innovation and market creativity that has made the Internet the tremendous success that it is today.

5. Conclusions and Future Work

In this article, we have argued that the fundamental misalignment of Internet stakeholders' economic incentives will hamper any government strategy based solely on voluntary information sharing and public-private partnership from effectively addressing the potential threats to national security posed by Internet vulnerability. In essence, we assert that a policy for cybersecurity based on market forces is not only appropriate but unavoidable, in the sense that stakeholders will always act in accordance with their economic incentives. However, we emphasize that such a policy will work only if the stakeholders are properly motivated. Recent history shows conclusively that such incentives do not currently exist. Thus, we believe that the government should focus its efforts on developing policy initiatives, using regulation, taxation, subsidies, legal liability, and other methods of influence as necessary to correct the current misalignment of incentives among Internet stakeholders.

This development of a framework based on economic incentives reveals a number of important issues that represent significant research topics in their own right. Debates on the roles and responsibilities for software vendors, ISPs, and the individuals and organizations that use software are ongoing. The issue of the threat posed by a technology monoculture (whether it be Microsoft, Cisco, or some other) seems far from resolved. And as the network infrastructure becomes more integral to the functioning of society, the threat posed by software worms also becomes more significant.

Successful development of a secure cyber infrastructure will require careful consideration of the evolving technical, economic, and policy issues outlined above. Current national policy could benefit immediately from this approach by initiating a dialogue with the aforementioned stakeholders about the capabilities, roles, and responsibilities that each has within the infrastructure. Several public-private partnerships have emerged in the last few years, and those organizations would provide ideal venues for discussing these issues. However, in collaborating toward possible solutions, the government should recognize that it must do more than adopt the desires of industry, since the economic incentives of corporations are not necessarily aligned with the public good.

In the meantime, growing national dependence on the Internet and associated information infrastructure increases the risk to the nation. In the absence of change, a "cyber 9/11" may be required to move individuals, corporations, and the government into action. Our ultimate objective in advocating this research agenda is to preempt the need for such a wake up call.

6. Acknowledgements

The ideas here have been influenced greatly by interaction and support from a number of individuals including Drs. William J. Perry, Michael May, and David Elliott. An early version of parts of this work was conducted in collaboration with Ekaterina Drozdova. We thank Deborah Gordon for her kind assistance throughout our efforts as part of the Preventive Defense Project. Finally, we would like to acknowledge many other colleagues and experts in the broader CISAC community, including Seymour Goodman, Stephen Lukasik, and the participants of the Seminars on Critical Infrastructure Vulnerability and Security at CISAC, who provided helpful comments and suggestions as we developed this report.

References

[1] R. Anderson, "Why Information Security is Hard – An Economic Perspective," University of Cambridge Computer Laboratory, 2001.

[2] Baskerville, R.: Information Systems Security Design Methods: Implications for Information Systems Development; ACM Computing Surveys; Volume 25, No. 4, December 1993; pp. 375-414.

[3] S. Berinato. "Courts Make Users Liable for Security Glitches," CIO Magazine. February 1, 2004.

[4] Carnegie Mellon Press Release. "Carnegie Mellon Leads Team Receiving $7.5 Million from NSF to Develop High Speed Telecommunications Network Reaching Every Home in America" September 27, 2003.

[5] *The Economist*. "Fighting the worms of mass destruction." November 27, 2003.

[6] Ernst & Young. *Global Information Security Survey 2004.* October 2004. Available electronically at http://www.ey.com.

[7] D. Geer, K. Soo Hoo, and A. Jaquith. "Information Security: Why the Future Belongs to the Quants," *IEEE Journal of Security and Privacy*, July/August 2003.

[8] D. Geer, C.P. Pfleeger, B. Schneier, J.S. Quarterman, P. Metzger, R. Bace, and P. Gutmann. *CyberInsecurity—The Cost of Monopoly*. Computer & Communications Industry Association. September 2003. Available electronically at http://www.ccianet.org/papers/cyberinsecurity.pdf.

[9] L. A. Gordon, M. P. Loeb, and W. L. Lucyshyn, "Economic Aspects of Controlling Capital Investments in Cyberspace Security for Critical Infrastructure Assets, " 2nd Annual Workshop on Economics and Information Security, University of Maryland, May 29-30, 2003.

[10] M. Landesman. "CyberInsecurity: Much Ado About Nothing" About.com. Available electronically at http://antivirus.about.com/cs/allabout/a/cyberinsecurity.htm.

[11] R. Lemos. "Worm Exposes Apathy, Microsoft Flaws" CNET News.com, January 26, 2003.

[12] R. Lemos. "Microsoft fails Slammer's security test" CNET News.com, January 27, 2003.

[13] McGhie, Lynda, "Software Patch Management – The New Frontier", SBQ – Secure Business Quarterly, Vol. Three- Issue Two, 2003. http://www.sbq.com/sbq/patch/sbq_patch_lmcghie.pdf

[14] McGraw, G. Software security. *IEEE Security & Privacy Magazine*, Vol. 2, Issue 2, March-April 2004.

[15] D. Moore, V. Paxson, S. Savage, C. Shannon, and S. Staniford. Inside the Slammer Worm. *IEEE Security & Privacy*, July-August 2003.

[16] National Academy of Sciences, "Why the Market for Security Has Not Worked Well," Chapter in *Computers at Risk: Safe Computing in the Information Age*, 1990.

[17] H. R. Varian, "System Reliability and Free Riding," 1st Annual Workshop on Economics and Information Security, University of California at Berkeley, May 16-17, 2001.

[18] W. Willinger and J. C. Doyle. Robustness and the Internet: Design and Evolution. In *Robust design: A Repertoire of Biological, Ecological, and Engineering Case Studies*, E. Jen, Editor, Oxford University Press (to appear).

Additional References on Cybersecurity Policy

[19] The White House. "Presidential Executive Order 13010—Critical Infrastructure Protection." July 1996. http://www.ciao.gov/resource/pccip/eo13010.pdf

[20] K. Soo Hoo, K. Malpass, K. Harrington, D. Elliott, S. Goodman. "Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda," CISAC Conference/Workshop Report, October 1997.

[21] President's Commission on Critical Infrastructure Protection. "Critical Foundations," Technical report, The White House, 1997. http://www.ciao.gov/resource/pccip/report_index.htm

[22] D. Alderson, D. D. Elliott, G. Grove, T. Holiday, S. J. Lukasik, and S. E. Goodman. "Workshop on Protecting and Assuring Critical National Infrastructure: Next Steps, February 26-27, 1998" Technical report, Center for International Security and Arms Control, Stanford University, 1998.

[23] The White House. "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." May 22, 1998.

[24] K. Soo Hoo, G. Grove, E. Drozdova, S. Lukasik, D. Elliott, and S. Goodman. "Workshop Report: Regional Interest Group on Information Security: Sharing Information and Exploring Collaborative Opportunities" CISAC Conference/Workshop Report, December 1998.

[25] The White House. "National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue." 2000.

[26] General Accounting Office. Report GAO-01-822, "Combating Terrorism: Selected Challenges and Related Recommendations." September 2001.

[27] The White House. "Executive Order 13228 - Establishing the Office of Homeland Security and the Homeland Security Council." October 8, 2001.

[28] The White House. "Executive Order 13231 - Critical Infrastructure Protection in the Information Age." October 16, 2001.

[29] Institute for Information Infrastructure Protection (I3P). "Cybersecurity Research and Development Agenda." January 2003. http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf

[30] The White House. The National Strategy to Secure Cyberspace. February 2003.

[31] National Security Telecommunications Advisory Committee, "2003 Research and Development Exchange," March 13-14, 2003. http://www.ncs.gov/NSTAC/2003RDXProceedingsCameraReady.pdf

[32] Department of Homeland Security Office of Inspector General. "Progress and Challenges in Securing the Nation's Cyberspace." Office of Information Technology Report OIG-04-29, July 2004.