Center for Technology Innovation at BROOKINGS

July 21, 2011

Reuters/Hyungwon Kang - Rear Admiral Mike Brown, deputy assistant secretary for Cyber Security and Communications, briefs the media on Cyber Storm III exercise at the National Cybersecurity & Communications Integration Center in Arlington Virginia.

Economic and Policy Frameworks for Cybersecurity Risks

Allan Friedman

ABSTRACT

Congress and the Obama administration have advanced dozens of proposals addressing cybersecurity. While many of these bills propose admirable policies, they often attempt to address a wide range of issues under a poorly matched set of frameworks.

This paper offers three observations built around a framework of risk management to help focus the discussion. First, we caution against conflating different threats simply because they all involve information technology. Crime, espionage and international conflict are very different threats, and grouping them together can lead to poorly framed solutions. Second, we argue that looking at cybersecurity from the perspective of economics can offer important insight into identifying important policy opportunities. Finally, we suggest a series of governance frameworks that can be used in a complementary fashion to address many of the issues discussed.

Allan A. Friedman is research director of the Center for Technology Innovation at Brookings. He is also a fellow in Governance Studies.

Introduction

A frequent refrain is that the Internet was not designed with security in mind. While this is true, it fails to capture the nature of the problem: risk is a part of information systems. It is not simply a matter of bolting on security components, or even building a new, trustworthy network to handle our key transactions. The fact is that the risk has been there all along, and there are no direct, technical solutions to addressing systematic risk. Risk is a natural side effect of complex systems. Security itself is a subcomponent of risk; the past few years have demonstrated that a country is just as likely to be knocked off the internet by a typo (Mills, 2009) or a scrap metal scavenger (Parfitt, 2011) as they are by an unfriendly neighbor.

One can draw an analogy to the state of the world at the publication of Rachel Carson's *Silent Spring*. Her book did not introduce the risks to a world dependent on heavy industry and toxic pesticides. The dangers were present, but increased awareness forced a decision of how to adapt as a society. What threats will we protect ourselves against, what will we tolerate for the sake of efficiency, and what risk will remain exposed simply because we cannot overcome the policy problems to fix it?

As of July, 2011, Congress was considering or about to consider 22 bills on cybersecurity, in addition to proposed legislation from the White House (CSIS, 2011). While many of these bills propose admirable policies, they still attempt to address a wide range of issues under a poorly matched set of frameworks. This paper offers three observations to help focus the discussion:

- First, we caution against conflating different threats simply because they all involve information technology. Crime, espionage and international conflict are very different threats, and grouping them together can lead to poorly framed solutions.

- Second, we argue that looking at cybersecurity from the perspective of an economist can offer important insight into identifying important policy opportunities.
- Finally, we suggest a series of governance frameworks that can be used in a complementary fashion to address many of the issues discussed. It is important to note that this essay does not attempt to address every challenge we face in addressing the risks in our information infrastructure, but rather offers an approach to thinking about that risk more generally.

Unpacking 'Cybersecurity'

One obstacle to building constructive cybersecurity policy is the perceived need to build a single, comprehensive set of policies to address the entire range of cybersecurity issues. The 2010 cover story in the Economist (2010), boldly titled "Cyberwar," covered issues ranging from credit card fraud, to industrial espionage, to international law and conflict, switching back and forth between topics. There is no governmental organization or academic discipline that can or should be able to address these areas substantially and simultaneously.

In support of their proposed legislation in the summer of 2011, three senators wrote an op-ed in the *Washington Post* and motivated their proposals with references to recent, high-profile attacks, including Citigroup, RSA, and the Stuxnet worm. (Lieberman, Collins, & Carper, 2011). Independent of the merits of the legislation, it is important to recognize just how different these three examples are. The Stuxnet worm was an incredibly sophisticated attempt to effect a kinetic disruption of a nation's defense program, incorporating novel attack strategies, previously unused vulnerabilities and stolen trusted signed keys from certificate authorities. Citigroup's attackers, by contrast, exploited weak security by guessing account numbers in order to steal credit card numbers, resulting in less than $3 million in losses (Albanesius, 2011). These attacks differ dramatically from the one against computer security company RSA, which was a well-planned multi-stage attack to apparently exfiltrate data and intellectual property from defense contractors.

These three areas, national security (including state-sponsored security-relevant intelligence gathering), industrial espionage, and cybercrime, all differ dramatically in terms of scale, stakeholders, timeframe and level of social importance. The scale of the national security threat has been amply explored in a number of books by noted experts in the national security field. It is hard to imagine a more serious threat than the disruption of the military's ability to defend the country, or an unknown foreign power disabling massive amounts of the nation's critical infrastructure. The scale of defense is similarly massive: the U.S. Department of Defense already has about 90,000 personnel dedicated to working on its networks (McMichael, 2010).

The specter of espionage also looms large. There are widespread reports of

regular attempts to monitor the communications of government officials. Many companies have come forward claiming to have been the victims of industrial espionage- some sophisticated actor has copied vast amounts of their most precious intellectual property and trade secrets. Department of Defense Deputy Secretary William J. Lynn calls intellectual espionage "the most significant cyberthreat faced by the United States" (Lynn, 2010). While copying data does not destroy its utility, exposing a firm's secrets can cripple its future competitiveness. When this happens at a national scale, it can wreak devastation and cripple an innovation-driven economy. Yet assessing its scope is quite hard, since many companies are reluctant to disclose an attack. Actual numbers are hard to come by. A report by the U.K. government estimates that U.K. businesses lose over £16 billion (Detica, 2011), greater than 1 percent of the value of the entire British economy in 2010. On the other hand, the report is "based on assumptions and informed judgments rather than specific examples of cyber crime, or from data of a classified or commercially-sensitive origin," so it is hard to determine how valid these numbers are. In general, companies have demonstrated great reluctance to come forward and disclose details of espionage, or even acknowledge it occurred.

It is also hard to assess the scale of cybercrime. The Chief Security Officer of AT&T testified that cybercrime yielded $1 trillion in revenue. This would put cybercrime on course to be close to 2 percent of the global economy, larger than the entire pharmaceutical industry. A common vector of extracting value is credit card fraud. Here, again, there is a conflict in the numbers. One estimate puts card fraud at $8.6 billion (Aite Group, 2009), while another suggests $37 billion (Javelin, 2011). These two estimates point us to either a fraud rate of 0.25 percent or 1.1 percent of the $3.34 trillion in credit card transactions in 2009 (Federal Reserve System, 2011). Even these numbers mislead, given how inefficient many cyber schemes are. One researcher discovered that it takes 350 million spam emails to convert just 28 sales (Kanich, 2008). Crime also has a limited impact, with incidence largely contained in sectors of value. Cybercrooks attack banks and bank-like services, as well as identity platforms, because "that's where the money is."

No one likes crime, and policies should be set to reduce the crime rate, but no one argues that we should aim for zero crime. Fraud has become a built-in expense in most business models, particularly in open infrastructures like identity and payment. Indeed, there is a trade-off between fraud reduction and enabling transactions such as e-commerce. The original diffusion of payment cards in the U.S. is due, in part, to consumer protection laws that allowed consumers to carry and use cards without bearing much of the risk of fraud.

Crime as a question of public interest poses a two-fold threat. First, it imposes a direct, marginal cost on the sectors attacked. This development might be seen as the cost of doing business, similar to shop-lifting: deserving of government attention, but not a huge priority. As fraud grows, though, it might approach a tipping point. That is, if attacks on a certain digital platform or application grow too large, components of the information infrastructure could be abandoned. The risk of critical failure of a major building block of the internet ecosystem demands

a larger public interest.

With respect to national security, what does a "tolerable" rate of compromise look like? Recent public statements by administration and elected officials, for example, indicate that any terrorist attacks would be considered a "loss" to terrorism. While not as extreme, the question of espionage is even harder to determine. It is hard to imagine how the compromise of a single firm's intellectual property would pose an existential threat to American interests (outside of a very narrow set of defense-related documents), but a national scale of data exfiltration could measurably impact the long term competitiveness of the country.

Each area demonstrates some exigency, and a need for public intervention, but who should bear the primary responsibility for solving the problem? National defense, of course, falls under the direct responsibility of the government. Absent specific obstacles requiring government intervention, it remains uncertain as to who bears the responsibility for the process and shoulders the costs.

Espionage should be of public interest to policymakers concerned with the long-term competitiveness of American industry, but it should be of even greater interest to the managers and shareholders of individual companies. It is hard to imagine some economic function that combines a set of security incidents regarding competitive data and intellectual property to have an impact on the macroeconomic level without also registering at the micro-, or firm-level. To put it another way, if intellectual property stolen from a company threatens the long-term interest of the country as a whole, surely it should impact the long-term interests of that company's shareholders even more so.

Finally, the time-frame varies across these three issues. Crime drags on the economy and erodes trust in the information infrastructure. This phenomenon is ongoing and, by most accounts, getting worse. Cybercrime is also distributed broadly across the economy, since it targets those components on which much of the digital economy rests: payments and identity. While it may not be an existential threat, it is certainly pressing.

By contrast, threats to the critical infrastructure from foreign powers do represent a serious threat to our national interest. Should it be considered an immediate threat to be addressed through direct remediation? If it is not time-sensitive, then gradually building security properties into an evolving infrastructure serves as a better use of resources than focusing on immediately altering basic architectural properties. What is the set of conditions under which we might be attacked, and is it easily reachable from the current state? National preparedness is a priority, but if a longer time-horizon offers a greater chance of a more robust and resilient network, building out a planned, coordinated infrastructure will ultimately lead to greater security.

Framing matters

Disambiguating the nature of cybersecurity risk is key to building frameworks for

policies to address the real issues we face. Framing the issue as a national security problem does have some advantages, of course. National security solutions come with national security budgets. On the other hand, they also come with other baggage of the national security apparatus: large centralized bureaucracies, poor tradeoffs against economic benefits and civil liberties, and less consideration for the (much larger) civil side of cyberspace. Moreover, cyberspace is not an American territory, and we will require the cooperation and engagement of our allies and the broader international community to establish norms of acceptable behavior and jurisdictional authority. Other nations would be less likely to follow our lead if initiatives are framed as a question of American national security.

The calls to impose "law and order" on a wild west state-of-nature are also misguided. This implies that we might expect to achieve some direct state of normalization by fiat that resembles the pre-IT status quo. All revolutionary technologies go through a wild west phase while upsetting the status quo before a new equilibrium arises (Spar, 2002).

An economic framework will allow us to navigate the comparison of values between different approaches of mitigating risk. It can also help evaluate potential tradeoffs against the efficiencies of an insecure but flexible system, the benefits of risk reduction, and the costs of extending out the frontier to maintain both efficiency and security.

Cybersecurity as an Economic Problem

Cyberspace may be a new domain, but it is composed of systems, networks, and the protocols and standards that allow data to flow efficiently and meaningfully. Each of these systems and networks is ultimately under the control of a set of actors who choose to take specific actions regarding the security of the network. Similarly, the agreed-upon standards that run the network, from the IP protocol up through the mechanisms by which banks settle accounts in a credit card network, are the outcome of processes with stakeholders and influencers. These stakeholders, too, can choose to take specific actions. The economic approach to information security focuses on the incentives of these actors, and whether these incentives align with a socially optimal level of security. This security exists to counter bad actors, who have their own incentives. This section explores the incentives of attackers and defenders, and explains some distortions in the market for security that inhibit investment and behavior to reduce risk.

The attacker's incentives

During the first major wave of rapidly spreading malware, observers marveled at the damage done by internet worms such as ILOVEYOU, Code Red, and Blaster, as they flooded networks with copies of themselves. Observers also noted the fact that many of these worms did remarkably little damage to the host machine, they

simply spread. The creators were apparently not seeking any noteworthy gain beyond introducing something large and destructive into the internet ecosystem. Today, however, most attackers seek to gain something. Whether it is to destroy a system, obtain valuable intellectual property and data, or old fashioned profit, one can model today's cyberthreat as an actor seeking some goal.

The natural question, then, is what that goal is, and how important is the realization of it? If we can understand how much the cyber-adversary would pay in time, effort, acquired expertise, and expenditure, we can better understand an approach to defense.

In the national security context, the obvious goal is the disruption of systems. As discussed above, much has been written on the myriad ways a well-equipped and well-informed attacker could inflict grievous harm on any society dependent on information technology. National security, of course, is a high priority for any country, and there is every reason to expect a large willingness to pay for offensive capacity.

One can expect a similar approach to intellectual property, although here one might make some assumptions about the rationality of the attacker. The intellectual property has some value to the attacker, and hence, the budget would be a function of this value. We can even begin to put upper bounds on the expenditures of cyber exfiltration costs, since a determined adversary could obtain company secrets through other means, such as bribing an insider.

In both the national security case and the espionage case, one must assume a reasonably large budget of the attacker. This includes a key component: the intelligence budget. This includes the ability to value and even stolen data, or the expertise to know which systems to target. The attacker must have considerable knowledge of what he is trying to do, and how to execute it well, particularly if he wishes to minimize the risk of detection.

Incentives in cybercrime

There is a greater understanding of the economics of crime, particularly when one assumes financial motive. What is noteworthy about much of cybercrime is the small ratio of attacker's profit to damage. In one recent case, the United States Secret Service apprehended an individual found in possession of over 300,000 credit card accounts, which have been linked to some $36 million in fraud. Yet the best estimates in the criminal filing claim that "In all, the defendant personally received over $100,000 from his credit card fraud scheme" (United States vs. Hackett, 2011). While this is hardly a pittance, this is not an astronomical sum. Estimates vary on the value of credit card information on the black market, but the low end is almost always less than one dollar for a usable credit card number and expiration date, while the upper estimates seldom rise above a few tens of dollars (e.g. Moore, 2009; Symantec, 2011; Panda Security, 2011).

The low returns to those who steal account information have roots on both the

supply-side and the demand-side. Ironically, the large numbers of credit card account information stolen drives down prices in a competitive market. The demand-side of this market must, in turn, find some mechanism of extracting value from these stolen account credentials without alerting active fraud detection mechanisms or compromising their own identity. A complex ecosystem has emerged to launder money through networks of handlers and mules. Much of this requires at least some manual intervention, raising the scaling costs.

Can criminals be deterred? Laws have been passed, with a renewed attention on inter-agency and international cooperation. Recent cases have demonstrated that law enforcement can achieve a non-trivial level of success in investigating and pursuing attackers. However, the jurisdictional issues and anonymity afforded by internet technology can impede investigations, and give attackers a sense of immunity to continue attacks. Moreover, it is important to remember that few law enforcement regimes successfully deter all crime. The international nature, and fluid nature of many online crimes make it difficult to engage in enforcement models specifically designed to deter crime, such as those described by Kleiman and Kilmer (2009). As the stakes rise to espionage or international conflict, the incentives to invest in clandestine activities that preclude attribution become greater. Disincentivizing attacks through enforcement and deterrence shows little promise.

We do, however, have one data point in favor of the efficacy of international law enforcement cooperation. Wang and Kim (2009) found that cyber-attacks originating from countries that have recently joined the Council of Europe Convention on Cybercrime fall between 15 percent and 25 percent. While this reduction could be explained by direct cooperation between signatory states, it is also possible that joining the treaty is indicative of a broader effort to take cybercrime more seriously.

Modeling attack and defense

Any model of even slightly sophisticated attackers must include a feedback mechanism where attackers are expected to adapt to defenses. Real-world evidence supports this. Phishing gangs switched from using domains registered in Hong Kong (.hk) to domains registered in China (.cn) as the Hong Kong Authorities became more proficient in shutting them down quickly (Moore and Clayton, 2007). Similarly, Day, Palmen, and Greenstadt (2008) show that websites hosting malware shift to more lax hosting providers as enforcement incentives are brought to bear. There is even evidence that state-sponsored espionage is adaptive. As government agencies step up their information security practices, American scholars and academics have come under attack from those seeking access to their emails and personal files.

Understanding the attacker can aid in better understanding defense. Bohme and Moore (2009) begin with an assumption that the attacker will begin by trying to compromise the weakest link in the defenses, although they do not expect the

defender to know which component is the weak link. Following from these assumptions, they show that under certain circumstances, a rational defender would use the attacker to identify the important components in her system to strengthen and reinforce. In a dynamic game, the defender can continually raise the cost to the attacker while minimizing her investment in security.

Investment in security

On the defensive side, we must begin with the assumption that organizations can invest resources and effort to gain some benefit of security. Absent this assumption, the game is already over, and we can only focus on damage control. Below, we explore why actors might not be properly incentivized to invest in security, but first we must understand what security investment looks like, and how to think about the optimal level.

We can draw a distinction between two approaches to investing in security. In the first case, firms respond to existing threats, but do not proactively seek to address their exposed risk. This reactive posture is quite common: companies only invest in data loss prevention systems, for example, after they have lost data, or have reason to believe they may be at serious risk. They do not internalize the risk. In this case, investment will often only occur after harm has been done, and or in the face of future projected harm, such as the risks of lawsuits, or to improve a reputation.

Grossklags, Christin, and Chuang (2008) argue that this approach can be rational and even socially optimal. They frame it as a question of self-insurance, and show that it is sometimes advantageous. Returning to the question of data loss, there is evidence that suffering a breach has a small but significant impact on a company's share price (Acquisti, Friedman, and Telang, 2006). Yet this risk might be smaller than a systematic attempt to prevent potential breaches. The challenge here is that covering one's expected expenses of a security incident through self-insurance does not address any negative externalities that might arise. Investing in protection, on the other hand, reduces the overall likelihood of an incident, and thus can be viewed as a public good.

In this alternate model, firms or agencies can seek out particular security features. This is more common in industries that are regulated, where security features are mandated by law. In this case, security investment is legal compliance. Rowe and Galleher (2006) neatly frame the contrasts between prophylactic investment and responsive investment as two complementary investment functions. The reactive approach involves a decision to throw some amount of money to fix a problem: maximizing the security gained for a given budget constraint. The proactive security paradigm seeks to meet a specific security goal: minimizing cost subject to a specified security goal.

The impetus to invest more in security depends on the context, of course. In general, it can be internal, from a security-focused corporate culture or leader, to

the needs of businesses (such as Amazon building a network resistant to Denial-of-service attacks), or in reaction to past breaches of security. Alternatively, the motivation could come from external regulations, or client demand.

Vendors are not insensitive to demand for security, but that demand is often tempered by clients who seek other features and lower prices, which can come at the expense of security. In the software, hardware and IT services markets, offering new features and being the first to the market is key. A first-mover advantage can translate to greater sales, not just for a given generation, but future sales and support costs through technical lock-in. Adding security features and engaging in rigorous pre-release testing adds time, complexity and cost to the vendor. As such, vendors often invest in security through consistent maintenance via patches to newly discovered vulnerabilities. There has been a great deal of analysis on the optimal means of discovering and disclosing vulnerabilities. A market for vulnerabilities or "bug bounties" can increase the likelihood that the vendor will patch before an attacker will exploit a vulnerability, as long as the vendor patches in a safe and timely fashion. Since rapid patching has its own costs, a vendor may not rush to address the risk, thus exposing users to potential harm. Because of this, some advocates prompt public disclosure of vulnerabilities, while others maintain that information about vulnerabilities should not be disclosed until developers have had a reasonable opportunity to diagnose and offer fully tested patches, workarounds, or other corrective measures.

Market failures in cybersecurity

Given the high level of risk from the constant threat of attackers, why don't we see more investment in security? In an optimal world, the market would demand more security, and the builders and maintainers of systems to invest more. There are several reasons why one would not expect the market for security to function well. There are abundant negative externalities, poor information and predictable behavioral reasons why market actors may not be expected to invest in socially optimal levels of security.

To begin with, the very nature of networked technology offers some insights into the dynamics of cybersecurity markets. Information technology often yields its greatest benefits when everyone uses the same standards and platforms to maximize interconnectivity. Referred to as the "network effect," this phenomenon predicts that the value of a particular technology increases as the number of users increases (See Economides, 2007 for a survey of the network effect applied to IT). While this is usually framed as a positive externality, since each adopter adds value to others, there are negative components. First, the network effect predicts the rise of dominant systems. As fewer systems and networks become integral to the infrastructure, it makes them more valuable to an attacker. Geer draws the parallel to the ecological risks of monoculture (Geer, 2003). For example, if a Facebook account now is a major source of interpersonal communication and allows comments on other websites and, a compromised account can be used for

targeted phishing attacks and comment spam.

Many dominant products, including operating systems and social networks, are built to support a platform for other products. Other firms can provide innovative, complementary goods and services to enhance the value of these platforms. The original product designer has an incentive to make it as easy to develop complementary products. Imposing security requirements or building security into the platform from the beginning can serve as an impediment to the developers of these complementary products.

Finally, the network effect can amplify the barriers of entry for newer, more secure products, since switching costs include the forgone value of the old network. Even adding new security components can be difficult if it requires individual decisions. Many security innovations, such as DNSSEC, yield their benefits to the entire network. There is little incentive to be the early adopter, since network security products often do not improve overall security until other users adopt them. Indeed, products that are not subject to network externalities and offer benefits to the early adopters, such as SSH and IPsec, are more likely to succeed and diffuse quickly (Ozment and Schechter, 2006).

In general, if someone is responsible for protecting the system while someone else bears the cost of failure, then we might expect to see more failures. Economists refer to incidents when the social harms of a given action differ from the private costs of the transaction as "externalities."Pollution is a commonly used example of a negative externality, since the actions of the producer affect others in a way not reflected in the price. When individuals allow their machines to be captured by botnets that can be part of malicious activity against a third party, they are not internalizing the harms of failing to protect themselves. Unpatched vulnerabilities could be seen as a negative externality. So too are data breaches that harm the data subjects more than the breached party.

Externalities can arise from the expectations of others. Schelling cites the perverse incentives for helmets in hockey as an example where competition prevents socially optimal behavior (Schelling, 2006). He noted that while no player would voluntarily choose to wear a helmet, believing it imposed a slight disadvantage, most players were in favor of everyone wearing a helmet. Similarly, even though few market players would choose to invest in security at the expense of their competitive edge, it is quite possible that everyone would be better off with higher-levels of investment.

Finally, the market for security is fraught with information asymmetries that prevent optimal decision-making. Anderson (2001) helped launch the field of economics of information security by observing that the market for security products paralleled Ackerloff's (1970) market for lemons, or bad used-cars. Buyers are unwilling to pay for what they cannot measure. Producers are therefore unwilling to invest in producing security, but will still assert the security of their products. Like an untrustworthy used car market, bad security products will drive out good ones. Standards have emerged to certify that products do indeed meet specific security requirements. To be certified, the dominant practice is for the

vendor to bear the costs of evaluating the product. This can introduce perverse incentives, where the vendor will seek out evaluation firms with whom it can negotiate "sweetheart deals". (NAP, 2007)

Even in good faith, it is very difficult to measure the effectiveness of a defensive measure. And when they can be adequately and simply verified, the product will, more often than not, close one vector of attack without precluding threat via other vectors. As such, a defender would only rationally expend some fraction of the value of a loss for a narrow defense, since risk still remains.

While different aspects of cybersecurity involve a wide range of incentives and economic forces, there is ample evidence for a market failure in security investment. What policies can use these same economic forces to promote better social outcomes?

Frameworks for Governance

One approach to understanding governance issues for cybersecurity is to look at the incidence of responsibilities distributed between private actors and the government. At one extreme, the government can pro-actively establish some baseline of security that it forces sets of actors to adopt through regulation. With less intervention, the government can actively dictate the incentives of private actors by establishing some model for liability. Alternatively, the government can empower better endogenous market forces by creating standards, promoting best practices and funding research and development. The least interventionist approach would leave the government trying to influence the market for security by leveraging its purchasing power to drive market behavior from their clients and contractors in the hope that this will propagate out.

As above, the governance models depend on the characteristics of the cyber-risks. Different problems will rely on different approaches to public policy. Addressing the simple security risks requires some set of incentives, either pro-active or reactive. Thinking about national security issues demands modeling the world as a set of reachable states, where decisions must only be made in light of prior events. Addressing espionage calls into question the trade-offs of securing systems, and relies on the role of transparency. A response to cyber crime must build on the principles of least-cost avoidance, and aligning the harms of fraud with the potential to address it.

Motivating basic security

The first step is to understand the lack of fairly straightforward security processes. There are abundant low-hanging fruit in the world of insecurities. Recent news of the attacks on webservers by quasi-anarchist “hacktivist” groups raised eyebrows as the targets included a contractor for several defense and intelligence agencies. The responsible party claims to have gained access to IRC Federal’s systems

through a SQL injection attack, and gained access to further data because of unencrypted passwords (Bright, 2011). SQL injection attacks are a well-known method of trying to gain access to servers running databases, and solutions are fairly straightforward. One security researcher writes, "It's somewhat shameful that there are so many successful SQL Injection attacks occurring, because it is EXTREMELY simple to avoid SQL Injection vulnerabilities" (OWASP, 2011). Furthermore, most basic guide to system administration includes lessons on the treatment of account information, including encrypted and salted passwords.

There are many other examples of easy fixes that online actors can take. One recent study found that attackers were using search engines to find outdated and unpatched versions of web services software to attack (Moore and Clayton, 2011). Popular sites such as Facebook and Twitter allow transmission of personal information and critical credentials without encryption by default, enabling users sharing an open wireless network to hijack their accounts (Butler, 2010). Adopting these small security measures is not technically difficult, or even terribly complex. It will, however, require spending money. What can motivate these investments?

Compliance vs. deterrence

There are two basic approaches to governing most private sector security practices in the United States. Companies can either bear the responsibility for complying with established security standards, or decide to invest a specific amount in some measures to avoid punishment following a security incident. The former focuses on establishing some set of security processes and practices, often with formal specific obligations. The latter is focused on rationally avoiding adverse outcomes in uncertain conditions. The two approaches can be complementary when applied to something like closing elementary security holes, but there are potential conflicts between the two approaches.

Industry-specific regulations can come from the government, with authority delegated from Congress to administrative agencies. Federal legislation requires the development of standards for information security practices, and delegates power to establish, update and enforce these standards to regulatory bodies. These agencies seek input from industry through an open rulemaking process. Examples in this space include the standards found in HIPAA's Privacy Rule and GLBA's Privacy and Security rules. Standards can also be driven by the private sector through industry associations and contracts. The Payment Card Industry's Data Security Standard, for example, dictates a set of practices and protections needed for organizations that handle payment card data.

While compliance mechanisms are often seen as heavy-handed regulation, they seek to enforce a minimum standard of security. In theory, standards target risk and thus reduce the probability of a harmful event. One common complaint about a compliance model is that the organizational incentives shift from reducing the possibility of a security incident to reducing the possibility of sanction from non-compliance. The open question is under what conditions does the focus on

compliance overlap with appropriate risk reduction.

Another approach is to promote good behavior through the fear of suffering some adverse consequence. This can take the form of reputation mechanisms through transparency and disclosure. Currently, 46 states and the District of Columbia have data breach notification laws, which require firms to report incidents that compromise personal data, and notify the data subjects. There have been several proposals to create a national data breach law. These laws are built on the assumption that reporting an incident will have some adverse affect, and would therefore want to report fewer incidents. The adverse harms could come from damage to a firm's reputation, or the monetary costs of notification and fraud prevention services. Evidence suggests that firms suffer small but significant losses to their stock price (Acquisti, Friedman and Telang, 2006), although some industry observers put the cost much higher. Transparency may not have a constant effect over time, as more reported incidents could reduce the perceived severity of any given incident. Alternatively, in the right environment, falling prey to a basic attack that already hit others earlier could signal a failure to learn, and hint at broader dereliction of duty.

A stronger model of deterrence is to make the punishment explicit through a liability model. Firms that are found negligent in their duties to build and maintain secure systems are punished following an incident. With defined damages, this can force companies to internalize the full cost of an attack. Larger damages can compensate for the uncertainty inherent in an unmanaged risk. Firms can be liable for direct harms to individuals (in the case of data breaches or fraud) or just the costs of helping others recover from the effects of an attack (in the case of a technology vendor patching or updating the product).

Liability introduces its own risks. Too little, and it has no effect. But if the responsibilities and expectations for acceptable, non-negligent behavior are too broad, liability can raise costs, serve as a barrier of entry for competition and stifle innovation. Threats of lawsuits can scare off entrepreneurs and venture capitalists, increasing the overhead of small companies and products built on open-source software. Yet the same threats create strong incentives to engineer security into systems at the earliest development stage across the sector, rather than seeking hastily address risk after deployment. Recent theoretical work asserts that the benefits of a liability model vary greatly depending on the economics of the market for software environment, as well as empirical questions about the threat faced (August and Tunca, 2011).

Insurance can address the risks large damages in a liability regime. There is already a growing market to cover the harms that a firm suffers following a cyber-attack, particularly in medium-sized businesses that lack the capacity to self-insure. As the insurer now bears much of the risk of bad security, an underwriter can compel the covered entity to adopt good security practices that minimize risk.

Deterrence and compliance have some common and even convergent features. A negligence model for insurance would require an understanding of the appropriate standard of care. This begins to resemble a set of guidelines that

demand compliance. Moreover, some deterrent efforts can take on a compliance feel at the expense of the focus on risk reduction. Data breach laws focus on all disclosed data, from intentional attacks to lost laptops. If misplacing a laptop is more likely in a large organization, then security resources are best spent encrypting and tracking data even if the actual harms of lost media are quite unlikely. Meanwhile, there are fewer resources to be spent addressing other risks that could potentially do more damage, such as an intentional targeted attack.

Unfortunately, deterrence and compliance do not always play well together, particularly when it comes to information-sharing. Under a compliance regime, organizations not only have an incentive to advertise their compliance, but they have incentives to share details about when the security standards were effective or ineffective. If a compliant firm suffers a security incident, it has an incentive to share details about the attack with others to demonstrate that it was compliant and therefore the firm is not to blame for the successful attack. However, when a firm can be punished for a successful attack, sharing information can harm the company by exposing it to greater claims of negligence. This can lead to an unwillingness to share threat information across organizations. Furthermore, if avoiding an incident is seen as a competitive good, then disclosing efficient means for effective security can be seen to only help one's competitors.

Neither a deterrence framework nor a compliance framework is perfect for driving a widespread investment for good security. Nonetheless, some balance of these two forces will be necessary in the current climate of market failure. Other specific areas of risk require different mechanisms.

National security and deterrence

When discussing the national security risks, many fall back on the established governance principles of deterrence that grew out of economic game theory. Indeed, many in the field bemoan the lack of an effective deterrence strategy. Since the technology offers a low barrier of entry and makes attribution all but impossible against a determined adversary, the approaches used in our nuclear deterrent strategy, for example, fall far short.

One approach is to re-engineer the Internet to offer some mechanism of control. This is usually framed in terms of enabling strong authentication to allow for attribution. Attribution, the theory goes, leads to effective deterrence, since an attack can be met with response. Several prominent national security experts with extensive experience inside the intelligence community have called for re-engineering the entire Internet to make it more secure. These proposals, coming from the likes of former NSA chiefs Michael Hayden (Pruitt, 2010) and Michael McConnell (McConnell, 2010), aim halt the most serious threats, but at a substantial cost. Proposals like this date back to at least the beginning of the century (Pruitt, 2001). They are deeply flawed for several reasons. Leaving aside the civil liberty and human rights questions and issues of feasibility and cost, such a dramatic step would make little strategic sense. To work, proposed system must

be not just resilient against an attack, but actually make subversion impossible—or at least outside the price range of potential attackers. While this may limit some smaller potential adversaries, international conflicts tend to come with pretty large price tags. Moreover, any technical guarantee of robust authentication at the network level cannot defend against subversion of the end points. This includes not only vulnerable computer systems, but also vulnerable people who can be deceived, bought or coerced into malicious activities.

The architecture of the internet notwithstanding, deterrence theory suggests the importance of a declared policy about responses to cyber incidents at the national security level. A recent claim that the U.S. might respond in a kinetic fashion to a cyber attack prompted great controversy (Gorman and Barnes, 2011). How could this model of aggression be good? Looking at this through a lens of deterrence theory does indeed suggest some risk of conflict escalation. However, the situation must be approached from the perspective of the optimal response. If a decision to respond to an attack must be made, the country has been the victim of an attack, and is considering range of potential responses. Why would we wish to artificially constrain this approach? Moreover, defense analysts understand the nature of kinetic responses and, most importantly, have a model for the worst-case scenario. A mistake with a bomb might blow up a school; this can be factored in to the risk calculations. Offensive cyber-operations, on the other hand, have a largely unknown error margin, and the dynamics of a poorly executed attack are quite hard to model in the nonlinear, networked world.

An alternate approach is to build the models by looking not at the explicit decision to attack, but at the relative incentives for countries' approach to cyberspace. We focus-model the trade-offs between building out offensive capacity and focusing on defending ourselves. One model found that there will always be an incentive for at least one party to behave aggressively, although the dynamics can be altered by looking at the decision not to invest in defensive capacity as a source of risk from other threat vectors, such as crime (Friedman, Moore and Procaccia, 2010). Embracing a risk-based approach to security can be a socially-optimal approach. Interestingly, the model also predicts better outcomes when the parties are not equally matched in technical capacity.

Espionage and transparency

Addressing espionage, a more subtle yet potentially dangerous threat, requires further policy shifts. Some of it is quite straightforward: the Department of Defense's recent strategy, launched with specific attention on espionage, maintains "Most vulnerabilities of and malicious acts against DoD systems can be addressed through good cyber hygiene". (DoD, 2011) This falls under the model of low hanging fruits discussed above. One might assume that this applies to attacks against the sensitive data of private sector firms as well. Indeed, while we lack information about many attacks against private actors, they often begin with a straightforward attempt, such as a targeted phishing email.

However, we must also assume that if information is valuable to the attacker, there will continue to be risks to critical data. An open question is whether any firm can simultaneously make effective use of data across a distributed information architecture, and effectively protect that data. Limiting access to data is key to preventing its release, yet the efficiency of large organizations often depends on widespread and flexible access to data. Any determined adversary represents a tradeoff that the defending organization must make: how much will they pay to protect the data?

For the private sector, the managers and shareholders must decide this question. This, of course, requires a transparent environment where these costs can be evaluated. Even in a world where managers have the data to make these decisions, will they make them in an optimal fashion for their shareholders? Investment in security is always a cost, while the long term harms of losing competitive information accrue over a long, uncertain time horizon. Yet these harms have bearing on the present value of a company. Do investors care? Interestingly, the chairman of the Security Exchange Commission recently claimed the commission "was not aware that investors have asked for more disclosure in this area." (Lynch, 2011)

If industrial espionage is important enough to be a national priority, it must have some impact on the shareholders of the victim firm as well. Alternatively, if the consensus in the marketplace is that an incident does not negatively impact the long term value of the company, why should it be a matter of public policy? Following from the assumption that it does matter, the lack of demand for cyber security data points to a market failure. Regulators must step in and demand disclosure about cybersecurity incidents. These definitions should be broad enough to allow uncertain investors to react accordingly following an attack.

Incident reporting only allows a negative, reactive model. Firms can attempt to assert a positive security stance through committing to security certifications, such as the ISO 27001 standard. This communicates a short run investment to mitigate a long term risk. Is this likely to be rewarded? Skepticism about certifications and standards might be warranted after looking at the history of environmental risk reduction: one recent study demonstrated that the stock market actually punished firms that adopted ISO environmental risk protection standards (Cañón-de-Francia and Garcés-Ayerbe, 2009). This can be interpreted as either a misuse of resources, or a hidden reactive signal about an undisclosed problem. Both causal mechanisms also apply to information security. In the face of an expected loss of explicit shareholder value, managers may choose against standards adoption.

Beyond this, one can look at the costs and trade-offs in building better, more secure software. Apart from the incentives discussed above, data minimization and compartmentalization play an important role in reducing the risk of data theft. As high profile cases like the wiki leaks incident with State Department cables illustrate, allowing everyone access to all information invites disaster. At the same time, breaking up the flow of information can impose costs in terms of organizational efficiency and effectiveness. This is particularly true in the

intelligence community. Systems that automatically enable information to flow where it is needed without overprovisioning permissions are possible but not easy. This problem cannot be solved in the general case, but rather must be designed to meet the needs of the organization in question.

Cybercrime and intermediaries

The cybercrime ecosystem depends of several key sets of actors comprise the infrastructure of the digital economy. Most classes of cyber crime are detectable at some level, and these intermediary actors are in a position to intervene. One can identify bottlenecks in the cybercrime food chain, where the pool of actors is concentrated, less diverse and often subject to regulation. This makes these intermediaries an ideal point for policy interventions that align the interests in preventing crime with the ability to limit damage and raise the costs to the attackers.

Criminals depend on these intermediaries to access the internet, host web servers and domain name servers, and even transfer and extract money. Different intermediaries can play a key role in addressing different aspects of crime. There is no uniform approach, but interventions need to be evaluated for cheap implementation for the intermediaries and maximum inconvenience for the bad actors.

Malicious behavior on the web requires a web presence, which requires some hosting mechanism. bad actors often seek out bullet-proof hosting, from firms who do not respond to complaints from banks or other private companies. They are resistant to legal interventions as well, and are often based in jurisdictions that are less vulnerable to foreign law enforcement. On the other hand, while geographically diverse, these hosts are somewhat economically concentrated. Taking out one host can do substantial damage to a range of malicious operations. The disconnection of a California server hosting company called McColo led to a large drop in global spam volumes (Clayton, 2009). This case also illustrates the potential to target intermediaries through their own bottlenecks. McColo was knocked off the Internet when security journalist Brian Krebs shared research about its nefarious activities with McColo's internet service providers, who decided to withdraw their services. Schachtman (2011) proposes systematizing this approach by publishing a list of the most offending hosting companies by some consensus process, drawing this to the attention of their ISPs and even threatening those ISPs with further punishment by going after their upstream providers.

Internet Service Providers are the ultimate intermediary on the Internet, providing the needed connectivity to good and bad actors alike. Because of their key role in enabling Internet communication, there is general aversion in the United States to relying on ISPs to police content. From the service providers' perspective, once they start monitoring for any specific behavior, it opens the door to broader duties. But some malicious behavior is not only relatively easy to detect, but it is also benefits the service providers. High traffic malicious activity, such as

the denial of service attacks used in financially- and politically-motivated attempts to prevent public access to specific web sites and servers, poses a cost to the ISP in the form of packets it must send to other networks. On scales large enough to disable websites, this can represent an appreciable cost. Large ISPs have begun cooperating by detecting ongoing distributed denial of service attacks across different networks and blocking the involved traffic from their own subscribers.

Once an ISP has identified a subscriber as a source of malicious traffic, what should it do? The wrinkle in this question lies in the distinction between the individual customer, and the device under his control that is attached to the network. Since many attacks depend on botnets of compromised machines, it is highly unlikely that the customer is actually aware of the malicious activity. While makes assigning responsibility difficult, it also allows the ISP to frame subscriber intervention as a value-added security service. To test this hypothesis, Wood and Rowe (2011) surveyed consumers about several attributes of potential ISP-based security services, including imposing software defenses and quarantines following a compromise. They find that the most respondents would pay for lots of security and little obligation was around $7.25 each month. This suggests that market demand is present, but may not be sufficient to pay for the customer support costs of retail security services.

On the fraud side, financial and credit institutions serve both as a vector of fraud and a means to extract value from fraud. When a criminal seeks to open a new line of credit with a victim's identity credentials, these credentials are verified by credit agencies that also have access to the details of the credit application. This data can be scrutinized more closely to make fraud more difficult and costly to the attacker. A recent study of fraudulent credit applications showed that the impostors supplied obviously fake information, which was accepted by the credit grantors (Hoofnagle, 2010). While closer scrutiny would raise the price of managing personal credit ratings, the responsible agencies are in an ideal position to serve as a strong line of defense.

Financial institutions are also critical for value extraction at the other end of the fraud food chain. The spam economy, for example, is built around networks of botnets sending out diverse spam messages which drive gullible internet marks to a bevy of fake pharmacy websites run by a set of affiliate networks. The spam is hard to detect centrally, hosting can be protected, and the members of the affiliate networks work hard to hide themselves. At some point, however, the victim must pay the network through the pharmacy. For a credit card purchase, the merchant must have a merchant relationship with an acquiring bank to process the credit card information. Levchenko et al (2011) find that just 13 banks handled almost all of the 76 trial purchases they made through spam networks, with three of them handling the majority. This hints at the ability to directly intervene at the financial level, by either pressuring the acquiring banks directly or allowing consumer credit card banks to refuse settlement of funds for suspicious purchases.

Finally, focusing on the intermediaries aligns incentives for understanding the risk of tipping points in online crime. Up to a point, crime represents a simple cost

tradeoff for the organizations that bear some cost of victimization. These costs can be seen as part of doing business, or a margin of error. However, above a certain level, these costs threaten the basic business model of the organization responsible, introducing a new class of risk: that the providers of the infrastructure will remove functionality or reduce functionality of the infrastructure. This risk of a tipping point represents a genuine public interest, but requires transparency and cooperation from the banks and other intermediaries in question.

Conclusion

The incredible benefits that information technology has brought modern organizations have not come without risk. These risks vary in size and scope, from revealing new vulnerabilities in our critical infrastructures to enabling new forms of fraud. The wide range and diversity of these threats points away from holistic solutions, or treating risks to the digital infrastructure as monolithic problems of cybersecurity. Instead, we must study the incentives of both malicious actors and organizations that provide and use these vulnerable systems and networks. The misalignment of incentives and other distortions lead to an under-investment in security, a market failure.

There remain clear policy questions of what the optimal level of security is, but this is a political question that must be resolved through public discussions of the tolerable risk and acceptable expenses in security investment and inefficiencies. Governance frameworks must be evaluated in terms of how they promote investment, how they alter incentives, and who will bear the expenses and risks.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor
Christine Jacobs

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu

This paper is distributed in the expectation that it may elicit useful comments and is subject to subsequent revision. The views expressed in this piece are those of the authors and should not be attributed to the staff, officers or trustees of the Brookings Institution.

References

2011 Identity Fraud Survey Report, Javelin Strategy & Research, February 2011.

Acquisti, Alessandro, Allan Friedman, and Rahul Telang, "Is There a Cost to Privacy Breaches? An Event Study," International Conference on Information Systems (ICIS), 2006.

Akerlof, George A. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism," *The Quarterly Journal of Economics* Volume 84, Issue 3, pg 488-500, 1970.

Albanesius, Chloe, "Citi: Hackers Stole $2.7 Million From Customers," *PCmag*, June 27, 2011.
http://www.pcmag.com/article2/0,2817,2387671,00.asp

Anderson, Ross, "Why Information Security is Hard - an Economic Perspective," Proceedings of the 17th Annual Computer Security Applications Conference, 2001.

Bohme, Rainer and Tyler Moore, "The Iterated Weakest Link," *IEEE Security and Privacy*, Volume 8, Issue 1, pg 53-55, 2010.

Butler, Eric "Firesheep," *codebutler*, October 24, 2010.
http://codebutler.com/firesheep

Cañón-de-Francia, Joaquín, and Concepción Garcés-Ayerbe, "ISO 14001 Environmental Certification: A Sign Valued by the Market?" *Environmental and Resource Economics,* Volume 44, Issue 2, October, 2009.

Card Fraud in the United States: The Case for Encryption, Aite Group, January 13, 2010.

Chapman, Glenn, "US flank exposed on cyber war front: Hayden," *AFP*, July 29, 2010.
http://www.google.com/hostednews/afp/article/ALeqM5jy16bC0-og0TgT9-IZXcze1eaApg

Clayton, Richard. How much did shutting down McColo help? Sixth Conference on Email and Anti-Spam, July 2009.

Detica. "The Cost of Cyber Crime," Cabinet Office, February 17, 2011.
http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

The Cyber-Crime Black Market: Uncovered, Panda Security, 2011.

CSIS. "Cyber Legislation," CSIS Technology and Public Policy Blog, June 17, 2011.
Day, Oliver, Brandon Palmen, and Richard Greenstadt, ``Reinterpreting the Disclosure Debate for Web Infections,'' *Managing Information Risk and the Economics of Security*, ed. M. Eric Johnson, New York: Springer, 2008.

Debit Card Interchange Fees and Routing, Board of Governors of the Federal Reserve System, June 30, 2011.

Department of Defense Strategy for Operating in Cyberspace, U.S. Department of Defense, July 2011.

Economides, Nicholas, "The Economics of the Internet," *The New Palgrave Dictionary of Economics*, 2nd Edition, January, 2007.

"War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?" *The Economist*, July 1, 2010.
http://www.economist.com/node/16478792

Friedman, Allan, Tyler Moore and Ariel Procaccia. "Cyber-sword vs. cyber-shield: The Dynamics of US Cybersecurity Policy Priorities" Under Review, 2010.

Geer Jr., D.E. "Monopoly Considered Harmful," *IEEE Security and Privacy*, Volume 1, Issue 6, pg 14-17, 2003.

Goodman, Seymour E. and Herbert Lin, National Research Council (U.S.), Committee on Improving Cybersecurity Research in the United States, *Toward a Safer and more Secure Cyberspace*, National Academies Press, 2007.

Gorman, Siobhan and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, May 31, 2011.
http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html

Grossklags, Jens, Nicolas Christin, and John Chuang, "Secure or insure?: a game-theoretic analysis of information security games," Proceeding of the 17th international conference on World Wide Web, 2008.

Hoofnagle, Chris Jay, "Internalizing Identity Theft," *UCLA Journal of Law and Technology*, pg 1, 2010.

Kanich, Chris et al. "Spamalytics: An Empirical Analysis of Spam Marketing Conversion," Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008.

Kleiman, Mark and Beau Kilmer, "The Dynamics of Deterrence," Proceedings of the National Academy of Sciences of the United States of America, 106(34), 2009.

Lieberman, Joe, Susan Collins, and Tom Carper, "A gold standard in cyber-defense," *The Washington Post*, July 7, 2011. http://www.washingtonpost.com/opinions/a-gold-standard-in-cyber-defense/2011/07/01/gIQAjsZk2H_story.html

Lynch, Sarah N. "SEC 'seriously' looking at cybersecurity woes," *Reuters*, June 8, 2011. http://www.msnbc.msn.com/id/43332013/ns/technology_and_science-security/t/sec-seriously-looking-cybersecurity-woes/

Lynn, William, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, 2010. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

McConnell, Mike, "Mike McConnel on how to win the cyber-war we're losing," *The Washington Post*, February 28, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

McMichael, William H. "DoD Cyber Command is officially online," *AirForceTimes*, May 21, 2010. http://www.airforcetimes.com/news/2010/05/military_cyber_command_052110

Mills, Elinor, "Internet breaks in Sweden after DNS maintenance error," *CNET*, October 13, 2009. http://news.cnet.com/8301-27080_3--10374062-245.html

Moore, Tyler et al. "The Economics of Online Crime," *Journal of Economic Perspectives*, 2009.

Moore, Tyler and Richard Clayton, "An Empirical Analysis of the Current State of Phishing Attack and Defence," Sixth Workshop on the Economics of Information Security, June 7-8, 2007: Pittsburgh, PA, USA.

Moore, Tyler and Richard Clayton, "The Impact of Public Information on Phishing Attack and Defense," *Communications & Strategies*, 81, pg 45-68, 2011.

OWASP, 2011. "SQL Injection Prevention Cheat Sheet," The Open Web Application Security Project, May 27, 2011. https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

Ozment, Andy and Stuart Schechter, "Bootstrapping the Adoption of Internet Security Protocols," in The Fifth Annual Workshop on the Economics of Information Security, Cambridge, UK, June 2006.

Parfitt, Tom, "Georgian woman cuts off web access to whole of Armenia," *The Guardian.* April 6, 2011. http://www.guardian.co.uk/world/2011/apr/06/georgian-woman-cuts-web-access

Pruitt, Scarlet, "Gov't moves to next phase in building private 'Net," *Network World*, November 28, 2001. http://www.networkworld.com/news/2001/1128privatenet.html

Rowe, Brent R. and Michael P. Gallaher, "Private Sector Cyber Security Investment Strategies: An Empirical Analysis," Presented at The Fifth Workshop on the Economics of Information Security (WEIS), 2006.

Schelling, Thomas C. *Micromotives and Macrobehavior,* W. W. Norton & Company, 2006.

Schachtman, Noah. "Pirates of the ISPs: Tactics for Turning Online Crooks Into International Pariahs" Brookings Institution 21st Century Defense Initiative, Forthcoming.

Spar, Debora, *Ruling the Waves,* Harcourt, 2002.

Symantec Internet Security Threat Report: Trends for 2010, Symantec, 2011.

United States of America v. Rogelio Hackett Jr., no. 1:11CR96 (E.D. Va.) April 21, 2011.

Wang, Qiu-Hong and Seung Hyun Kim, "Cyberattacks: Does Physical Boundry Matter?" Proceedings of the International Conference on Information Systems (ICIS), 2009.

Wood, Dallas and Brent Rowe. "Assessing Home Internet Users' Demand for Security:Will They Pay ISPs?" 10th Workshop on the Economics of Information Security, June 2011.