2011

Developing Cyber Security Synergy

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

Work supported by
the Offices of the Provost,
the Vice President for Research,
and the School of Engineering and Applied Science of
The George Washington University

Table of Contents

Letter from Dean David Dolling

School of Engineering and Applied Science

The School of Engineering and Applied Sciences (SEAS) has a long history of leadership in solving major technological challenges. The current preoccupation of government, industry and the media with theft of government and corporate secrets and identify theft focuses the spotlight on an area SEAS has been a leader on for a long time. SEAS has an education track for undergraduates in computer security and a certificate and two master's programs at the graduate level, and has already graduated several doctoral students in cyber security.

SEAS decided some time ago to organize a collaborative institute with contributors coming from across the broadest spectrum of organizations in GW, and to empower institute staff to conduct research, education and policy activities which would address the cyber security problems in a new, effective manner. This Institute, the Cyber Security Policy and Research Institute, is directed by Lance Hoffman, Professor Emeritus in the Computer Science department and the author or editor of numerous articles and five books on computer security and privacy. Professor Hoffman developed the first course on computer security in a United States University in 1970 and instituted GW's program in cyber security in 1977.

Cyber security is a complex, multi dimensional problem that requires strong scientific skills, but also demands management capabilities and an appreciation of the role that all disciplines may play in addressing it. The SEAS faculty and research community is already engaging in such a collaborative fashion and providing creative ideas to help solve this cyber security challenge. SEAS has an active research program in cyber security. Let me mention just a few of these projects.

- CyberWatch: This is a network of more than sixty academic institutions focusing on developing a stronger cyber security workforce. We provide many services to them, including project and event management for the Collegiate Cyber Defense Competition.
- Cyber security scholarships: We provide government-funded full scholarships for students from many majors across GW that combine a traditional education in their chosen major enhanced by detailed knowledge in cyber security provided by additional courses that address emerging technical and government policy-related issues often using guest lectures by government and outside experts. These students have all attended the lectures on which the papers in this book are based, for example. They also receive hands-on experience in a laboratory that demonstrates traditional and emerging attacks and defenses. Since 2002, these students have gone on to work at 30 government organizations.
- Hardware/Software Approaches to Software Security: A strong level of trust in the system software and hardware is crucial to the widespread deployment of embedded systems. Specific problems being considered include defense against Trojan horse circuits and hardware wrappers that check every memory access and track CPU cycles consumed by each software component.

As you can see, SEAS projects are leading edge and multidisciplinary. There are many others in cyber security, and I invite you to visit the CSPRI website www.cspri.seas.gwu.edu to examine them for yourself.

Introductory Remarks from Director Lance Hoffman

Cyber Security Policy and Research Institute

What a broad collection of challenges and opportunities faces cyber security researchers today! The Cyber Security Policy and Research Institute (CSPRI) is committed to researching solutions to these, informing policymakers, and helping provide GW students an education appropriate for leaders in defining the course of the nation and the world with regard to cyber security. This booklet, containing papers from our 2010-11 seminar series, highlights some of the current expert thought at GW related to various aspects of cyber security.

The overriding theme is that the problem and the solutions are interdisciplinary and must be treated as such. The papers in this booklet, described below, repeatedly offer up lessons from work in fields not always mentioned in the same breath as cyber security. These lessons can provide key insights for cyber security practitioners, educators, and researchers, so that "rather than trying to bolt on exotic solutions focusing on tiny slivers of the technological challenge, holistic and synergistic solutions can be developed," to quote the paper by Prof. Julie Ryan of the School of Engineering and Applied Sciences.

Prof. Ryan laments that time to market has been the driving force in cyber security innovation, rather than a measured and systematic development of well-engineered technologies, and that market forces of adoption have overwhelmed the development processes. She thinks that cyber security must be everyone's job, not just the "elite geeks (although they are very important!)."

Prof. Joseph Cordes of the Columbian College of Arts and Sciences applies lessons from classical economic theory to cyber security. He notes that policy analysis of cyber security options can learn from the evolution of policy in other areas, most notably environmental policy and homeland security policy, from research on the development of voluntary institutions as response to private market failure, and from comparative analysis of policies in other countries and the European Union.

Professor Jeffrey Rosen of the Law School describes the difficulty of translating constitutional values in light of new technologies and believes that the greatest threats to privacy in the 21st Century will come not from the government acting alone, but from private companies, such as Internet Service Providers, Facebook, and Google, acting in conjunction with the government. He draws lessons from the legal literature and suggests that at least three privacy protecting mechanisms -- storage and viewing rules, use restrictions, and minimization -- can be generalized to apply to many of the surveillance technologies from airport scanners to ubiquitous surveillance by GPS-equipped devices that have been proposed after the attacks on the United States on September 11, 2011.

Patricia MacTaggart, a lead research scientist, and Stephanie Fiore, a graduate student in the School of Public Health and Health Services, note that as health information technology evolves and health

care reform moves forward, patient privacy and security are essential to keeping the system credible, trusted, and operating.

Prof. Neil Sikka of the School of Medicine and Health Sciences points out that unstoppable movement to digitization and mobility in health care records brings with it risks such as theft and loss of medical records on portable devices that can be mitigated by the use of new hardware and software technologies such as biometrics, radio frequency identification (RFID), virtualization, full disk encryption, and processor controls.

Computing and data processing is increasingly carried out in the Internet cloud. Prof. Ross Lumley of the School of Business identifies cloud-related research areas including intrusion detection, forensic tools, and security guidelines.

Professor Frederic Lemieux of the College of Professional Studies discusses how forensic sciences are being applied to cyber crime and describes his research that scrutinizes cyber investigation methods and practices, comparing them to a traditional investigative model to identify effective ways to investigate cyber crime.

Prof. Charles Glaser of the Elliot School of International Affairs takes note of the "attribution problem" which arises when a state cannot determine who has attacked it and therefore cannot credibly threaten to respond, and suggests that the importance of this has been exaggerated. Using lessons from deterrence theory, he discusses deterrence of cyber attacks designed to damage the economy and society and those designed to weaken conventional military forces, and notes the importance of integrating deterrence into a multilayer policy designed to protect against external cyber attacks.

Prof. Diana Burley of the Graduate School of Education and Human Development investigated the turnover intentions among future members of the federal government's cyber security workforce and asks how individual, job-related, and organizational factors influence their ex-ante intention to stay? Person-organization fit and the variety of workplace experiences were found important in maintaining a strong employment relationship. This finding can be extended for the private sector, since it and the government have similar issues in developing and maintaining a cyber security workforce.

Approaches from all the disciplines above are necessary if we are to develop practical and efficient solutions to cyber security problems that provide the utility that cyber systems can bring along with a "socially optimal amount of cyber security" (to quote Prof. Cordes' paper). The GW researchers who lectured in 2010-11 in our series (and many others whose contributions are not noted here) are increasingly working across disciplinary borders to develop scalable, viable, practical solutions that address the problems with the multidisciplinary sophistication these issues require. CSPRI is looking forward to continuing to encourage, facilitate, and carry out these research activities in cyber security.

An Overview of the Economics of Cyber Security and Cyber Security Policy

Joseph J. Cordes

Introduction

In May 2011, McKinsey and Company released a major study documenting the world-wide economic impact of the Internet. A widely-cited statistic from the report is that on average, the Internet has added between 3 and 4 percentage points to the gross domestic products of the economies of the developed world. In terms of the United States, this translates into additional total output of between $440 and $580 billion, or between $1,400 and $1,900 per capita. This amount does not include what economists call the "consumer surplus" associated with the Internet which, according to McKinsey, equals on the order of $200 to $330 per year in economic value enjoyed by consumers.[1]

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

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

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

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

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

The Demand and Supply of Cyber Security

The basic economic model of demand and supply provides a useful starting point. Figure 1, which is taken from Bauer and van Eeten (2009), presents a simple version of such a model in which it is assumed that there are two markets: a market for attacks populated by those who seek to breach cyber security and a market for security comprised of those who seek to thwart such breaches. A key insight is that both attackers and defenders need to devote scarce time and resources either to attacking or to defending, and that if both

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

attackers and defenders strive to make rational decisions, at any moment there is some chosen volume of attacks, denoted by V, which depends in part on the amount of security S (left panel of Figure 1). Conversely, there is also some chosen level of security denoted by S that depends in part on the volume of attacks V (right panel of Figure 1).

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

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

The Simple Analytics of Cyber Security

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

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

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

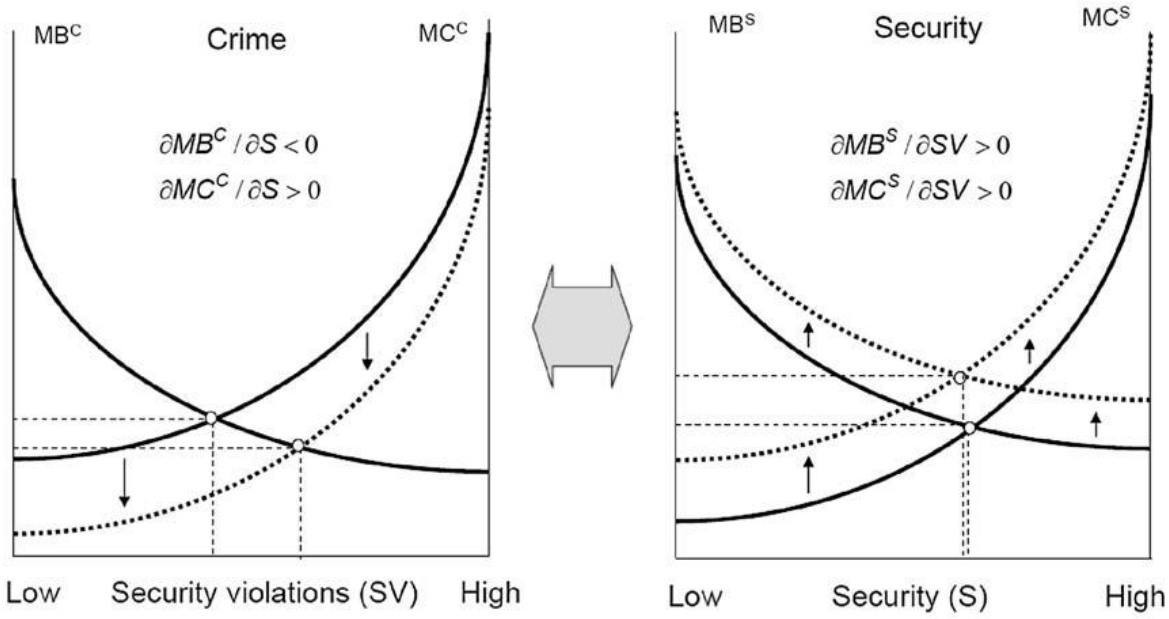
- Similarly, given some level of attack volume, defenders balance the cost of attaining additional security against the benefits from the added security. As in the market for attacks, one can imagine an equilibrium in which the chosen level of security, S, is the point at which the marginal benefit from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

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

- Similarly, the chosen volume of security is the result of benefit cost balancing by defenders, and the level of security can increase or decrease in response to factors that reduce (increase) costs of security and/or increase (reduce) the benefits from greater security. For example, other things remaining constant, technological innovations that reduce the cost of defending against cyber attacks would shift the cost of cyber security downward, which initially would lead to an increase in cyber

security. This effect would be reinforced in the market for cyber attacks because a higher level of cyber-security would raise the cost of attacks, thereby reducing the desired volume of attacks. This change, in turn, would have "second-order effects" in the market for cyber security by reducing somewhat both the benefits of cyber-security measures and further reducing the costs of defending against them.

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



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

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

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

- Second, the model illustrates the importance of recognizing linkages between the behavior of both attackers and defenders in assessing the effects of policies. Consider for example, the case in which some external factor reduces the cost of attacks. As indicated in the left-hand panel, the immediate consequence would be to increase the equilibrium volume of attacks. However, this in turn would also increase both the benefits of defending against attacks, and also the costs of mounting such

defenses. In the specific case shown in Figure 1, these two effects in the market for cyber security are shown as roughly cancelling each other out, in which case the overall level of cyber security (as measured by the volume of attacks) would decline, unless defenders were willing to invest additional resources in cyber defenses over and above those that would be privately optimal in response to the initial increase volume of attacks from V0 to V1.

Table 1: Incentives to Enhance (Reduce) Security (Bauer and van Eeten)

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

What is the Socially Optimal Amount of Cyber Security?

The simple model sketched out in Figure 1 also provides a basis for defining, at least in principle, the concept of a socially optimal amount of cyber security. Figure 2 provides a simple graphical exposition. In Figure 2, the **MSCS** line is similar to the security supply curve in Figure 1, with the important modification that it stands for the marginal social cost of attaining additional increments of cyber-security. Social cost includes not only the private cost of cyber-security measures that are directly borne by private parties, but any and all other resource costs that are incurred. For example, the social cost of enhanced encryption of on-line financial records would include not only the direct costs of developing, installing, and maintaining the more secure system borne by the financial institutions making the investment in the enhanced encryption, but also any costs that third parties needed to make in order to adapt their own systems to the new system. Similarly the

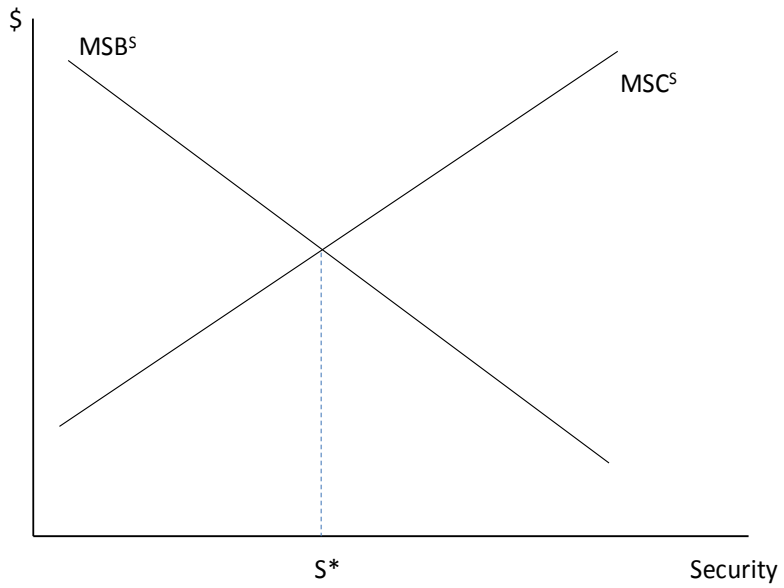
MSBS schedule stands for the marginal social benefit derived from additional increments of cyber security. Social benefit includes not only the benefits of cyber security measures that are received by those investing in such measures, but any and all benefits flowing to other parties. For example, the social benefit from investing in greater cyber security by institution A would include the direct benefits from enhanced security to A plus any benefits from greater security at site A that might spillover to other parties as a result of improved security at A.

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

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

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

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



Private Market Failure and Cyber Security

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

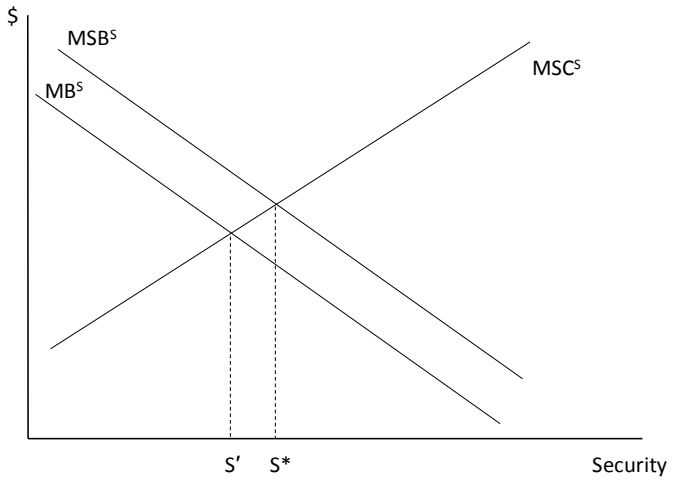
A further contribution of microeconomic policy analysis is to identify cases in which balancing of private benefits and costs in the market for cyber security is not likely to lead to a balancing of social benefits and costs, as shown in Figure 2. An extensive literature in public economics has identified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

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

Network Externalities

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

Figure 3: Underinvestment in Cyber Security



Public Security Goods

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

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

Information Asymmetries and Lemons Problems

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

Coordination Failures

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

Table 2: Prisoner's Dilemma Security Game Payoff

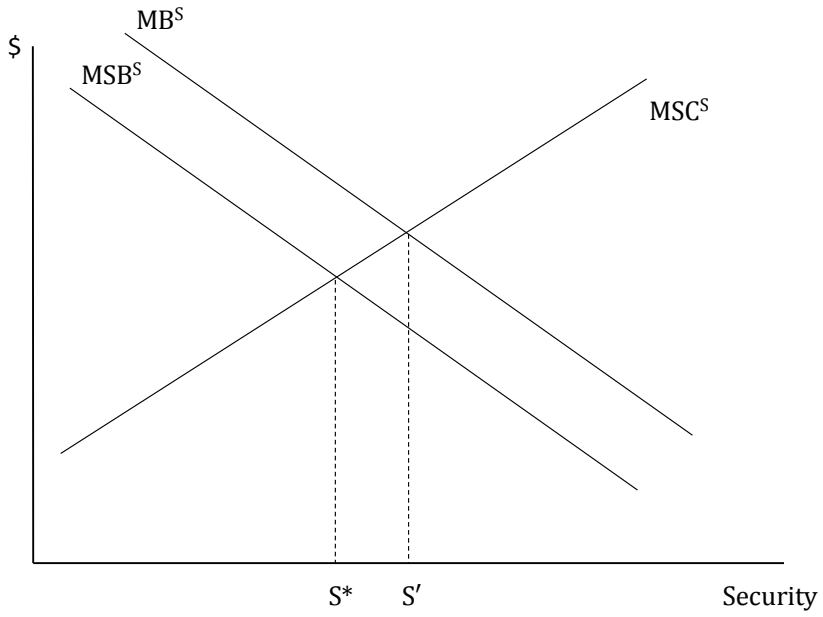
Firm A	**Firm B**	
	Secure Network	**Don't Secure Network**
Secure Network	(20,20)	(10, 30)
Don't Secure Network	(30, 10)	(15, 15)

Source: Powell (2001)

Private Security Actions and Threat Shifting

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

Figure 4: Overspending on Cyber Security



Policy Responses

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

Minimal/Low Intervention

An important role of public policy can simply be to see to it that legal rules provide the right incentives. For example, private parties are more likely to invest in cyber-security if they must also bear some of the cost of cyber-security failures. A classic illustration is that of legal rules assigning liability for cyber breaches such as identify theft and/or cyber financial theft. Americans take it for granted that banks and other financial

institutions are responsible for making good most losses associated with such occurrences. Such is not, however, the case in much of Europe where institutions are not as responsible. Not surprisingly, as several analysts have noted, the American legal approach has created stronger incentives for American financial institutions than their European counterparts to invest in measures to minimize the likelihood of such breaches.

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

More Active Intervention

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

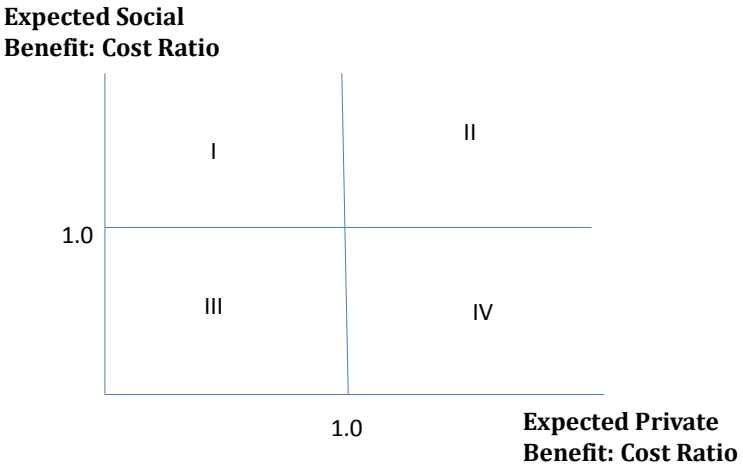
Table 3 below provides a simple taxonomy of possible government actions based both on the degree of government intrusion into private market decisions and which side of "market" is affected by the public policy, and Figure 4 provides a simple classification of cases when more or less activist government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

Table 3: A Simple Taxonomy of Cyber Security Policies

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

The basic message of Figure 5 is that the need for more or less active government involvement in the realm of cyber-security depends on (a) the mix of "private" and "public" benefit. Roughly speaking, the higher the ratio of public to private benefit the stronger the case for policy activism. In the case of public benefits, an additional factor is whether these benefits are more commercial in nature or whether they have more to do with national security.

Figure 5: Public vs. Private Actions



Summary and Future Research

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

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

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

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

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

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

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business

Ross A. Lumley

Introduction

We are now in the midst of a classic technology hype cycle called cloud computing. In the vocabulary of the Gartner Group [1] we are at the peak of inflated expectations. Despite the media hyping cloud computing, there can still be tremendous benefit to many who adopt a cloud computing strategy. This benefit exists for industry, government and the general public alike. We already see the consumer extensively using cloud computing with such services as Google Mail, YouTube, Flickr and many others.

A widespread concern regarding cloud computing is security. People's initial reaction is to avoid having private data in the cloud. While this represents a general lack of understanding, it can be a valid concern. This paper will focus on the issues, solution strategies, and areas for potential research.

Cloud Computing Defined

Before addressing the issues, it is important to understand what cloud computing means, the different types of cloud computing, and the various delivery mechanisms.

The National Institute of Standards and Technology (NIST) has been very involved in setting a framework for cloud computing use by the government. A mission statement on the NIST Cloud Computing website tells us what NIST sees as their role: [2] "NIST's role in cloud computing is to promote the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards" of cloud computing. While the NIST definition is by no means the only definition in industry, it offers one that is clear, concise and well thought out.

A working definition of cloud computing from Mell [3] of NIST is as follows: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is defined in terms of 1) essential characteristics, 2) service models and 3) deployment models.

1. The Essential Cloud Characteristics are:
    - On-demand self-service
    - Broad network access
    - Resource pooling
    - Location independence
    - Rapid elasticity
    - Measured service

2. The Cloud Service Models are:
    - Software as a Service (SaaS)—Use provider's applications over a network
    - Platform as a Service (PaaS)—Deploy customer-created applications to a cloud
    - Infrastructure as a Service (IaaS)—Rent processing, storage, network capacity, and other fundamental computing resources

3. The Cloud Deployment Models are:
    - Private cloud: Enterprise owned or leased
    - Community cloud: Shared infrastructure for specific community
    - Public cloud: Sold to the public, mega-scale infrastructure
    - Hybrid cloud: Composition of two or more cloud types

Focusing on the Cloud Service Models, as shown in Figure 1, NIST [2] highlights a shared security management responsibility that we discuss further in Issue #1 below. The figure illustrates the security control responsibilities between the cloud provider and the cloud customer.

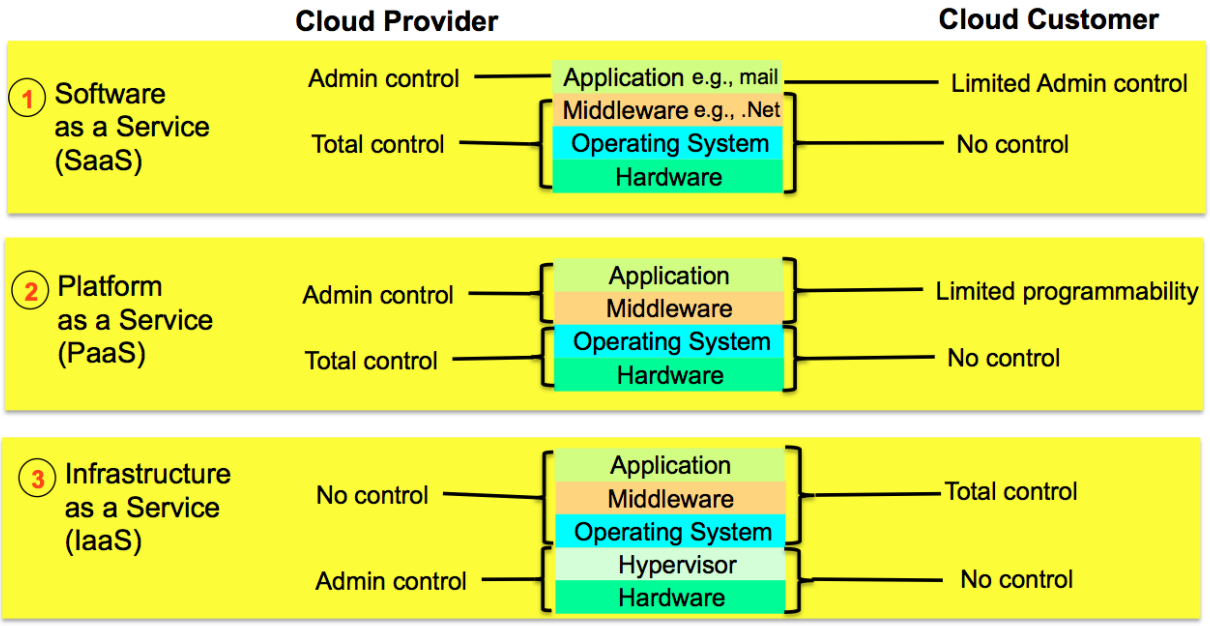


Figure 1. NIST Cloud Service Model Definition (source: NIST [2])

The cloud service models in Figure 1 are not merely three independent approaches to cloud computing. In Figure 2, Briscoe and Marinos [4] show the many interrelationships between these service models and the actors. Later in this paper, we will see that this concept adds new security issues. Gartner [5] refers to this as the "layered cloud architecture."

Cloud Computing Issues

How does the simple security model known as the CIA (Confidentiality, Integrity, and Availability) triad for security pertain to cloud computing? We will discuss eight key issues with cloud computing and explore where these issues fit within CIA.

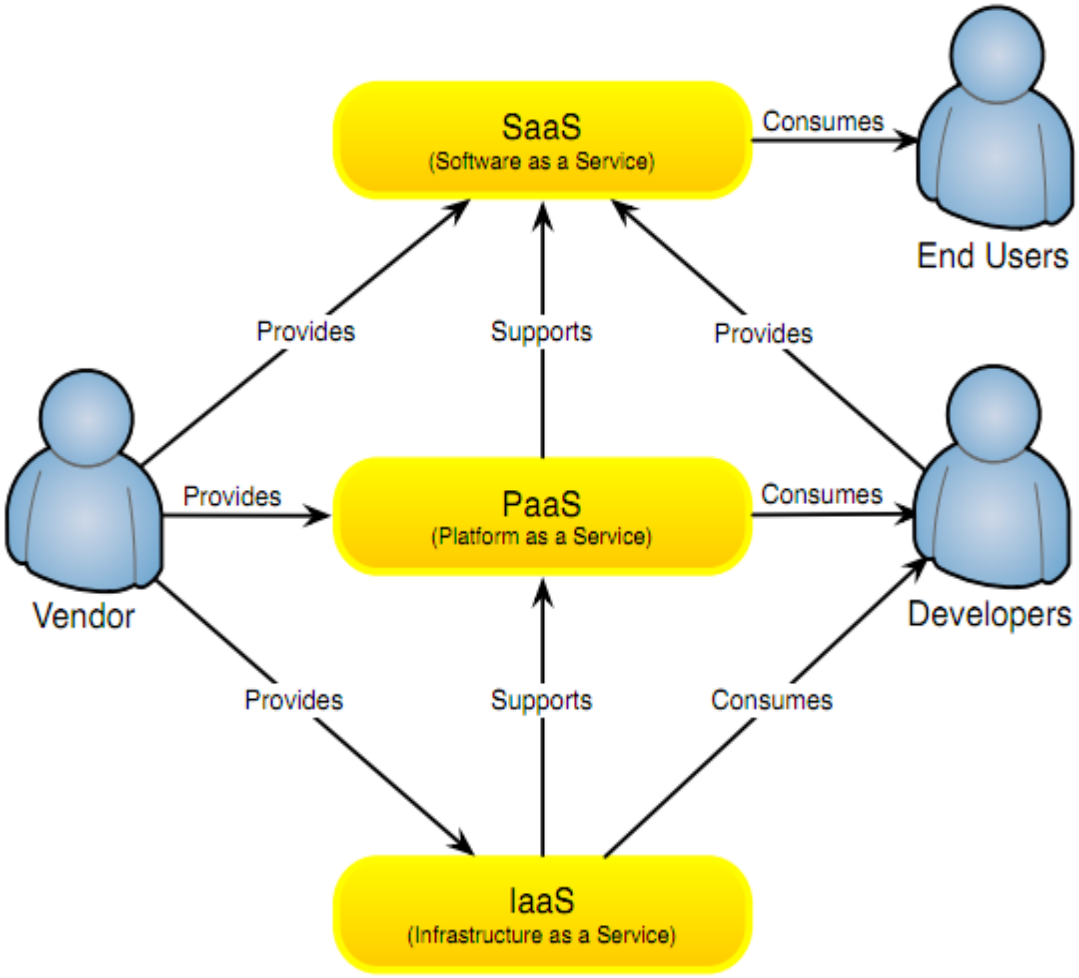


Figure 2. Cloud Computing Layer Interrelationships (source: Briscoe and Marinos [4])

Recently, Congress conducted a hearing to probe the potential issues that might be facing the federal government as it moves aggressively into cloud computing. [6] "Federal Chief Information Officer (CIO) Vivek Kundra said the government spends a quarter of its $80 billion annual IT budget on basic infrastructure such as hardware, software, electricity, and personnel. He said shifting to the cloud could significantly lower these costs." Kundra had a long track record of leveraging cloud computing when he was CIO for the District of Columbia.

During the hearing, it was noted that 22 of 24 agencies have concerns about security in the cloud computing deployment model. Fortunately, the vendor community assured Congress that the providers have resolved the security issues. The vendor community may be overly optimistic. In a survey, Microsoft [7] found that while 58% of the general population and 86% of senior business leaders are excited about the potential of cloud computing, more than 90% of these same people are concerned about the security, access, and privacy of their own data in the cloud. In addition, the survey found that the majority of all audiences believe the U.S. government should establish laws, rules, and policies for cloud computing.

Change Drivers

So why the sudden rush into cloud computing? Haven't we seen unsuccessful attempts at grid computing and utility computing which share many characteristics of cloud computing, most recently Application Service Providers (ASPs)? Several key factors are driving the current stampede. Technology congruence is a major factor as previous attempts into similar infrastructures have fallen short and failed. Many intertwined technologies must be ready to support the infrastructure concurrently, such as broadband availability and virtualization technologies. As the convergence of technologies approaches a feasible level for developing products and service, innovation rapidly leads to practical solutions. That is exactly what we've been seeing from Google, Amazon, Microsoft and many others. Next, in periods of economic challenges we often see radical shifts in infrastructure solutions as businesses look to cut costs and open up possibilities to gain competitive advantages. Governments also see an opportunity to cut cost and add to their agility.

Key Issues with Cloud Computing Security

The following is a discussion of key security issues, which are somewhat unique when considering cloud computing.

Issue #1: Who is responsible for security?

Figure 1 identifies the various cloud computing service models and provides some insight into the responsibilities for security administration. One thing is clear: the responsibility for securing the infrastructure is a shared responsibility between the cloud services provider and the cloud services customer. The distribution of that responsibility between the two participants depends on the deployment model as shown in Figure 1. This issue involves the responsibility for the entire CIA triad.

A significant problem from a security management perspective is: how do we conduct security audits and establish that assurances are in place? This clearly calls for cooperation between the cloud computing services provider and cloud computing services customer and is discussed in Issue #2.

Issue #2: How do we gain transparency into cloud services provider security management?

In a speech [8] to the Brookings Institute, Microsoft General Counsel Brad Smith urged the cloud computing vendor community to "band together to create rules on privacy and security or face the prospect of having the U.S. Congress pass regulations." Security requirements of government customers cannot be met without this vendor/customer cooperation.

Heiser [5] addresses the issue of transparency by positing, "the ability to thoroughly analyze the security and continuity risks of many of today's Internet-based commercial services is much reduced compared with traditional computing." He also points out that third-party certifications are immature and unable to address all aspects of cloud computing risk. He identifies three key risk factors in digital implementations as accessibility, complexity, and extensibility.

One solution put forth by the federal government is the creation of the Federal Risk and Authorization Management Program (FedRAMP) which is an interagency effort led by the General Services Administration (GSA), under the authority of the Federal Chief Information Officer (CIO), and with joint authorization support from the Department of Homeland Security (DHS), Department of Defense (DoD), and GSA. [9]

FedRAMP defines their mission as follows:

> FedRAMP has been established to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products. FedRAMP allows joint authorizations and continuous

> security monitoring services for government and commercial cloud computing systems intended for multi-agency use. Joint authorization of cloud providers results in a common security risk model that can be leveraged across the federal government. The use of this common security risk model provides a consistent baseline for cloud-based technologies. This common baseline ensures that the benefits of cloud-based technologies are effectively integrated across the various cloud computing solutions currently proposed within the government. The risk model will also enable the government to "approve once, and use often" by ensuring multiple agencies gain the benefit and insight of the FedRAMP's authorization and access to service provider's authorization packages.

It is becoming clear at this point that there are many potential benefits to the wide array of computing paradigms, but the real security concern is how to verify the security measures and processes in place. The work of NIST and FEDRAMP provides a major step forward in addressing these issues since the federal government has enormous power to ensure that the cloud providers will work with the community.

Issue #3: How do we conduct penetration tests?

Penetration testing (pentest), a key part of vulnerability management, is an approach for evaluating the security of a computer system or network. We must be able to conduct a pentest in a cloud computing environment without triggering a response from the provider or causing loss of service for our company as well as any of the multitenant customers. The provider will try to prevent this from happening. This would affect the availability tenet of CIA.

Amazon [10] has published a policy that includes a procedure for customers to conduct a pentest. An Amazon Elastic Compute Cloud (EC2) customer that wants to simulate a real-world attack without violating that policy is required to request permission to do a pentest. Amazon keeps this request confidential and answers within 24 hours in a non-automated fashion. While Amazon's recent policy provides a workable methodology for conducting a pentest, there are many other cloud service models that need a similar solution.

Issue #4: What happens when a cloud computing service provider goes bankrupt or is acquired by another company?

With any outsourcing strategy, it is standard practice to have many performance terms defined in a Service Level Agreement (SLA). In addition to an SLA, some unique issues must be dealt with, such as ownership of the data, the right to audit, and the location of the data (at least from a country perspective). One critical issue is caused by the potential for vendor lock-in due to the proprietary nature of many cloud provider services. The proprietary nature combined with the potential for a cloud provider to go out of business or be acquired by a company with different policies poses a serious potential problem. SLAs and other contractual arrangements can provide effective protection. There are also strategies for minimizing the impact of proprietary services such as basing services on open source and industry standard based products.

This is an example of the availability in the CIA triad. Planning for the possible event falls into the business continuity and disaster planning process.

Issue #5: How do we gather forensic evidence in the case of a breach?

Computer forensic investigations are based on quantitative analysis of computer systems searching for evidence that can be used in legal proceedings. How do we gather forensic evidence when the cloud instance becomes a crime scene? [11] From a CIA perspective this would be an investigation into a breach of all three tenets.

In December 2009, Amazon introduced Elastic Block Storage (EBS) boot volumes allowing the launching of a virtual machine image from a virtual storage area network (SAN). This is similar to attaching an external drive to a physical computer.

John Reese [12] describes a process for gathering forensics at the IaaS level of cloud computing. He points out that with the new EBS-based server in the Amazon cloud, you have the ability to take a snapshot of the running virtual system the moment you learn of a compromise. A snapshot takes just a few seconds and then you can take the compromised server offline. With the compromised server offline, you can begin the forensics process by attaching copies of the snapshot you took prior to taking the server offline to separate cloud-based servers. You can even run investigative tests against the data with the knowledge that you have a snapshot of a pristine copy of the compromised state.

This approach offers a sound solution in the case of the Amazon IaaS offerings, but things get more complicated as we move up to the PaaS and SaaS levels. At these levels, we see in Figure 1 that the shared security management responsibilities between the provider and customer move up into the development platform level and even the application itself with SaaS.

Issue #6: Hypervisor vulnerabilities

A key technology introduced with cloud computing is the hypervisor, i.e. the low-level operating system layer (sometimes known as a virtual machine monitor) which allows multiple operating systems (called guests) to run concurrently on a host computer. The hypervisor function exists whenever we are using virtualization. It essentially presents virtual hardware to the software running above the hypervisor layer. As can be seen in Figure 1 at the IaaS level, the hypervisor separates the layers that the cloud service provider controls from the layers controlled by the customer.

As always happens when we introduce new technology to gain a new capability, we also add new risks, vulnerabilities, and the potential for exploits. In the public cloud it is common that these guest operating systems will belong to totally different customers, a concept referred to as multi-tenancy. The introduction of the hypervisor, along with the paradigm of public cloud computing, can result in a new type of threat of a hypervisor breach allowing one virtual machine customer to gain access to the data of a different customer. Because the hypervisor handles multiple virtual machines within a physical machine, an attack against the hypervisor could compromise multiple applications and, in the case of public cloud computing services, multiple customers' systems and applications could be compromised. The attacker then could steal user information, spread malware, or deploy the cloud's computing resources for other attacks.

Hypervisor vulnerabilities are certainly patched quickly once discovered, but as an intrusion detection capability, NC State and IBM [13] researchers have developed a prototype security tool that operates in stealth mode to determine the security of a hypervisor so as not to tip off attackers. The so-called HyperSentry software runs outside the hypervisor to verify in real time whether malware or an attacker has compromised it.

Issue #7: Layered cloud architecture

Cloud computing enables a decoupling of the layers, with both the customer and service provider taking on whatever level of value-added services with which they are most comfortable. In an increasing number of cases, the provider is itself the buyer of a lower-level service, such as a platform, infrastructure, or physical rack space. While the PaaS model is less popular today as a service for end users, a growing number of SaaS offerings are hosted within some other vendor's PaaS or IaaS service.

Such a nested hosting arrangement increases the platform risks and especially the network risks associated with a multi-tenanted environment, and it adds layers between the customer and the actual point of operations. This, combined with lack of transparency, increases the complexity and thus the security risks.

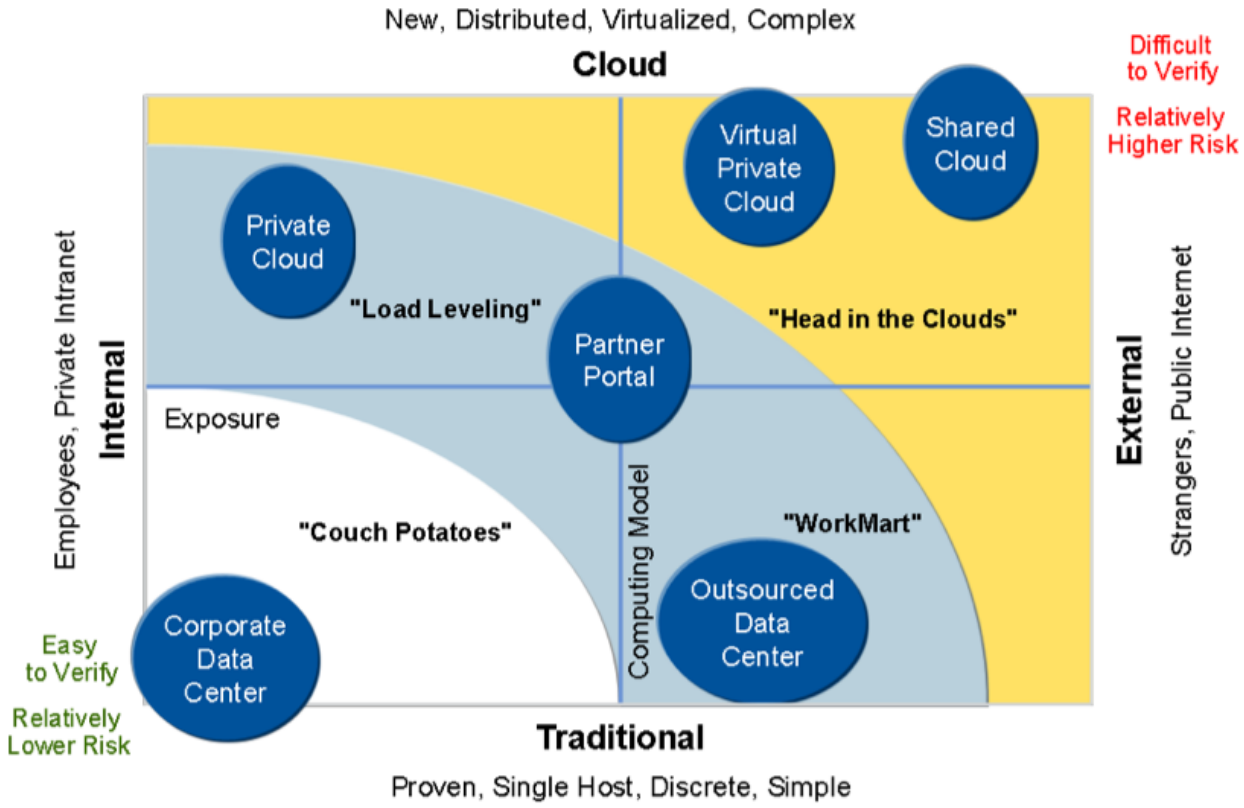


Figure 3. Complexity and Accessibility Increase Risk (source: Heiser [15])

Issue #8: Lack of direct experience

We are now asking inexperienced bureaucrats and non-technical policy makers to set regulations on cloud computing use. At a conference in 2010, Balding [14], founder of cloudsecurity.org, asked a room of 100 security professionals how many had actually used the cloud for data storage and how many have actually launched an instance of an Amazon Elastic Compute Cloud (EC2) virtual machine. The response was that twenty had used cloud data storage and six had launched an EC2 instance. These are security professionals, so one can imagine the folklore that influences the bulk of the community.

In Figure 3, Heiser [5] provides an interesting view of cloud computing technologies, and from this a roadmap for the enterprise to move from the familiar corporate data center to a fully shared cloud environment. The characterization of the regions represents different levels of maturity and competence in situating data and applications in the same deployment models identified by NIST as mentioned earlier. The level of risk is lowest for the corporate data center because complexity is lower. He states that services in the upper right are complex and highly exposed with reduced transparency and thus the most challenging for conducting risk management. The maturity level in dealing with these issues should dictate the type of cloud computing service appropriate for a given organization.

The Bottom Line on the Issues

Beyond the issues of analysis and verification, the security issues largely become those with which we are already familiar, at least from a procedural standpoint. Issues are being identified, but in most cases we have solutions given appropriate access and cooperation. Cloud computing presents new challenges but the problems are familiar and all fall under the CIA triad. These are familiar risk management problems of risk analysis and mitigation. Outsourcing is not new and as always with outsourcing, transparency is a problem. But the U.S. Federal Government is addressing many of these vendor transparency issues through FedRAMP and the NIST efforts. Application software vulnerabilities do and will exist but these typically are the same as with traditional computing (especially at the SaaS level).

Above all, we need to develop and tailor policies, procedures, standards, and tools specifically to address the above issues. In the next section, we will outline research endeavors that also will combine with other processes mentioned above to address these issues.

Research Areas of Interest for Cloud Computing Security

As discussed above, many of the issues we have raised are addressed with established security management techniques or changes that have already been put forth to deal with unique challenges. This is only the beginning in addressing security concerns with cloud computing. Much work and research needs to be done to answer all the issues. Research into cloud computing security issues includes the following:

- Specific intrusion detection tools for the cloud (e.g. OSSEC Open Source Host-based Intrusion Detection System).
- Forensic tools for cloud services models Paas and SaaS. The EBS Volumes on Amazon's cloud services offer a very effective way to snapshot a running virtual server on IaaS.
- The safety of SaaS cloud offerings is a broad and very important area. We need all manner of research into the safety of popular cloud SaaS offerings. The Open Web Application Security Project (OWASP) guidelines focus on improving the security of application software. Similar guidelines should be identified for SaaS applications.
- Policy research that may shape new laws.
- The hybrid deployment model identified by the NIST definitions offers a good strategy for having a common infrastructure where a part resides behind the firewall. This approach needs further research but has the potential to address concerns about moving private data into the cloud.

The research topics described above are part of the agenda for the Cloud Computing Research Laboratory at The George Washington University Science and Technology Campus in Ashburn, Virginia.

As we enter a new era of global business, with proper security management in place, cloud computing offers much more than just another computing platform. Instead, greater business agility and flexibility becomes possible in defining new business models and formulating enterprise strategy.

References

[1] David Mitchell Smith. "Hype Cycle for Cloud Computing." *Gartner Research Group*, 00201557, Web. 3 Dec. 2010.

[2] "Presentation on Effectively and Securely Using the Cloud Computing Paradigm." *csrc.nist.gov*. Web. 18, December 2010. http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt

[3] Peter Mell and Tim Grance. "The NIST Definition of Cloud Computing." *National Institute of Standards and Technology, Information Technology Laboratory.* Version 15, 2009. http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[4] Gerald Briscoe and Alexandros Marinos. "Digital Ecosystems in the Clouds: Towards Community Cloud Computing," 2009, http://arxiv.org/pdf/0903.0694v3

[5] Jay Heiser. "Analyzing the Risk Dimensions of Cloud and SaaS Computing." *Gartner Research Publication* G00174873, 2010.

[6] "Oversight Daily--Committee Examines Government-wide Transition to Cloud Computing." *Committee on Oversight and Government Reform*. N.p., 1 July 2010. Web. 19 Dec. 2010. http://oversight.house.gov/index.php?option=com_content&view=article&id=5015:oversight-daily-committee-examines-cloud-computing&catid=88:blog&Itemid=57

[7] Grant Gross. "Microsoft Calls for Cloud Computing Transparency." *IDG News,* Jan. 2010. http://www.pcworld.com/article/187294/microsoft_calls_for_cloud_computing_transparency.html

[8] "Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud." *Microsoft News Center,* January 2010. http://www.microsoft.com/presspass/press/2010/jan10/1-20brookingspr.mspx

[9] *cio.gov*. Web. 18 Dec. 2010. http://cio.gov/pages-nonnews.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP

[10] *Amazon.com*. Web. 18, Dec. 2010. http://aws.amazon.com/security/penetration-testing/

[11] Webb Hobson. "Securing the Cloud: Digital Investigations for the Cloud." *Sans,* November 2010. http://computer-forensics.sans.org/summit-archives/2010/files/eu-digital-forensics-incident-response-summit-emma-webb-hobson-new-computer-forensics-techniques-panel.pdf

[12] George Reese. "Cloud Forensics Using EBS Boot Volumes." *Oreilly.com*,. Web. 18, January 2010. http://broadcast.oreilly.com/2010/01/cloud-forensics-using-ebs-boot-volumes.html

[13] Kelly Jackson Higgins. "NC State, IBM Researchers Create „Stealth " Hypervisor Security Tool Will Ultimately Be Offered as Open Source." *Darkreading.com*. Web. 18, September 2010.. http://www.darkreading.com/database-security/167901020/security/application-security/227500269/index.html

[14] Craig Balding. "Cloud Security Threats Survey." *Cloudsecurity.org/blog*. Web. 18, February 2010. http://cloudsecurity.org/blog/2010/02/23/cloud-security-threats-survey.html

[15] owasp.org. Web. http://www.owasp.org/index.php/Main_Page

Recruiting, Educating, and Retaining Cyber Security Professionals in the Federal Workforce: Lessons Learned but not yet Applied

Diana L. Burley

Introduction

President Obama, like Presidents Bush (ref. *National Strategy to Secure Cyberspace*) and Clinton (ref. *National Plan for Information Systems Protection*) before him, has made the recruitment and retention of cyber security professionals a national security priority.[1] Noting that cyberspace underpins almost every facet of modern society and that the nation's computer networks face constant attack from a host of enemies, Mr. Obama asserts that cyber security risks pose some of the most serious economic and national security challenges of the 21st Century (CPR 2009).

To effectively meet this challenge, industry analysts suggest that the United States must develop a comprehensive and coordinated effort to recruit and retain cyber security professionals in the federal workforce (Partnership for Public Service/Booz Allen Hamilton 2009). For many federal agencies this effort includes innovative strategies to bolster the federal workforce. For instance, service corps programs, which provide educational scholarships in exchange for some period of public service, are being used as creative recruitment and socialization tools. The federal cyber corps programs, offered through the National Science Foundation in partnership with the Departments of Defense and Homeland Security, are model service corps programs. The federal cyber corps programs consist of the Federal Cyber Service: Scholarship for Service (SFS) program and the Information Assurance Scholarship Program (IASP). The larger of these two offerings, the SFS program, is the focus of this study.

SFS is an inter-agency service corps program that recruits future members of the federal cyber security workforce (see https://sfs.opm.gov/). Since the program's inception in 2001, the federal government has distributed more than $75 million in scholarship support, with another $15 million used to develop curricular innovations and socialization activities, for nearly 800 current and future members of the federal cyber corps. The SFS program was offered through 21 different academic institutions (see the program website at https://sfs.opm.gov for a list of participating institutions) and had 196 current students at the time of this study. In exchange for post-graduation service in the federal cyber corps, SFS students receive scholarship support for up to two years of study in a cyber security program. These two years of study can be the last two years of undergraduate study, two years of a master's degree, or two years of doctoral study as new as possible to degree completion.

Although service corps programs like SFS are an effective recruitment method, they do not guarantee that the new service corps members will remain in the federal cyber security workforce after the public service commitment period expires. Although significant research has been conducted on the turnover intentions of IT professionals once they are engaged in an employment relationship, not much is known about the ex-ante turnover intentions of future IT professionals. Moreover, no study of the turnover intentions of future cyber-security professionals has been done. Given the high cost of this recruitment and socialization tool, however, it is critical to gain insight about the turnover intentions of cyber corps participants prior to their entrance into the federal cyber corps. Thus, this study investigated the turnover intentions among future members of the federal cyber corps and asks the question of how do individual, job-related and organizational factors influence their ex-ante intention to stay? This report summarizes the study premise, conceptual framework and findings. The report concludes with a brief discussion of the implications of the study results.

[1] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>

Determinants of Turnover Intentions

The high cost of recruitment and socialization activities, along with the strategic importance of an organization's human capital, has led to the wide investigation of employee retention and turnover in the scholarly IT literature (e.g. Agarwal et al. 2007, Kim and Lee 2007). For public sector IT workers, job-related factors such as public service motivation (e.g. Perry, 1997), affective commitment to the agency (e.g. Mowday, Steers and Porter 1979, Naff and Crum 1999, Kim and Lee 2007), role ambiguity and conflict (e.g. Igharia and Greenhaus 1992, Kim 2005, Reid et al. 2008) and organizational factors such as task variety (e.g. Reid et al. 2008) have been identified as key antecedents of turnover intention. Agarwal et al. (2007) experimentally examine the ex-ante turnover intentions of new IT workforce entrants. Focusing on risk and situational variety, their findings reinforce the importance of individual, job-related, and organizational factors on turnover intentions, and suggest that the interaction of these factors can influence turnover intentions.

This study extended the research on ex-ante turnover intentions among public sector IT workers by focusing on future members of the federal cyber corps as indicated by their participation in the SFS service corps program. Four antecedents of turnover intention are considered: affective commitment to the agency, public service motivation, role stressors (role ambiguity, role conflict), and preferred variety. As suggested by Agarwal et al. (2007), focusing the analysis to a limited set of antecedents that have been shown to be relevant factors for public sector IT workers, has both theoretical and practical benefits. Theoretically, fewer variables allow for a more parsimonious explanation. Practically, fewer variables should facilitate the use of study results to influence recruitment and retention activities.

The conceptual model, adapted from Agarwal et al. (2007) and shown in Figure 1, posits that the role stressors of role ambiguity and role conflict, and commitment to public service directly influence turnover intentions, and that the influence of affective commitment to the agency is moderated by individual preferences of an ideal work environment. Although Agarwal and her colleagues (2007) include situational risk in their model, it is not included here. Situational risk refers to the level of vulnerability associated with the organization. This study focused on future IT professionals who have already made the commitment to go to work for the federal government and SFS participants are effectively guaranteed employment for the length of their service period (typically 2 years).

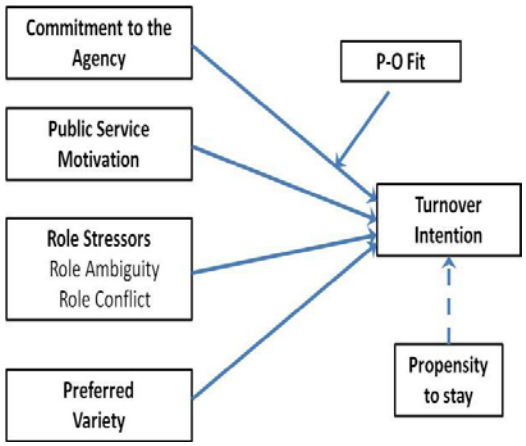


Figure 1. Conceptual model of turnover intentions for future cyber corps members.

The second adaptation of the model is the inclusion of affective commitment to the agency. Affective commitment to the agency has been shown to be an important consideration for turnover intention in the

public and non-profit sectors (Kim and Lee 2007). Affective commitment is the strong belief in and acceptance of the organizational (or agency) mission (Mowday, Steers and Porter 1979). Although the overall mission of the federal government is consistent across agencies, each individual agency has its own distinct mission. Public sector agencies are mission-driven institutions where employee mission attachment plays a significant role in retention (Kim and Lee 2007). The mission at NASA is very different than at the Department of Defense, which is different from the mission at the Department of Education.

Given these distinctions, matching the agency mission to individual preferences of an ideal work environment is an important factor to consider. For cyber security professionals, a significant distinction exists between Department of Defense and intelligence community agencies and civilian agencies. Thus, the model includes affective commitment to the agency with a moderator of person-organization fit. Though support for the moderating effect of situational variety was not supported in the Agarwal et al. (2007) study, as they suggest, additional exploration is warranted.

Public service motivation has been empirically shown to have a negative association with employee turnover intentions in government agencies (Naff and Crum 1999). Further, Ihrke (2004) suggests that the fit between an agency's mission and the preferred mission of the individual employee is a determining factor for intention to stay in that agency; finding that a fundamental change in the mission of a federal agency significantly influenced the desire to change jobs.

Role ambiguity is the extent to which the responsibilities of and expectations for the role are not well defined (Bostrom 1981). The more clearly a role is defined, the easier it is for the employee to fulfill role requirements (Bostrom 1981). IT professionals often experience role ambiguity as their tasks are often broadly defined and variable (Igharia and Greenhaus 1992). Moore (2000) found that role ambiguity and role conflict are contributing factors of work exhaustion and turnover intentions of IT professionals. Role conflict occurs when employees perceive an inconsistency in expectations and job requirements (Bostrom 1981), and has a negative influence on IT employee retention (Igharia and Greenhaus 1992).

Preferred variety refers to the individual preferences for variety that a job could offer in their career. Specifically, this variable refers to the preference for variety of work experience, the variety to mobility among IT jobs, and the preference for variety of skills obtained in this job. Larger, more complex agencies are likely to have a greater variety of both technologies and experiences than smaller agencies. It is also true that the desired amount of variety in an organization varies across individuals (e.g. Inman 2001). Given the importance of the person-organization fit for reducing turnover (Kristof 1996), it is critical to understand preferred variety with turnover intentions.

Finally, we include propensity to stay as a control variable for turnover intention in the context of future members of the federal cyber corps since there may be differences in each individuals' propensity to remain in a specific job. In this context, propensity to stay refers to the individual's expected employment duration with a single agency.

Data Collection and Sample Demographics

Study participants included future members of the federal cyber corps as indicated by their current participation in the Federal Cyber Service: Scholarship for Service (SFS) program. At the time of this study, the program included 196 participating students and all 196 SFS students were included in the study sample population. Data collection occurred through a web-based survey administered during early January 2010. Data collection efforts resulted in 122 survey responses; yielding a 61% response rate. Of these, 106 responses (or 54% of the population) were complete and used in the analysis.

Table 1 shows the demographic characteristics of the sample. The 106 respondents attended 21 different academic institutions. Of them, 69% joined their program in 2009, 62% had relevant prior work experience,

63% were under the age of 25, 78% were male, and 75% were enrolled in master's degree programs. Slightly more than 50% of respondents identified themselves as majoring in computer science or engineering. Less than 10% responded favorably to the statement that they would likely leave the public sector cyber corps at the end of their service period, and approximately 60% indicated a preference to work for an intelligence or security agency.

Table 1. Sample Demographics.

Variable		Frequency	%
Gender			
	Male	83	77.6
	Female	24	22.4
Age			
	<25	67	62.6
	25-35	40	37.4
Degree Program			
	BA	21	20.1
	MS	78	75
	PhD	5	4.8
Prior Work Experience		66	62.3
Concentration/Major			
	Computer science/Engineering	56	52.9
	Information Assurance/Security	27	25.5
	Information Science/Management	23	21.7
Year of Program Entry			
	2008	24	23
	2009	70	67.3
	2010	7	6.7

Analysis Method

The survey instrument was designed to collect data on the relationship between individual, job-related and organizational factors and the ex-ante intention to stay in the federal cyber corps. Variables were measured using survey items as provided in the validated instruments used in Argawal et al. (2007) for preferred variety, Bright (2008) for person-organization fit and propensity to stay, Tsui et al. (1997) for commitment, Perry (1996) for public service motivation, and Moore (2000) for role ambiguity and role conflict. Items were measured using a seven-point Likert-type scale ranging from strongly disagree to strongly agree. Item correlations and regression models were used to determine if/how individual, job-related and organizational factors influence the ex-ante intention to stay of future members of the federal cyber corps. Findings are summarized below.

Summary Findings

Table 2 shows the combined response means for each of the key variables in the model. Of the scaled items, respondents indicated that the variety of tasks and experiences, along with the fit between their individual preferences and the organizational priorities were important antecedents to turnover intention. The job related characteristics, balanced workload, and role conflict also proved to be important factors for turnover intention. Public service motivation and the attachment to agency mission were not as important to turnover intention.

The results of the correlation and regression analyses provided the following key findings:

- Individual factors: Public service motivation was significantly, negatively correlated with turnover intention.
- Job-related factors: Respondents preferred a high degree of task variety. However, they wanted this variety to come with clear job roles and low levels of role conflict. Both role ambiguity and role conflict were positively correlated with turnover intention.
- Organizational factors: Mission attachment was negatively associated with turnover intention. The higher the attachment to the agency mission, the lower the turnover intention.
- The better the fit between workplace mission and preferred mission of the individuals, the lower the turnover intention.
- The results did not indicate significant differences in motivators for turnover intentions based on demographic variables, program tenure, or academic major.

Table 2. Combined Response Means

Items	Combined Mean
Preferred variety	6.16
Person-organization fit	6.07
Propensity to stay	5.71
Role ambiguity	5.68
Balanced workload	5.63
Public service motivation	5.37
Role conflict	5.34
Mission attachment	4.99

Conclusion

This research sought to explore how individual, job-related and organizational factors influence the ex-ante intention to stay in the workforce of future members of the federal cyber security workforce. The results of this study suggest that this population of future members of the federal cyber security workforce will be driven by similar individual, job-based, and organizational characteristics as those which motivate current members of the public sector IT workforce to remain with their employer. The results highlight the importance of person-organization fit in maintaining a strong employment relationship and suggest that care should be taken to ensure that employees and employers are properly matched.

References

Agarwal, R. and Ferratt. 1999. *Coping with Labor Scarcity in Information Technology: Strategies and Practices for Effective Recruitment and Retention*, Cincinnati, OH: Pinnaflex.

Agarwal, R., Ferratt, T. and De, P. 2007. "An Experimental Investigation of Turnover Intentions Among New Entrants in IT," *The Database for Advances in Information Systems*.

Baroudi, J. J. 1985. "The impact of role variables on IT personnel work attitudes and intentions," *Management Information Systems Quarterly*. 9, 4, 341-356.

Bostrom, R. P. 1981. Role conflict and ambiguity: Critical variables in the user-designer relationship.
Igharia, M. and Greenhaus, J. H. 1992. "Determinants of MIS employees' turnover intentions: A structural equation model," *Communications of the ACM*, 359, 2, 34-45.

Ihrke, D. M. 2004. "Mission Change in a Federal Agency and its Link to Employee Transfer Preferences," *American Review of Public Administration.* 34, 2, 181-198.

Inman, J. 2001. "The Role of Sensory-Specific Satiety in Attribute-Level Variety Seeking," *Journal of Consumer Research*, 28, 1, 105-120.

Kim, S. 2005. "Factors Affecting State Government Information Technology Employee Turnover Intentions," *The American Review of Public Administration*, 35, 2, 137-155.

Kim, S. E. and Lee, J. W. 2007. "Is Mission Attachment an Effective Management Tool for Employee Retention? An Empirical Analysis of a Nonprofit Human Services Agency," *Review of Public Personnel Administration*, 27, 227-248.

Kim, S., Wright, B. E. 2007. "IT Employee Work Exhaustion: Toward an Integrated Model of Antecedents and Consequences," *Review of Public Personnel Administration*, June, 27,147-170.

Lewis, G. B. and Frank, S. A. 2002. Who wants to work for government? *Public Administration Review*, 62, 395-404.

Mowday, Steers, R. M. and Porter, L. W., (1979). The Measurement of Organizational Commitment. *Journal of Vocational Behavior*, 14, 224-247.

Naff, K. C. and Crum, J. 1999. Working for America: Does Public Service Motivation Make a Difference? *Review of Public Personnel Administration*, 19, 4, 5-16.

Opsahl, A. 2008. IT Workforce shortage Forces Government to Change Recruiting Methods. Public CIO Magazine, 2/1/2008.

Porter, L. W. and Steers, R. M. 1973. Organizational work and personal factors in employee turnover and absenteeism. Psychological Bulletin, 80, 2, 151-176.

Reid, M. F., Riemenschneider, C. K., Allen, M. W. and Armstrong, D. J. 2008. "Information Technology Employees in State Government," *The American Review of Public Administration*, 38, 1. 41-61.

Rigas, P. 2009. "A model of turnover intention among technically-oriented information systems professions," *Information Resources Management Journal*, 22:1, pp. 1-23.

Cyber Security: The Mess We're In and Why It's Going to Get Worse

Julie J.C.H. Ryan

Introduction

We, collectively, have dug ourselves into a hole with the decisions we have made in the last 30 years in cyber security. Systematically, humans have adopted information technology at a dizzying pace, paying essentially no attention at all to security in the process. Despite the repeated efforts of scientists, policy makers, and engineers to both draw attention to the problem and to provide solutions, the market forces of adoption have overwhelmed the development processes. Time to market has been the driving force in innovation, rather than a measured and systematic development of well-engineered technologies.

Now we are faced with a system that is not only highly complex and tightly coupled, but also riddled with holes and critically dependent on knowledge. The lack of systematic engineering to reduce the impact of exploited vulnerabilities is but one problem. An additional complicating factor is that so many so-called security engineers have little appreciation for either understanding or calculating the systemic effects of security choices in architectures. A disturbing number of certified security experts are woefully ignorant on many important issues in computer security. These symptoms of a kludged system in general have led to a reality where large corporations have to retrain newly hired computer scientists on how to develop relatively bug-free software, users of products routinely are forced to accept licenses that declaim any performance issues, and where information security officers play the functional equivalent of "whack-a-mole" with enterprise systems in order to thwart the bad guys.

To make things worse, the landscape of attacks and vulnerabilities has continued to evolve as well, making the existing situation extremely dicey. This is to be expected, since attackers have nothing but motivation to get better at their craft. But meanwhile, the products that continue to flood the market continue to have significant vulnerabilities that are just waiting to be discovered by the attackers. Even more disturbingly, the users of information technology seem to have thrown up their collective hands in the functional equivalent of "it's not my job." The result is a situation where attacks are effective, mistakes are prevalent, and critical processes are at extreme risk. (Really, it's fairly amazing that this whole kludged system works at all, much less as well as it does.) And it's only going to get worse unless we make radical changes in the way we approach the problem space.

The State of Affairs: A Brief Summary

Forty-one years after the publication of the landmark Defense Science Board report on Security Controls for Computer Systems (Ware 1970), we find ourselves in a computer ecosystem that is proliferated, entrenched, and poorly engineered. On top of this, attackers are moving beyond crude blast-type weapons and developing more sophisticated attacks. In fact, what could be referred to as 'Precision Weapons' are emerging. The use of the nomenclature 'precision weapons' is not without controversy (what is?), but the weapons being seen in the attack space are much more precise than the launch-and-see-where-it-goes weapons of only a few years back. Stuxnet, for example, seems to have been aimed very deliberately at a specific set of SCADA systems used by the Iranians in their nuclear program, limiting damage in other locales (Matrosov et al 2011). Targeted Malicious Email (TME), also known more colloquially as spear-phishing, is an extremely sophisticated combination of social engineering and targeted attack (Amin 2011). Software is not the only vector being exploited: supply chains are at risk as more evidence of counterfeit hardware is discovered (ICE 2010, Hsu 2010), leading some to wonder what modifications (if any) have been made to hardware elements manufactured in unsupervised facilities.

To complicate things, cyber security is increasingly seen as elite task, the purview of those with specialized training, rather than everyone's job. This leads to systemic weaknesses in enterprises which then are easily

exploitable. This also leads to systems being built with little or no consideration for security engineering. Unfortunately, security is and always has been a pay now or pay later proposition and it seems like the pay later option is now coming home to roost. Besides the costs associated with patching the gaping holes in systems that leave enterprises vulnerable, a non-trivial expense, it is with some relief to the security community that the lawyers have (finally) arrived, both in the international policy arena and in the product liability arena (CCDCOE 2009, 2010; Meyer 2008).

There is a common element to this challenging set of circumstances. That is the element of knowledge. Knowledge is gained and used by attackers in order to develop and execute their actions. Knowledge is increasingly accessed in complex ways for good purposes, where "good" can be operationally defined as including such various legitimate purposes as developing market awareness, advertising, law enforcement, and intellectual property protection. The knowledge needed to safely and securely use information technology is ignored by vast numbers of users, some because they do not have the fundamental skills needed to use such knowledge, others because they are overwhelmed by the complexity of the situation. Finally, the knowledge of how to secure systems is implemented in isolated and sometimes stupid ways by 'security professionals'.

So we have in a very real sense a knowledge war underway, which is currently being lost by the good guys. An anecdote to describe how bad the situation is: at a conference of security professionals, an executive from a security services company was asked to define his top priorities. He said, "Cyrptography, Education, and Security." This is illustrative, in that most true security professionals consider cryptography to be an enabling technology for security, not something entirely separate. Unfortunately, this situation is not unique. The growth of the security certification market has led to an increase in those that are considered to be qualified to perform security services for the enterprise. Without naming names, it has been my distinctly unpleasant experience to discover, through classroom interactions, a disturbingly large number of students holding those certifications who do not understand some extremely fundamental concepts in cyber security. And yet these are the individuals we as a society trust to have the requisite knowledge needed to ensure a modicum of security in our systems.

What is All This Stuff?

It's complicated. Really, it is. Here is a brief review of all the material mentioned in the brief summary above for those readers who are not already intimately familiar with the referenced elements.

Stuxnet. First of all, it's a "worm." A worm is a category of malicious software (malware) that is self-replicating and mobile. In other words, it is capable of both reproducing itself and spreading the infection to other platforms. Next, researchers who have studied it carefully say that it appears to be specifically designed to go after software manufactured by Siemen's Corporation for use in their industrial control systems, specifically the supervisory control and data acquisition (SCADA) systems. The worm takes advantage of poor practices, as might be expected. After all, if someone leaves the front door open, why should a burglar bother to break in a window? In particular, the worm looked for default passwords in SCADA systems, used USB flash drives to spread itself, and exploited some Microsoft Windows vulnerabilities. Researchers estimated that the development of this worm must have required a sophisticated team of developers working several years with access to very specific testing environments. Many excellent analyses of the Stuxnet worm have been published. Two that are recommended to those who would like to research further are Matrosov et al 2011 and Schneier 2010.

Targeted Malicious Email (TME). Also known as spear-phishing, TME targets high value people specifically and believably in order to get the targets to take some sort of action, typically opening an infected attachment to an email. TME hijacks trusted relationships in order to effectively achieve the objectives of the attack. It is both very high impact and very difficult to detect, simply because of the nature of the attack. To illustrate the problem, consider the reaction of a senior executive for product development for a major software company

when she receives an email from the head of marketing for that same organization. Looking at the "From" line, the first reaction is that the email is legitimate. Now consider if the email "Subject" line contains the title of an on-going discussion between the two parties. This further emphasizes the legitimacy of the email. That is what TME looks like: a fully legitimate email that matches the current operational patterns extremely well. Then when the recipient opens the attachment to the email, surreptitiously added malware is executed on the targeted system. The purposes for TME can vary, but typical motivations are data exfiltration (stealing information) and sometimes data infiltration (opening backdoors into the greater network). In other words, espionage tends to be a prime motivation for TME.

Counterfeit Hardware. In the last five years, an increasing number of cases of counterfeit hardware have been discovered. One of the biggest cases was that of Cisco routers and network cards, which had been manufactured in China and provided to customers such as "U.S. Marine Corps, U.S. Air Force, FBI, BOP, Federal Aviation Administration, Department of Energy, as well as defense contractors, universities, school districts and financial institutions." (ICE 2010) What actual activities were going on in those systems, besides the legitimate activities, is anyone's guess: it is notoriously hard to detect activities that are surreptitious. Another case was that of counterfeit chips sold for use in missile systems: "…more than 59,000 counterfeit computer microchips from China to the U.S. Navy and other clients for military use aboard American warships, fighter planes, missile and antimissile systems." (Hsu 2010) It doesn't take much of an imagination to think of scenarios where being able to control the actions of an adversary's missile might be advantageous.

Cyber Security Elitism

In history, information security has long been held to be the responsibility of everyone. Rose Mary Sheldon, in her excellent book "Intelligence Activities in Ancient Rome", tells us of a Carthaginian ship captain who "deliberately drove his ship off course and into a shoal" in order to protect the secret of commercial interests of the state and was duly rewarded in return. (Sheldon 2005 pg 41) In World War II, citizens were admonished regularly that "loose lips sink ships," with the idea of reminding everyone that keeping secrets was everyone's job. (AdCouncil 2011)

The attitude that security is everyone's job is gone. This is partly because actually doing security well is time-consuming, boring, and detail oriented. The "Grandma problem" has long been a recognized challenge in security research, as has the "accidental help desk" phenomenon. The "Grandma problem" refers to the recognized challenges associated with elderly people not completely understanding new technologies. The "accidental help desk" phenomenon is reflected in the over-reliance in some workplaces on the one person who understands the technology. In the first case, Grandma suffers from diminished memory and needs to use easy to remember passwords, which are easy to crack, and never remembers to update her anti-virus software definitions. In the second case, the poor sap who is continually bugged by his colleagues to come fix their computers is rarely adequately trained but usually keeps the productivity at an acceptable level such that more professional help is avoidable, thus encouraging poor computing environments to flourish. In both cases, the situation opens the door to the rampant spread of malware. Because of the increasing interconnectedness of systems, these weak links endanger even the best protected systems, for example when the Grandson of Grandma brings an infected USB drive into work after visiting Grandma.

But beyond these two well-understood challenges, there is a more deeply seated attitude that information security is something that someone else does. It is not part of everyone's job description and increasingly employees expect that security is a service that is provided. As a result, poor security practices flourish. Employees looking to get their jobs done quickly find work-arounds for security controls, usually clueless as to how they are subverting their workplaces. Some real examples are described in the following paragraphs.

Example 1: I was invited to speak to a governmental advisory group. As part of the preparation, I was asked to send my personal information, including my social security number and other identifying information, to the staff who was coordinating the event. Despite the fact that the form on which I was to record this

information clearly stated "do not transmit this form through unsecured email," the staff asked that I send them the form via email. When I protested, they informed me that because their email address was on a dot mil branch of the internet, it was secure. It took several go rounds with the staff before I got them to realize that unless encryption was used, there was absolutely no security in the transmission.

Example 2: A civilian employee of the US Department of Defense was ordered to travel to Kuwait. The US Army staff in Kuwait requested that he send an extraordinary amount of personally identifying information to them prior to his arrival. Why they needed or wanted this information is a mystery that has not yet been solved. Why they were willing to accept custodial responsibility for this information is an additional mystery. But they wanted it and they wanted it emailed to them. When the employee protested, the Army staff in Kuwait assured him that it was perfectly secure, since the information would be stored in pdf file format. It is not clear whether or not they ever got the message that sending information in plain text was not a great security solution. Luckily for the employee, the trip was cancelled and his information was not subjected to this incredible situation.

Example 3: An employee of a small company providing services to the US Department of Energy was required to use hardware encryption products in his network in order to establish secure communications with the DOE lab he was supporting. Despite the fact that the crypto card was in a folder that was marked in big red letters "Do Not Send Through Inter Office Mail," the card was sent to the contractor through inter-office mail, subject to who knows whose inspection and perhaps modification.

These situations seem incredible, but they are all true. The pervasive lack of personal responsibility for even the most mundane security elements of a job subverts all other security efforts. This must change if the security situation is ever to be made better. Somehow, security needs to be everyone's job, not just the job of the geek down the hall.

Systems Development

To exacerbate this situation, systems are being built with no security engineering whatsoever. Nancy R. Mead from Carnegie Mellon University, who has been following this problem for many years, succinctly writes:

> When security requirements are considered, they are often developed independently of other requirements engineering activities. As a result, specific security requirements are often neglected, and functional requirements are specified in blissful ignorance of security aspects. In reviewing requirements documents, we typically find that security requirements, when they exist, are in a section by themselves and have been copied from a generic list of security features. The requirements elicitation and analysis that are needed to get a better set of security requirements seldom take place. (Mead 2010)

When systems are developed without taking security requirements into account, they by definition are vulnerable to mischief. Too often I hear from students and colleagues of security requirements, as poorly defined as they might be, being pushed from the development phase to the operations and maintenance phase, thereby almost guaranteeing they will never be funded or met. I also hear of security compliance monitors who view security as a box to be checked rather than a function to be tested, resulting in paper security rather than real security. Efforts to force more structure on the security community, such as Sarbanes-Oxley and FISMA, have resulted in the growth of entire industries helping clients achieve compliance with the letter of the law. Has security improved as a result? Possibly for some enterprises, but not for the cyberspace ecosystem as a whole, particularly when one considers the interaction of systems subject to compliance regulation and those that are not subject.

The Lawyers Have Arrived

That the legal community is beginning to be engaged is perceived as good news in a large portion of the security community. There are two ways that lawyers are starting to become engaged, and both are productive. First, in the realm of cyber-warfare, and, second, in the area of software utility.

In the realm of cyber-warfare, the lawyers are starting to understand and debate the geopolitical implications of multi-jurisdictional issues, such as attacks in cyberspace. The attacks on Estonia in 2007 got the attention of the legal community in a serious way, which the subsequent attacks on Georgia in 2008 solidified. There are active discussions and conferences being held to consider the laws of armed conflict and neutrality with regards to cyber-warfare and many, many lawyers are paying attention.

In the area of software utility, some legal scholars are starting to develop theories of negligence in information technology, something that the industry has fought long and hard to avoid. Dan Ryan in his paper "Product Liability for Security Software" (2003) discusses the fact that developers use contract disclaimers to protect themselves from liabilities associated with flawed software. It is no secret that software licenses typically contain declaimers that state that any problems with the software are not the fault of the developers and that the software is not warranted to actually work correctly. To the uninitiated, this is an amazing concept. To the security community, it is an infuriating concept. Typical language in a license agreement, chosen at random, is the following, including the capitalization:

> WARRANTY DISCLAIMER. WE DO NOT WARRANT THAT THIS SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE. TO THE EXTENT ALLOWED BY LAW, WE EXPRESSLY DISCLAIM ALL EXPRESS WARRANTIES NOT STATED HERE AND ALL IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. (Software Pursuits, 2010)

Product liability lawyers are paying attention and at least one case exists where a class action suit was successful against a software developer:

> April 2008: Court Approves Final Nationwide Settlement Against Sage Software. Meyer & Associates is pleased to announce the final approval of a nationwide settlement against Sage Software. Originally filed in 2005, the nationwide class action lawsuit claimed that the Defendant designed, manufactured, distributed and supplied defective ACT! 2005 software. (Meyer 2008)

This is a hopeful sign that perhaps pressure will be brought to bear on systems developers that they have a duty to design and build systems that are carefully constructed and tested, rather than developed at the speed of light using whatever talent happens to be at hand and be affordable.

The 600 pound gorilla in the room is the fact that information technology is increasingly embedded everywhere. It is in cars, from the ignition system to the brakes. It is in buildings, from the elevators to the locks. It is in airplanes, from fly-by-wire systems to navigation. It is in traffic systems, from lights to law enforcement. It is in power grids, from transmission to "smart" usage systems. What could possibly go wrong? Besides everything, that is. The systems are increasingly complex and increasingly tightly coupled. A problem in one area can quickly affect other areas. Should we not expect that our dependence on these systems be founded on some sort of assurance that adequate security is considered and included? In 1994, Peter G. Neumann brought attention to this very issue in his book, "Computer Related Risks." Charles Ashbacher captured the problem succinctly in his review, stating:

> Published in 1995 [sic], it was certainly an eye opener to the dangers of being lax in the use of computers. It was a bit scary when I read it, although at the time, I was optimistic that the danger could be managed.

> However, my position since then has changed in the negative sense. In rereading this book, it is clear that the dangers are the same and are greater in both breadth and depth. This book was written before the explosive growth of the Internet has turned nearly every computer into a potential node in an evil botnet. Also, the use of computers in the management of the modern world has dramatically expanded, increasing the possible ways in which danger can make an appearance.
>
> In looking through the risks, there is not a single one that has disappeared rather than increased in the level of the danger. Some examples are e-mail spoofs, insider misuse of data, denial of service attacks, threats to privacy, viruses and other malware, security vulnerabilities, computer errors in election results and financial fraud. And so it goes. If you are interested in looking back and seeing how little has changed in terms of the risks inherent with computer use, then read this book. It was and remains the original "canary in the coal" mine concerning the dangers that universal use of computers will generate. (Ashbacher 2008)

It is a fairly depressing situation to consider. And Ashbacher is absolutely correct to be depressed about the future. It's only going to get worse, particularly when you consider where we are going and the rate at which we are traveling.

Inside the Brain

News torn from the headlines: "Mind-reading Systems Could Change Air Security" (Tarm 2010).

> "The system … projects images onto airport screens, such as symbols associated with a certain terrorist group … The logic is that people can't help reacting, even if only subtly, to familiar images that suddenly appear in unfamiliar places. If you strolled through an airport and saw a picture of your mother, Givon explained, you couldn't help but respond."

Another headline: "'Mind-Reading' Technology Showcased in NYC: Intel Software Uses Brain Scans to Determine What Items People are Thinking About" (AP 2010). The title of the story is tantalizing enough, but deeper in the story was something even more intriguing (emphases added):

> "Other innovations on display … : Cell phone technology that would use motion, GPS and audio data gathered through users' cell phones to track what they're doing and who they're with. The technology can distinguish activities such as walking, giving a business presentation and driving. It also compares audio readings from different cell phones to determine who is in the same room. This would allow users to share their activity information with their close friends and watch avatar versions of their friends throughout the day. It would also let users track and analyze data about how they spend their time." (AP 2010)

These types of technologies may appear to be benign to the casual user, fun even, but when thrown into a system riddled with poorly designed and insecure components, the potential for disaster looms large. And that's even without a despotic government wishing to use these technologies to squash revolts or calls for reform.

Conclusions

What used to be considered to be secure, soon will not be. The way we think about computer security needs to change. It is critical that the security community embrace the non-technical aspects as part of the whole problem space if there is to be any hope whatsoever of successfully attacking the problem space. A focus on enterprise security goals rather than security technologies would be a good start -- when security is an

architectural goal, there is less temptation to try to bolt on exotic solutions focusing on tiny slivers of the technological challenge. Instead, holistic and synergistic solutions must be developed. It is increasingly important that we architect solutions that incorporate human brains, taking into account intellectual property and human inadvertent activity.

Cyber security needs to be everyone's job, not just the elite geeks (although they are very important!). System developers must be held to a reasonable standard of conduct that accounts for security. Systems operators and service providers must be held equally responsible. Until these things occur, no real progress will be made. Cyber security requirements must be included in all system development efforts, even the small ones given the weak link theory. This needs to be real security engineering, not just bandaids or menu driven options.

This is a 'systems' issue, not simply a computer science or technology issue, and must be approached as such, taking into account all elements, including people, processes, including mental, inputs, outputs, and interfaces using 'Systems of Systems' approaches. Until such overarching approaches are taken, no real solutions will be found.

References

[AdCouncil 2011] AdCouncil. Security of War Information - Loose Lips Sink Ships (1942-1945). Online Archives of the Advertising Council. http://www.adcouncil.org/default.aspx?id=127

[Amin 2011] Rohan Amin, Detecting Targeted Malicious Email Campaigns Through Supervised Classification of Persistent Threat and Recipient Oriented Features. PhD Dissertation, 2011: The George Washington University.

[AP 2010] AP News. "'Mind-Reading' Technology Showcased in NYC: Intel Software Uses Brain Scans to Determine What Items People are Thinking About" AP News, NEW YORK, April 8, 2010 http://www.cbsnews.com/stories/2010/04/08/tech/main6374956.shtml

[Ashbacher 2008] Charles Ashbacher. Review of "Computer Related Risks". Amazon.com reviews, June 12, 2008. http://www.amazon.com/Computer-Related-Risks-Peter-G-Neumann/dp/020155805X/ref=sr_1_1?ie=UTF8&qid=1302375174&sr=8-1

[CCDCOE 2009] NATO Cooperative Cyber Defense Center of Excellence, Cyber Conflict Legal and Policy Conference 2009. September 9-11, 2009, Tallinn, Estonia. http://www.ccdcoe.org/legalconference/

[CCDCOE 2010] NATO Cooperative Cyber Defense Center of Excellence, Conference on Cyber Conflict. June 15-18, 2010, Tallinn, Estonia. http://www.ccdcoe.org/conference2010/

[Hsu 2010] Spencer S. Hsu Case targets microchips sold to Navy. Washington Post: September 15, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/09/14/AR2010091406962.html

[ICE 2010] US Immigration and Customs Enforcement, News Release Sept 7, 2010: Texas man sentenced for selling counterfeit "Cisco" routers. Available online at http://www.ice.gov/news/releases/1009/100907houston.htm

[Matrosov et al 2011] Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, Stuxnet Under the Microscope. ESET Corporation White Papers, January 2011. http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

[Mead 2010] Nancy R. Mead. Security Requirements Engineering. Software Engineering Institute, Carnegie Mellon University. 2006-08-10; Updated 2010-07-14. Available from https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/requirements/243-BSI.html?layoutType=plain

[Meyer 2008] Meyer & Associates, News Release April 2008: Court Approves Final Nationwide Settlement Against Sage Software. http://www.dmlaws.com/ConsumerClassAction/ClientSuccesses.aspx#sage

[Neumann 1994] Peter G. Neumann. Computer Related Risks. Addison-Wesley, 1994.

[Ryan 2003] Daniel J. Ryan. Product Liability for Security Software. IEEE Security & Privacy, v. 1 n. 1, January 2003.

[Schneier 2010] Bruce Schneier, Stuxnet. http://www.schneier.com/blog/archives/2010/10/stuxnet.html

[Sheldon 2005] Rose Mary Sheldon. Intelligence Activities in Ancient Rome: Trust in the Gods, but Verify. New York, 2005: Routledge Publishing Group.

[Software Pursuits 2010] Software Pursuits. Software License Agreement, Revised: 2010-03-02. http://www.softwarepursuits.com/license.asp

[Tarm 2010] Michael Tarm "Mind-reading Systems Could Change Air Security", The Aurora Sentinel, Jan 8, 2010, http://www.aurorasentinel.com/news/national/article_c618daa2-06df-5391-8702-472af15e8b3e.html

[Ware 1970] Willis Ware, Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security; Rand Report R609-1, The RAND Corporation, Santa Monica, CA (Feb. 1970)

Ryan References of General Interest

Ryan, Julie J.C.H. and Daniel J. Ryan, "Performance Metrics for Information Security Risk Management," IEEE Security and Privacy, vol. 6 no. 5, Sep/Oct 2008, pp. 38-44.

Ryan, Julie J.C.H. and Daniel J. Ryan. "Expected Benefits of Information Security Investments," Computers and Security, Vol. 25, Issue 8. Amsterdam: Elsevier. Pages 579-588. (November 2006). (http://www.sciencedirect.com/science/article/B6V8G-4KXDR1G-1/2/f3dbf2660eab68ae4bf87dde49b7f687)

Ryan, Julie J.C.H. "Use of Information Sharing Between Government and Industry as a Weapon," Journal of Information Warfare 5 no 2 (2006): 1 – 10.

Ryan, Julie J.C.H. and Daniel J. Ryan. "Proportional Hazards in Information Security," Risk Analysis 25 no. 1 (February 2005): 141.

Ryan, Julie J.C.H. and Corey D. Schou. "On Security Education, Training and Certifications," Information Systems Control Journal 6 (2004): 27.

Ryan, Julie J.C.H. "Information Security Tools and Practices: What Works?" IEEE Transactions on Computers 53 no. 8 (August 2004): 1060.

Ryan, Julie J.C.H. "Architecting Information Assurance," Proceedings of the 23rd IEEE International Performance Computing and Communications Conference, Phoenix, Arizona. 2004. pg. 669.

Ryan, Julie J.C.H. "Teaching Information Security to Engineering Managers," Proceedings of the 33rd ASEE/IEEE Frontiers in Education Conference, Boulder, Colorado. November 2003.

Jefferson, Theresa I. and Julie J.C.H. Ryan. "A Comparative Analysis of Privacy Policies of Popular E-Businesses," Proceedings of the 2003 ASEM National Conference, St. Louis, MO.

Ryan, Julie J.C.H. and Theresa I. Jefferson. "The Use, Misuse and Abuse of Statistics in Information Security Research," Proceedings of the 2003 ASEM National Conference, St. Louis, MO.

Ryan, Julie J.C.H. "The Effect of Public Budgetary and Policy Decisions on Development of Trusted Systems," Proceedings of the 2002 ASEM National Conference, Tampa, Florida. pp. 130 – 134.

Ryan, Daniel J. and Julie J.C.H. Ryan. "Institutional and Professional Liability in Information Assurance Education," Proceedings of the 2002 IEEE Workshop on Information Assurance at the United States Military Academy, West Point, NY June 2002.

Deterrence of Cyber Attacks and U.S. National Security

Charles L. Glaser

Introduction

This paper draws on deterrence theory to analyze the challenges that the United States faces in deterring cyber attacks. It begins by briefly reviewing the basic logic of deterrence theory and relating it to the challenge posed by cyber attacks. The following section explores what is commonly viewed as the key problem in deterring cyber attacks—the "attribution problem," which arises when a state cannot determine who has attacked it and therefore cannot credibly threaten to respond. This paper suggests that this barrier to deterrence has been exaggerated, while acknowledging that it does create a number of dangers. The following two sections discuss deterrence of different types of cyber attacks—those designed to damage the U.S. economy and society, and those designed to weaken U.S. conventional military forces. The final section highlights a few points, including the need for the United States to design a clear declaratory policy that explains its cyber deterrence strategy and the importance of integrating deterrence into a multilayer policy designed to protect the United States from cyber attacks.

Deterrence basics

In broad terms, we can envision protecting the United States with three separable, but complementary, layers of capability. The first layer is deterrence—capabilities and policies design to convince an adversary not to launch a cyber attack. The second layer is defense—capabilities designed to reduce the effectiveness of the adversary's cyber attack. The third layer is reconstitution and robustness—capabilities designed to enable U.S. systems to continue functioning once they have suffered cyber damage and to enable the United States to restore and rebuild its cyber capabilities after they have been damaged.

These layers achieve their objectives in different ways. Deterrence influences the adversary's intentions, convincing an adversary not to attack; defense works against the adversary's capabilities, defeating attacks that the adversary launches; reconstitution and robustness reduce the implications of successful attacks by the adversary. The layers complement each other by making up for limitations in other layers. If deterrence were known to be perfect, defense and reconstitution would be unnecessary; similarly, if defense were perfect, deterrence and reconstitution would be unnecessary. But, when none of the layers is perfect, each contributes to a country's overall ability to protect itself. This paper focuses on deterrence, among other reasons because the effectiveness of the other layers hinges primarily on technical considerations.

Deterrence theory was developed in the 1950s and 1960s primarily to address the new strategic challenges posed by nuclear weapons. Since then scholars have explored deterrence of conventional attacks, the relationship between the credibility of various type of deterrence commitments, deterrence of terrorists, and a variety of additional extensions and applications.[1] Deterrence involves convincing an adversary not to take an action by leading the adversary to believe that the costs of pursuing the action will exceed its benefits. An attacker's basic deterrence calculus depends on four components: 1) the benefits of taking the action—the larger the benefits, the harder the adversary is to deter; 2) the probability of achieving the benefits—the higher the probability, the harder the adversary is to deter; 3) the costs the defender will impose if the adversary takes the action—the higher the costs, the more likely the adversary is to be deterred; and 4) the adversary's assessment of the probability that the defender will inflict these costs—the higher this probability, the more likely the adversary is to be deterred. This last factor—the probability that the defender will carry out its deterrent threat—is commonly termed the credibility of the threat and has often been one of the thorniest issues for strategists to deal with. When the expected costs of an attack exceed the expected benefits, an attacker will be deterred.

In terms of this these four components, deterrence is frequently divided into two types—deterrence by punishment and deterrence by denial. When relying on a strategy of deterrence by punishment, the United States threatens to inflict costs in retaliation for being attacked. The effectiveness of deterrence by punishment depends on both the size of the costs being threatened and the credibility of the threat. Credibility depends on both the ability to retaliate and the will to retaliate. The credibility of its nuclear threats was a major concern for the United States during the Cold War because the United States was defending allies—which it valued less than its own country and, therefore, was willing to run only smaller risks to protect—and was highly vulnerable to Soviet nuclear escalation. While there was no doubt about the U.S. ability to inflict massive retaliatory damage, many U.S. leaders worried about the effectiveness of the U.S. nuclear deterrent due to doubts about its credibility.

For analyzing a deterrence-by-punishment strategy for dealing with cyber attacks we will need to assess the credibility of U.S. threats for responding to cyber attacks. Here we flag three issues. First, the most commonly cited barrier to deterring cyber attacks is the "attribution problem": most analysts believe that the United States will have great difficulty determining who launched a cyber attack; if the United States is not confident about who launched an attack, then it may be unwilling to retaliate; an attacker that recognizes this problem will doubt the credibility of U.S. threats. Second, the credibility of U.S. threats will require the attacker to believe that the United States has the ability to retaliate. This could pose different challenges in the cyber realm than in the kinetic realm. The United States can demonstrate its conventional and nuclear capabilities by buying forces, testing these systems, and engaging in training and exercises, all of which are observable (to varying degrees) by its adversaries. In contrast, U.S. offensive cyber capabilities may be entirely invisible. In addition, they may be untested against adversary systems, leaving the adversary with some doubt about the effectiveness of U.S. capabilities. Third, the United States could threaten traditional kinetic attacks in response to a cyber attack, but this would likely raise different doubts about U.S. credibility. Among other things, it would reflect concerns about the appropriateness of escalating from cyber to kinetic attacks and concerns about the risks to the United States, because this escalation might lead the adversary to escalate to still higher levels of conflict.

Deterrence by denial works by a different logic: in this approach, the United States deploys capabilities to convince its adversary that the probability of its attack succeeding are low; this reduces the expected benefits of the attack and can therefore result in successful deterrence. We see here a close relationship between the defense layer and the deterrence layer: defensive cyber capabilities that the adversary believed would be effective can convince the adversary not to attack in the first place. Pure denial strategies have limitations: even if an adversary believes that its attack is unlikely to succeed, he may not be deterred if the costs of attacking are low. For example, some scholars have expressed concern about conventional military strategies that emphasize deterrence-by-denial, because the key costs for the adversary of launching an attack are limited to the potential loss of soldiers and military materiel. This criticism was leveled at NATO's conventional strategy during the Cold War.[2] The problem is almost certainly worse for deterrence of cyber attacks because attacking would be essentially costless.[3] A partial "solution" is to integrate denial and punishment strategies, combining the ability to defeat attack with the threat to retaliate.

Cyber deterrence and the attribution problem

Many experts are quite pessimistic about the feasibility of attribution. For example, William Lynn, the U.S. Deputy Secretary of Defense recently wrote, "The forensic work necessary to identify an attacker may take months, if identification is possible at all."[4] Richard Clarke reports that a leading group of cyber experts concluded that it is "fruitless" to try to attribute the source of cyber attacks.[5] This view, however, may exaggerate the attribution problem by overlooking either the purposes of the attacker or the scenario in which the attack occurs.[6]

A state that launches a "countervalue" attack against the United States' economic infrastructure, economy, and/or society is likely to have a political purpose. Possible purposes could include compelling the United

States to make political concessions during a crisis before a war starts, compelling the United States to stop fighting a war, and reducing the U.S. ability to fight a war by weakening its economy and industrial infrastructure. For these compellent threats to be effective, the state would have to make demands and spell out its threat. In addition, it would have to provide the United States with some confidence that attacks would stop if the United States meets that attacker's demands. These communication requirements would largely eliminate the attribution problem. For the scenario of attacking to weaken the U.S. ability to fight, the country the United States was fighting would be immediately identified as the likely suspect; the possibility that the United States would likely come to this conclusion could be sufficient to deter the adversary's cyber attack. Alternatively, the attacker might not be deterred because the costs of U.S. retaliation were not large compared to the costs of the on-going war; but in this case the failure of deterrence would not result from the attribution problem, but instead from the size of the retaliatory costs the United States was threatening.

Of course, actors that lack political objectives are not covered by this argument. Terrorist groups are therefore a natural concern, as they are often viewed as motivated simply by the desire to damage the United States. A very different perspective disagrees, however, arguing that terrorist groups, including al Qaeda, are motivated by political goals and use terror attacks as a means to achieve their political ends.[7] If this is the case, a terrorist group will find itself facing communication requirements that are not unlike those facing states. A terrorist group might be hard to deter by retaliation because there are not good targets to hit in retaliation, and almost certainly no important cyber targets, but again the difficulty of deterrence would not result from attribution problems, but the more familiar problem of threatening attacks that would inflict sufficiently high costs on a terrorist group. Another type of actor that might be of concern here are hackers who are motivated by the technical challenge of undermining U.S. cyber systems and not by political objectives.

The attribution issue for "counterforce" attacks—those directed against U.S. capabilities—is quite different, but may be even less of a problem than with countervalue attacks launched by states. This type of attack is most likely to occur during a crisis or war, with the adversary employing the cyber attack to gain a military advantage. Attribution will likely not be a problem, because the United States will know which state it is involved with in a conflict. This is not to say that deterring this type of attack will not be difficult; it might be for reasons other than attribution. This is a separate issue that we deal with briefly below.

All of this said, the difficulty of attribution does create a variety of potential dangers. One possibility is dangerous mischief: a third party—country, terrorist group, or hacker—could launch a cyber attack against the United States while it was involved in a crisis or war with another state. Based on the logic sketched above, this could lead to misattribution, because the United States' first inclination would likely be to attribute the attack to the country it was already fighting. Consequently, the third party could use such an attack to generate escalation in the on-going conflict, with the goal of increasing the damage that the United States and/or its adversary would suffer. Another problem is that the inability to attribute attacks undermines the U.S. ability to deter (and otherwise respond) to much lower level cyber attacks, including data stealing, espionage, and disruption of commerce. At a minimum, attribution would enable the United States to try to deter these types of attack by promising to pursue legal actions. But at least for the most part, these types of attacks do not threaten vital U.S. national security interests, so from a security perspective the attribution problem does not generate large risks.

Deterring coercive countervalue cyber attacks

A standard deterrent strategy for deterring countervalue attacks is to threaten similar damage in retaliation. In the nuclear realm, holding the adversary's cities hostage—that is, vulnerable to retaliation—is considered the basic requirement for deterring the attacks against one's own cities. The analogy in the cyber realm would be to threaten a cyber attack that would inflict comparable damage against the same type of targets that the adversary had attacked.

But this raises the question of whether the United States should rely on cyber retaliation to deter cyber attacks. Because deterrence works by threatening costs with sufficient credibility, not by threatening specific types of attacks, this type of retaliation-in-kind is not strictly necessary for deterrence to be effective. Instead, the United States could threaten to use conventional weapons to inflict damage in retaliation. If the United States wanted to make clear that it was attempting to inflict comparable damage (for example, to avoid further escalation), it could attack similar targets. For example, if the adversary's cyber attack had destroyed part of the U.S. electric grid, oil refineries, and/or pipelines, the United States could attack these infrastructure targets in retaliation. Alternatively, except when facing a major power, the United States could threaten to invade the attacker's country or impose a new regime, if the country launched a highly destructive cyber attack against the United States.[8] These costs would be very different from those imposed by the adversary's cyber attack, but there is no reason that the costs have to come in similar types for an adversary to be deterred.

Deciding whether to rely on cyber retaliation or alternative types of retaliation is a major project that is beyond the scope of this short paper. Here we offer a few brief comments that suggest directions for further analysis. First, traditional kinetic capabilities have the advantage of being relatively easy to demonstrate and observe. As noted above, this could add to the credibility of kinetic threats compared to cyber threats. Second, a related point is that the United States would likely have greater confidence in its kinetic capabilities than its offensive cyber capabilities, because it would have been unable to test the latter, at least not fully. Third, the impact of kinetic attacks is likely easier to anticipate than is the impact of cyber attacks. If the United States wants to inflict a given amount of damage—to avoid inappropriate escalation or even to signal its willingness to deescalate—then it would see advantages in attacks that would result in damage that was relatively easy to estimate in advance and that would be easy to evaluate once they had occurred. Experts worry that cyber attacks could result in large uncertainties, leaving both the attacker and the attacked unsure about how much damage had been inflicted.[9]

But the case here is not entirely one sided—cyber deterrent threats could also have some advantages. First, cyber retaliatory attacks might provide a clearer means of tacit bargaining: the adversary is more likely to recognize a cyber attack as retaliation for its own cyber attack. Second, and related, cyber retaliation-in-kind would have benefits if cyber attacks were understood to represent a threshold between levels of violence. In this case, if the United States prefers that a cyber conflict not escalate to conventional or nuclear war, respecting the cyber threshold would help to avoid escalation, while pursuing interwar deterrence.

Whatever type or types of attacks the United States decides should constitute its strategy for deterring countervalue cyber attacks, the United States should develop a declaratory policy that lays out how it will respond, and why. Deterrence depends on the adversary understanding the threatened consequences. Laying out ahead of time the type and spectrum of responses can help a state to clarify its threats and to develop its adversary's expectations. This will be especially important if the United States finds that it requires not only the ability to deter initial cyber attacks, but also a more complex deterrence strategy that would enable it to engage in limited cyber wars in which cyber attacks are used for bargaining. Developing a well designed declaratory policy will be particularly important if the United States decides to rely on non-cyber retaliation, or to complement cyber retaliation with conventional attacks.

Deterring counter-military cyber attacks

Deterring counter-military attacks presents a host of different issues. First, deterring cyber attacks in isolation is probably not the key to deterring this type of attack. Both the United States and its adversary are likely to consider counter-military cyber attacks to be part of their overall conventional fighting capability. Within types of weaponry and warfare, the United States has traditionally distinguished between conventional and nuclear warfare, and has also made distinctions concerning chemical and biological weapons. In terms of counter-military attacks, cyber attacks may well not be considered a different type of warfare. Instead, counter-military cyber attacks are more likely to be viewed as a component of conventional

warfare. This would be in line with current categorizations, which for example include electronic warfare assets as an element of conventional capabilities. Similarly, imagine a cyber attack that damaged U.S. command and control capabilities. Why should the United States' response to this attack, or its deterrent threat that is designed to prevent the attack, be different if the damage is done by a kinetic attack than by a cyber attack?

Second, if the preceding line of argument is correct, then the challenge the United States faces in deterring counter-military cyber attacks is to be able to deter the adversary's overall conventional attack, including the offensive cyber capabilities that would be a component of this attack. This overall deterrent will depend on relative U.S. cyber capabilities, including both its ability to defend against the adversary's cyber attacks and its ability to use offensive cyber attacks to weaken its adversary's overall conventional capability. But, deterrence will depend still more broadly on how U.S. conventional capabilities compare to its adversary's. The adversary could be deterred from launching a conventional attack, including its counter-military cyber component, if the United States has the ability to win a conventional conflict, even if its adversary enjoys a cyber advantage. And, more in line with standard worries, an adversary that enjoys a net advantage in counter-military cyber capabilities might not be deterred, even if U.S. conventional forces are otherwise clearly superior. In any event, the basic point here is that impact of cyber capabilities on deterrence has to be understood in terms of their net impact on U.S. overall conventional capabilities.

Third, counter-military cyber capabilities would likely increase states' uncertainty about their conventional capabilities, which could make failures of deterrence more likely. Theorists have argued that uncertainties about the outcome of a war are a fundamental source of bargaining and deterrence failures. Uncertainty about outcomes and, closely related, disagreements about the outcome of a war, can prevent states from reaching a political bargain that they prefer to war.[10] Therefore, if cyber capabilities are potent enough to significantly influence assessments of war outcomes, then the increased uncertainty they will introduce could make war more likely.

Concluding thoughts

Deterring cyber attacks may not be as difficult as the emerging conventional wisdom suggests. This is partly because the attribution problem may be less severe than is generally believed. Because states are driven by political motives, they will be unable to use countervalue cyber attacks to achieve their objectives without making known their identities. A state will also likely be able to identify the source of counter-military attacks because these attacks will be most important in the context of a conventional war.

To support its deterrence policy, the United States needs a clear declaratory policy that lays out its plans for responding to various types of attacks. If the United States plans to rely partly on kinetic attacks and conventional operations to deter certain categories of cyber attack, this should be spelled out to increase the probability that adversaries appreciate the breadth of the United States' cyber deterrence strategy.

Finally, because even a well designed deterrent policy could fail, the United States must pay attention to the other layers that can contribute to protecting it from cyber attacks—both defense, and reconstitution and robustness undoubtedly have important roles to play and contributions to make. In addition to the direct protection this capability can provide, they can also contribute to the U.S. ability to deter cyber attacks because asymmetries in the ability to inflict cyber damage, especially countervalue damage, could provide a state with bargaining advantages. Evaluating the proper balance between these three layers of protection promises to be a highly complex, technical and imprecise enterprise. The brief evaluation presented in this paper suggests that cyber deterrent capabilities and strategy are sufficiently promising that they should not be the neglected as United States develops an integrated policy for reducing the danger posed by cyber attacks.

References

[1] Key early works include Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961); and Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966). On deterrence before the nuclear age, see George H. Quester, *Deterrence Before Hiroshima* (New York: Wiley, 1966); on conventional deterrence see John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983); for a thoughtful review, see Robert Jervis, "Deterrence Theory Revisited," *World Politics*, Vol. 31, No. 2 (Jan. 1979), pp. 289-324. On applying established deterrence concepts to cyber deterrence, see Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in Committee on Deterring Cyberattacks, National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (2010), at http:''www.nap.edu/catalog/12997.html

[2] Samuel P. Huntington, "Conventional Deterrence and Conventional Retaliation in Europe," *International Security*, Vol. 8, No. 3 (Winter 1983-84), pp. 32-56.

[3] A possible cost is that the defender will learn about the attacker's offensive cyber capabilities, resulting in a significant diminution of its future offense cyber capabilities.

[4] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, No. 5 (September/October 2010), pp. 97-198.

[5] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), p. 132.

[6] For this perspective and some of the issues we raise below, see Richard L. Kugler, "Deterrence of Cyber Attacks," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, D.C.: National Defense University Press, 2009).

[7] See for example Robert Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York: Random House, 2005).

[8] The possibility of relying on threats of different types of costs inflicted by different means has been identified as an option for the United States in deterring biological attacks; see for example, Victor A. Utgoff, "Nuclear Weapons and the Deterrence of Biological and Chemical Warfare," Occasional Paper No. 36 (Washington, D.C.: Henry L. Stimson Center, October 1997).

[9] On this point and many related ones, see Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Arlington, VA: RAND, 2009), chap. Three.

[10] See for example, James D. Fearon, "Rationalist Explanations for War," *International Organization*, Vol. 39, No. 3 (1995), pp. 379-414; and Robert Powell, *In the Shadow of Power: States and Strategies in International Politics* (Princeton: Princeton University Press, 1999).

From Perfect Citizen to Naked Bodyscanners—When is Surveillance Reasonable?

Jeffrey Rosen

In July 2010, the Wall Street Journal reported that the federal government is launching "Perfect Citizen," a program designed to identify cyber assaults on critical infrastructure controlled by the private and public sectors, including the electricity grid. Run by the National Security Agency, the surveillance "would rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack."[1]

Defenders of Perfect Citizen say that it's necessary to subject the private sector to the same detection systems that could prevent cyber attacks that might bring the entire communications network to its knees. Critics say that by surveilling millions of private communications without a warrant, Private Citizen represents precisely the kind of general search that the framers of the Fourth Amendment to the Constitution meant to forbid.

Is Perfect Citizen a troubling and unconstitutional intrusion of military surveillance into domestic affairs, or is it a reasonable response to a grave security threat that only NSA can provide?

I'd like to argue that Perfect Citizen is an emblem for the difficulty of translating constitutional values in light of new technologies that ensure that the greatest threats to privacy in the twenty-first century will come not from the government acting alone, but from private companies, such as Internet Service Providers, Facebook, and Google, acting in conjunction with the government. I'd like to argue that in order to satisfy the Fourth Amendment, Perfect Citizen would have to be implemented with a series of privacy protections to guarantee its legality, to ensure that it focuses on detecting and preventing serious threats, not low level wrongdoing. Then I'd like to use those privacy protections as a model for regulating a range of surveillance technologies in the twenty-first century—from airport scanners to ubiquitous surveillance by GPS devices—in order to protect the constitutional values in the twenty-first century.

How does Perfect Citizen work? It appears to represent an extension into private networks of cyber attack detection and prevention systems currently in place on government computers. As Jack Goldsmith describes in a paper for the Brookings Project on Technology and the Constitution, the current intrusion detection system, known as EINSTEIN 2, is being supplanted by an intrusion prevention system, known as EINSTEIN 3, which will use sensors to detect malicious attacks on privately owned computer networks and Internet Service Providers to stop them in real time before they can reach government computers.[2]

Goldsmith imagines that Perfect Citizen might extend EINSTEIN throughout public and private computer networks, and that the government might require a threat detection system to monitor all communications, public and private, without a warrant. He imagines that Perfect Citizen might be expanded to allow NSA, in conjunction with private firms, "to (a) suck up and monitor the content of private Internet communications, (b) store those communications, at least temporarily, (c) trace the source of malicious agents in these communications all over the globe, including inside the United States, and (d) take steps to thwart malicious communications, even when they originate in or use computers in, the United States."[3]

Would such a system be legal under current law? In his Brookings paper, Goldsmith argues that an extension of Perfect Citizen along these lines would require Congressional authorization. But if Congress authorized the extension of Perfect Citizen, would it violate the Fourth Amendment? According to Goldsmith, "The Fourth

[1] http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html
[2] http://www.brookings.edu/~/media/Files/rc/papers/2010/1208_4th_amendment_goldsmith/1208_4th_amendment_goldsmith.pdf
[3] Ibid, p. 9.

Amendment might not be viewed today to permit the unfathomably massive copying, storage, and analysis of private communications." Courts have held that there is no reasonable expectation of privacy in this information, and thus that the government collection and analysis of such information does not implicate the Fourth Amendment, although it might have to be authorized by statute.

Goldsmith concludes that the collection (or copying) and analysis of bulk communication content is another matter, although some Courts might be inclined to approve it under two existing doctrines—the third party doctrine, which holds that when you disclose information to third parties you assume the risk that the information may be disclosed to the government; and the special needs doctrine, which makes an exception to the Fourth Amendment warrant requirement for reasonable governmental actions with a purpose that goes "beyond routine law enforcement." Still, to be reasonable under the totality of the circumstances, Goldsmith concludes that Perfect Citizen would have to be implemented with at least three privacy protecting mechanisms.

First, storage and viewing. The fact that the only extremely suspicious communications are viewed by human beings (rather than computers) increases the reasonableness of the program: courts have held that searches (like dog sniffs) that only reveal contraband and don't reveal innocent information are quintessentially reasonable.

Second, use restrictions. To ensure that only cyber threats are targeted, the government could place use restrictions on communications that contain malicious signatures, allowing them to be stopped or destroyed, but not introduced as evidence in unrelated cases that do not involve national security, computer related crimes, or especially serious crimes. For models of use restrictions, the government could look to the original title III of the crime control bill of 1968, which was originally limited to violent felonies, but as a result of mission creep has now been extended to non-violent felonies.

Third, minimization. Goldsmith suggests a variety of minimization procedures to ensure that communications that do not prove to be threatening are destroyed and that suspicious communications are examined in ways that reveal no more privacy than necessary to meet the threat.[4] A model here is the original Carnivore system, where data was traceable but not personally identifiable unless there was a high probability that it revealed a serious threat.

I'd like to argue that Goldsmith's model can be generalized to many of the surveillance technologies that have been proposed after 9/11. To the degree that they rely on suspicionless searches, all can be designed in ways that make them more or less reasonable, depending on the legal and technological constraints imposed on them, such as viewing, storage, minimization requirements, and restrictions.

Consider the body scanners recently deployed at American airports that have created a national uproar. Eight years ago, when officials in Orlando International Airport first began testing the millimeter wave body scanners that have now caused a national uproar, the designers of the scanners at Pacific Northwest Laboratories made clear that U.S. officials faced a choice. They could deploy "naked machines," that display graphic images of the human body, or they could deploy "blob machines," developed by the same researchers, that were just as effective at identifying contraband but scrambled images of the naked body into a nondescript blob.

Since both versions of the body scanner promise the same amount of security, any sane attempt to balance privacy and security would seem to favor the blob machines over the naked machines. That is what European governments chose. Most European airport authorities have declined to adopt body scanners at all, because of evidence that they are not effective at detecting low density contraband. However, the handful of European

[4] Ibid, pp. 15-16.

airports that have adopted body scanners, such as Schiphol airport in Amsterdam, have chosen the blob machine over the naked machine.

The Schiphol blob machines contain another important privacy protection—images cannot be stored and transmitted. These choices reflect principled opposition to the naked machines, voiced by European privacy commissioners, like Germany's Peter Schaar, who emphasized the importance of designing body scanners in ways that protect privacy. "So far I have not seen a machine that protects personal rights," Schaar said earlier this year.[5]

In the United States, the Department of Homeland Security (DHS) made a very different choice, deploying the use of body scanners without any opportunity for public comment, and then appearing surprised by the backlash. The U.S. has implemented naked machines, not blob machines, and DHS required vendors to offer machines that were capable of storing and transmitting images, although a DHS privacy analysis emphasized that DHS has chosen to disable this capability after it was revealed by a Freedom of Information Act suit by the Electronic Privacy Information Center.[6] The Chief Privacy Officer of DHS did not insist on the two privacy features that European regulators have found crucial—namely blobbed images and no storage capacity of the machines. If both of these features were mandatory, they would address many of the privacy concerns and would shore up the argument that the machines are not unreasonable strip searches prohibited by the Fourth Amendment.[7]

A range of other surveillance technologies might be reasonable or unreasonable depending on whether they were implemented with similar constraints—from warrantless 24/7 GPS searches placed secretly by the police under a suspect's car, to the warrantless data mining that hopes to identify suspicious patterns of behavior that might prevent terrorism.

The model for all of these acts of constitutional translation is the great prophet of the need for the Constitution to adapt in light of these new technologies: Louis Brandeis. In his visionary dissenting opinion in the Olmstead case (1928), Brandies objected that a majority of the Court had approved the warrantless wiretapping of a suspected bootlegger. As private life had begun to be conducted over the wires in the age of radio, Brandeis observed, telephone conversations contained even more intimate information than sealed letters, which the Supreme Court had held in the nineteenth century could not be opened without a warrant. To protect the same amount of privacy that the framers of the Fourth and Fifth Amendments intended to protect, Brandeis concluded, it had become necessary to translate those amendments into the twentieth century, extending them to prohibit warrantless searches and seizures of conversations over the wires, even if the invasions occurred without physical invasions.

In a remarkably prescient passage, Brandeis then looked forward to the age of cyberspace, predicting that technologies of surveillance were likely to progress far beyond wiretapping. "Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will enabled to expose to a jury the most intimate occurrences of the home," he wrote. In anticipation of those future innovations, Brandeis challenged his colleagues to translate the Constitution once again to take account of the new technologies, or else risk protecting less privacy and freedom in the twenty-first century than the framers of the Constitution expected in the eighteenth century.

In evaluating technologies from Perfect Citizen to the naked machines, Brandeis would never have tolerated arid abstractions about how we lose all expectations of privacy when we walk in public places, or enter the airport, to expose our data to third parties, which has the effect of giving citizens less privacy in the age of

[5] http://www.thelocal.de/national/20100105-24357.html
[6] http://epic.org/privacy/body_scanners/DHS_PIA_07_23_09.pdf
[7] For an argument that the naked machines are unconstitutional, see http://www.washingtonpost.com/wp-dyn/content/article/2010/11/24/AR2010112404510.html

cloud computing than they had during the founding era. Brandeis might hold instead, like some states, that government intrusions must be no greater than necessary, encouraging judges to balance the intrusiveness of the search against the seriousness of the crime being prevented, as juries used to do during the founding era. Perhaps he might attempt to define how much privacy citizens in a free society should be entitled to expect, regardless of society's expectations. What is clear is that Brandeis would have considered it a duty to actively engage in the project of constitutional translation in order to preserve the framers' values in a very different technological world. As Brandeis put it, "If we would guide by the light of reason, we must let our minds be bold."

Security and Privacy: Clinical Case Studies

Neal Sikka

While it may seem that physician ethics, morals, and commitment to the Hippocratic Oath should be the cornerstone of privacy in healthcare, the rapid reliance on technology in health care with widespread digitalization of health care data required the development of formal regulation. The Federal government recognized the need for strict, but flexible standards for privacy and security in health care through the 1996 Health Care Insurance Portability and Accountability Act (HIPAA). This document will discuss the key principles and applications of HIPAA, special topics as addressed by the Department of Health and Human Services (HHS), and breach as a driver to investments in technology.

The enactment of new HITECH rules since November 2009 have raised penalties for breach of personal health information (PHI) by covered entities to fines that range from $100 to $50,000 per individual patient violation. The financial impact that federal regulations related to health care privacy and security can have on an individual provider or hospital is obvious. However, from a patient perspective, they often do not recognize the investment and effort involved in maintaining their privacy and security. It is perceived that a patient just signs a sheet a paper that authorizes use of their information; but, there is little explanation around the details of the disclosures outlined in what seems to be complicated legalese.

HIPAA has two major elements: Privacy and Security. The privacy framework relates to how a covered entity (CE) discloses PHI and the individual patient's right to privacy. The CE should ensure that individual's PHI remains confidential, that the integrity of the PHI is maintained, and that the PHI is made available to those entities the individual has authorized disclosure. These three warrantees apply to any PHI that the CE creates, maintains, or transmits. The CE should also ensure that the individual has access to their PHI and that it will protect PHI from threats to patient privacy (1). The security framework is applied through three safeguards: administrative, technical, and physical.

The Privacy framework serves as the building blocks for security. Regulations, privacy principles, standards, and business needs are the very bottom layer (3). The next layer that builds upon those elements is the goals and objectives of the health care organization (3). These two layers must be viewed in the context of a risk assessment that is conducted when new business is initiated, new workflows are created, or at some regular interval (2,3).

The administrative block of the security framework is made up of elements such as data minimization, training, and auditing (3). The physical block includes elements such as secure use, transport and storage (3). Finally, the technical block is often considered encryption, but may also include new security solution technologies in software, hardware, and services (2,3).

The HIPAA privacy and security principles ensure certain rights for the patient and their health care information. First, patients have the right to correct an error in their medical record. Next, they should have access to their record within a reasonable amount of time and are able to make the determination of to whom their data can be disclosed. The covered entity is accountable to disclose your private medical data only to those you have authorized disclosure. The covered entity is also accountable to put in place security safeguards to protect patient PHI, as well as for auditing who has access to PHI, and reporting breaches of PHI. The covered entity has obligations to make notifications to the individual patient whose data was breached as well as report to HHS and potentially the media based on the number of records breached. A breach investigation may ensue and could incur financial penalties for the covered entity (2).

One of the key principles in health care privacy management is the "minimum necessary standard."

> *"The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose."(2)*

This wording is vague and flexible to allow for the ease and expediency often required to provide high quality clinical care, clinical information management, and medical billing. Especially in clinical care, the minimum necessary standard may not be applied, as in requests by a health care provider for treatment purposes.

Covered Entities

So, who are covered entities and who are not covered entities? There are essentially three buckets that covered entities fit into:

- Health Care Providers – Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing Homes, Pharmacies
- Health Plans - Health insurance companies, HMOs, Company health plans, Federal and State Health care programs
- Health care clearinghouse – Organizations that process or facilitate the process of nonstandard format health information into standard formats

Organizations that are not considered covered entities include: Life Insurance, Employers, Workers Compensation Carriers, Schools, Child Protective Services, Law Enforcement, and Municipal Offices. It is important to note that these types of organizations do not need follow HIPAA regulations. They may have their own internally developed privacy and security policies or may follow local or state guidelines (2).

Organizations that are covered entities must bear the burden of proof that they train their workforce on implemented policies and procedures as related to HIPAA regulations. They must also document and be able to provide an audit report of training for employees as well as user level access to PHI. The CE must be able to demonstrate that all appropriate notifications for breach were made or that no breach occurred (2).

To determine if an organization is a covered entity, use the decision trees available at https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf.

Business Associates

Business Associates (BA) perform functions or assist in functions or activities that involve the use of or disclosure of PHI for covered entities. A covered entity may utilize a BA to perform services such as claims processing, data analysis, utilization review, quality assurance, billing, benefit management, or practice management (2). Other activities performed by business associates for covered entities may be legal, actuarial, accounting, or consulting (2). Some examples of business associates may include electronic medical records vendors, companies sponsoring research, companies involved in innovation, product development and testing, or companies providing hosted video teleconferencing services for telemedicine.

HIPAA requires that a covered entity have a business associate agreement in place with companies who are BAs to ensure defined limits regarding how the BA is allowed to disclose PHI. The BA agreement should also describe the process for the BA to report to the covered entity any violations of the disclosure limitations (4).

Special Topics

Public Health

For the protection of the public health, HIPAA regulation may allow CEs to disclose PHI. The objective of these disclosures include preventing or controlling disease outbreaks, risk of injury, or disability to organizations such as the Center for Disease Control and Prevention (CDC) or state or local health departments. These disclosures may be necessary for controlling the spread of sexually transmitted diseases or in cases of child or elderly abuse or neglect. They may also help the Food and Drug Administration (FDA) determine risk from pharmaceuticals or medical devices. Work place disease surveillance also falls under disclosure related to public health (5).

Research

Medical research requires the approval of the Institutional Review Board (IRB). Studies with minimal risk and no PHI may be granted as expedited or waived studies, but most studies do require the study participants to grant informed consent. The informed consent document outlines the objectives of the study, what is entailed in the subject's participation, any anticipated risks of participation, and details about how the patient's confidential information will be protected. Investigators should ensure privacy and security of any records that have identifiable information. Research generally falls under the minimum necessary principle (6).

Emergency Preparedness

HIPAA regulations are designed to allow for access to information required to treat patients, as well as billing and operations, during a disaster. In fact, the Secretary of HHS can order a suspension of certain rules for specific entities during a national disaster declaration (7). For example, a master patient index of all patients in multiple hospitals within a geographic location may be kept secure and unavailable to each other hospital in a network. When a disaster meeting the requirements of established policy occurs, the designated individual can allow the master index to become available to all hospitals in the network to help separated family members determine if they should look for a loved one at another networked hospital.

Genetic Information

The Genetic Information Nondiscrimination Act (GINA) is designed to prohibit discrimination based on genetic information in health coverage as well as in employment. In general, genetic information is to be treated at PHI (8). This area is in its infancy and is yet to be fully defined.

Mobile Health

Mobile health refers to mobility in health care. This includes both mobile phone based applications as well as wireless devices in the hospital, clinic, or home. Increasing mobility in health care, especially the use of laptops, smart phones, and tablets, is associated with increased security risks. Management of portable devices provides challenges to the enterprise to manage data during loss or theft. Mobile data must also be encrypted on the device, during transmission, and in use. A challenge in the area of wireless devices includes the correct association of wireless devices with the correct patient. Health care organizations should make sure that the use of mobile devices occurs in the appropriate business case and with a well thought out risk assessment.

Personal Health Records (PHRs)

A Personal Health Record (PHR) is an individually controlled health record that allows the patient to manage and track their health as well as share their data with whom they want. Unfortunately, adoption of PHRs has been very slow, with less than 10% of patients reported using a PHR. Interestingly, HIPAA does not apply to PHRs that are not offered by covered entities. These PHRs are governed by the privacy policies of the entity that offers them, and potentially other state or local regulations. However, HIPAA regulations do apply to how a PHI held by a covered entity enters the PHR. This is probably why there are often multiple steps required by your provider to release records directly to populate a self standing PHR like Google Health or Microsoft Health Vault (9).

Breach

Breach is the impermissible disclosure of information by a covered entity or business associate which compromises the privacy and security of PHI. Breaches may be subject to notification requirements or financial penalties based on the type and extent of the breach (4).

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) has developed a Risk Assessment tool to determine if notification of a breach is required. A reportable breach is a disclosure of unsecured PHI that violates HIPAA privacy regulations. However, there are criteria that exempt a covered entity from having to report the breach. The first exemption is an unauthorized access of PHI by an employee of the covered entity that is performed in good faith and within the scope of their organizational role. The second exemption is the inadvertent disclosure of PHI to another authorized person in the covered entity that is not disclosed further. The third exemption pertains to unauthorized disclosure of PHI which realistically cannot be retained by the unauthorized person (10).

Breaches must be reported to individuals whose PHI has been disclosed, and in some cases to the Office or Civil Rights and the Secretary of HHS. Breaches involving more than 500 individuals must be reported to the media. The CE has the obligation to report breaches in a timely manner and cooperate with any investigations initiated by HHS (4).

Unauthorized disclosures of PHI are a significant problem for health care organizations. Between September 2009 and September 2010 there were 166 data breach incidents involving over 500 individuals (11). The total number of individuals involved with those breaches was 4,905,768 (11). The largest incident exposed 1,220,000 individuals (11).

The average organization cost for a breach increased almost ten percent from 2008 to 2010 to over $7.2 million. Similarly the average cost of breach per individual record cost health care organizations over $200, also about a ten percent increase from 2008 to 2010. The elements that are included in these costs are the lost business associated with loss of credibility, the post breach response, the notification expenses such as mailings, and the investment for detection and escalation (11).

Case Studies

Controlling access to online PHI through Medical Staff Portal

Challenge: A busy academic hospital that grows rapidly often acquires multiple clinical information systems that are forced to interface with each other. Physicians and other practitioners require access to each system and may have workflows that require access to multiple systems at the same time. In addition, practitioner responsibilities often require them to complete documentation or access clinical information at home and during off hours.

Solutions: The Hospital deployed for all providers a portal that houses all clinical applications. The portal uses a Citrix client to provide access to registered providers. The Hospital also implemented a single sign on program to limit loss of multiple passwords associated with numerous clinical information systems. The portal has allowed the Hospital to better control access to clinical systems outside of the hospital as well as improve the ability to audit use of remote access.

Controlling access to PHI in clinical area, specifically for research study recruitment

Challenge: An increase in the number of clinical research studies and the use of undergraduate students as research assistants for subject recruitment was perceived as a risk for a medium sized academic hospital. Students were enrolled at the affiliated University but still required a credentialing process to be able to be in the clinical area of the hospital and access clinical systems. The Hospital wants to meet IRB, HIPAA research regulations, and follow the minimum necessary principle.

Solutions: The Hospital developed tighter controls to manage research assistants and their association with specific research projects. Each provider conducting research is now tied directly to a specific IRB number. Each research assistant must meet certain HR requirements (i.e. vaccinations, drug screening) as well as go through HIPAA training at the Hospital. However, access to the EMR has been eliminated for the time being for all research assistants. The Hospital is exploring possibilities to create a server with a copy of the EMR data that is de-identified and updated in real time for research assistants to scan for possible study subjects.

Securing Mobile and Portable devices

Challenge: As a large multi-specialty academic medical practice, providers are often utilizing laptop computers and mobile devices in patient care and research related activities. Tracking, securing, and managing the numerous devices to mitigate loss, theft or other breach is important to the enterprise.

Solution: The medical practice has taken a number of steps to mitigate risk related to the increased use of portable and mobile devices. First, an email filter automatically selects outgoing email that may contain PHI and sends it through a secure portal. Second, the IT department has moved the EMR to be hosted on a Citrix thin client. Finally, IT has increased accountability and enforcement of laptop registration and remote controllers. Additionally, new policies have been implemented to scrub devices that have been used overseas for viruses and malware.

Health care trends and Risk Mitigation

Numerous factors are driving health care towards an increase in digitization of both data and workflows. Health care providers at all levels and in all roles are becoming more mobile. Electronic health information exchange, new care models, and changes in health policy are creating new challenges in maintaining privacy and security of health care information. It is clear that there is an increased risk, and increased costs associated with that risk, both with large business impacts (3).

Health care organizations are prioritizing risk mitigation efforts. Some areas of focus include ensuring that encryption of PHI occurs at rest, in transit, and in use. Administrators are enhancing efforts to improve compliance with privacy and security policy and procedure. IT departments are examining various hardware and software solutions to mitigate risk from theft and loss of portable and mobile devices such as virtualization, full disk encryption, and processor controls (3). Close collaboration with clinical information system vendors and third party technical solutions can lead to improvements in authentication procedures to access PHI. The near future will see the increased use of biometrics, RFID and other similar technologies.

Health care is rapidly changing. Many aspects of clinical practice, new business models, and evolving policy and regulation make the environment somewhat unpredictable. However, what is clear is the movement to digitization and mobility. These changes are sure to expose new vulnerabilities. Mitigating privacy and security risks requires a pro-active approach driven by high stake consequences associated with breach that can hurt patients, be expensive, and damage reputations.

References

[1] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. Accessed March 21, 2011.

[2] http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html. Accessed March 20, 2011.

[3] Houlding, D. "Healthcare Security and Privacy", presentation shared March 2011. Intel Corporation.

[4] Heide, C. "Breach Notification for Unsecured Protected Health Information" presentation May 11, 2010. Accessed online March 17, 2011 at http://csrc.nist.gov/news_events/HIPAA May2010_workshop/presentations/1-3a-breach-notification-heide-ocr.pdf. Office of Civil Rights, Department of Health and Human Services.

[5] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html. Accessed March 21, 2011.

[6] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html. Accessed March 21, 2011.

[7] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/index.html. Accessed March 21, 2011.

[8] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/genetic/index.html. Accessed March 21, 2011

[9] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf. Accessed March 22, 2011.

[10] *Preventing a Data Breach and Protecting Health Records*, Kaufman, Rossin & Co. White Paper 2011.

[11] *2010 Annual Study: U.S. Cost of a Data Breach* , The Ponemon Institute, March 2011.

Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives

Frederic Lemieux

Introduction

Computers are used to commit crime and are the target of crime every day. Besides the magnitude and scope of the threat, one of the greatest challenges in fighting computer crime resides in the fundamental nature of the computing world. Cyber space is dynamic and changes often at a rapid pace. A computer's increasing sophistication, in terms of power capacity and communication speed, increases the criminal opportunity for motivated offenders as well as the availability of suitable targets. Moreover, the worldwide computer network has transformed computer crime from a local problem to an international security issue.

Cyber threats are currently significant enough to become a national security priority in several western countries including the United States. In order to better understand the challenges that the United States' cyber infrastructures are facing, it is necessary to examine how government agencies are addressing the threats posed by those who perpetrate computer-based crimes and attacks. On one hand, we know that computer crimes are often a "hi-tech" version of more traditional crimes such as theft, espionage, sabotage, and fraud. On the other hand, the ramification of cyber crimes are so extensive and technologically complex that they require specific knowledge to better understand the evolving nature of the threats as well as the tactics and strategies to investigate them.

This report is an effort to better understand the investigative processes and strategies of three United States federal agencies as they pursue cyber criminals and attempt to neutralize cyber threats. Our study focuses on investigations conducted by the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), and the Air Force Office of Special Investigations (AFOSI). The main objectives of this research are to understand how these agencies define "success" and what investigative models they use to address computer crime.

More precisely, this research scrutinizes cyber investigation methods and practices and compares them to a traditional investigative model, namely intelligence-led policing (ILP). ILP refers to a managerial model developed in the United Kingdom in the late 1990s. This model emphasizes the targeting of prolific offenders in order to diminish both victimization and crime volume (Lemieux 2006; Ratcliffe 2008). ILP relies heavily on inter-agency cooperation and intelligence sharing in order to enhance proactive law enforcement operations. Leads, tips, and other information related to serious offenders and criminal organizations are all part of the intelligence gathering and sharing in this model. This report begins to explore the extent to which ILP is applied or applicable to cyber investigations for both law enforcement and national security capacities.

Characterizing the threat

Law enforcement and national security agencies are currently facing highly diversified cyber threats. For police services "cyber crime," "computer crime," "information technology crime," and "high-tech crime" usually fall within two major categories of offenses: (1) the computer is the target of the offense, and therefore attacks on network confidentiality, integrity and/or availability (i.e. unauthorized access to and illicit tampering with systems, programs or data) all fall into this category and (2) traditional offenses such as theft, fraud, and forgery that are committed with the assistance of or by means of computers, computer networks and related information and communications technology. This categorization is largely recognized by experts in the field and most government agencies.

According to the Federal Bureau of Investigation (FBI), cyber crime results in serious monetary loss and extensive fraud. In 2010, the FBI reported that a typical loss can range from $223.00 (credit card fraud) to $3,000.00 (check fraud) per complaint. The same year, the top cyber crime complaint categories were the following (FBI 2010):

- Non-delivery (paying for merchandise online, but not receiving it);
- Auction fraud;
- Debit/credit card fraud;
- Confidence fraud (also referred to as advance fee fraud);
- Computer fraud;
- Check fraud;
- Nigerian letter fraud;
- Identity theft;
- Financial institutions fraud.

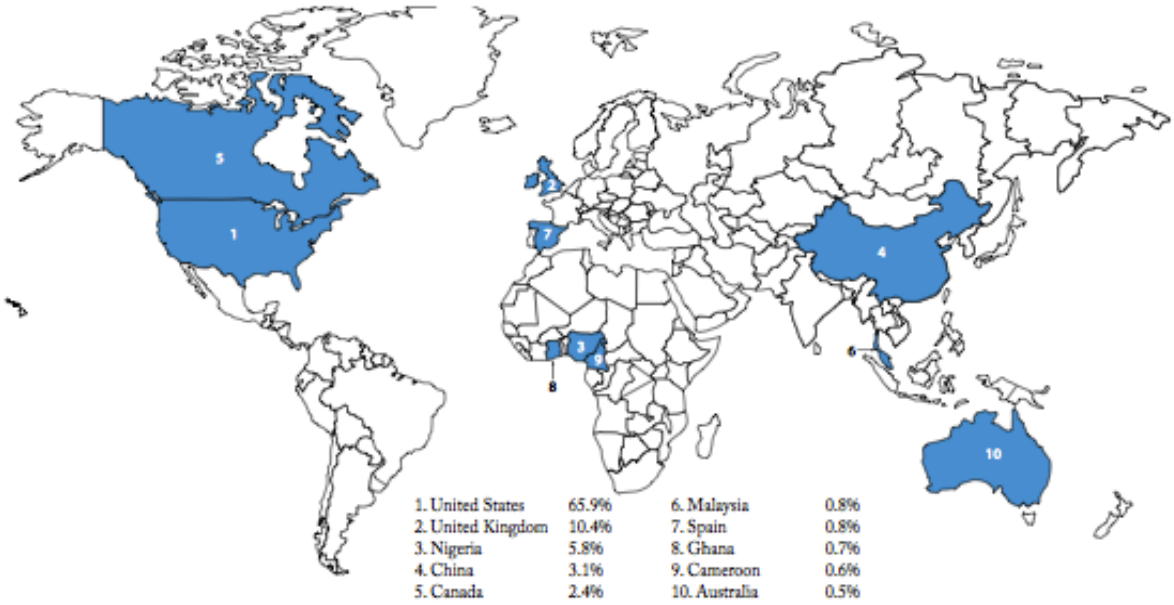
The existing literature on cyber crime investigation discusses the practical science of computer forensics at the technical level. Most of the writings in the field are intended for an audience already highly skilled in the use of computers. For example, Reyes' (2007) work addresses cyber crime from its technical beginnings, through the law enforcement role of pursuit and apprehension, to the final legal issue of prosecution. However, he does not delve into case management or the over-arching strategy of computer crime investigation. Mendell (2004) addresses computer crime investigations and forensics by examining the factors used in determining whether or not a given computer crime is "solvable." More precisely, this author explores the allocation of effort and resources in pursuing computer crime based on the probability of ultimately solving the crime. Mendell (2004) views computer crime investigation as a case by case approach, as opposed to presenting a cohesive model for understanding cyber crime investigation from a more strategic perspective.

When investigating cyber crime, law enforcement agencies face several challenges, including application of tactics, cooperation with concerned parties, and regularly operating between inconsistent legal frameworks in international investigations. The work of Hinduja (2007) addresses some key concepts to be aware of when examining the process of cyber investigations, such as the tactics of traditional crime and how they apply to computer crime. The author also discusses the necessity of outsourcing investigations to the private sector, as the ability to cooperate with private companies affects both the investigation process as well as outcome (success). In the same vein, Sussmann (1999) points out another critical factor in computer crime investigations: international cooperation. Many western countries may be at the forefront of computer crime forensics and investigations, but other nations may not, and cooperation with them is a critical and on-going challenge.

Kerr (2008) provides a valuable overview of recent cases in computer crime from a strictly legal standpoint. He outlines how the legal framework present in the United States allows for the prosecution of cyber crime, though this is not always the case in other countries. Figure 1 shows a worldwide distribution of origins of perpetrators and reflects the geographic challenges related to investigating computer crime.

Finally, funding presents a critical challenge for most law enforcement agencies. The size of a law enforcement agency's budget determines the number of agents it may employ and the amount of resources at its disposal. Investigation resources are always limited, in both the cyber and 'real' worlds, inevitably provoking a certain level of attrition in pursuits of particular cases. There is simply insufficient manpower and resources to adequately develop the skills of the workforce in charge of cyber crime investigation. Budget constraints and resource limitations are pervasive factors that heavily impact cyber crime investigation processes and tactics.

Figure 1: Origin of Computer Crime Perpetrators at the International Level (Source: Internet Crime Complaints Center, 2011)



Due to their importance within the realm of national security, crimes which target a computer system are of special interest to governments and private industries. The large quantity of classified information and data stored in government computers, as well as computer-dependent infrastructures within western countries represents critical political, economic, and security assets which require protection from attackers (state and non-state actors) both within and outside of a country. In retrospect, public awareness of the critical infrastructure and vulnerabilities of a computer network never fully developed until 1999 when Y2K became a front-page issue that highlighted society's dependence on computer systems for everything from ensuring prompt arrival of trains to protection of nuclear reactors.

Today, national security preoccupations are directed in part toward large scale cyber attacks which could target public and private computer infrastructures. However, according to Table 1, most cyber attacks are largely limited to denial of service attacks or incidents lacking long term impact (e.g. e-mail bombing or defacing of public domain websites). Most attacks perpetrated by state and non-state actors lack the capability to cause harm to a person, to damage property, or to incite fear in the general population. In most cases, damage has been limited to computer stations, websites, software, and email communications.

Table 1: Widely publicized breaches of national security and critical infrastructures

Year	Attacker	Target	Consequence
1982	United States - CIA	Logic bomb targeting USSR Siberian gas pipeline	Destruction
1999 & 2000	Russia	Pentagon, NASA, National Labs	Steeling information espionage
2004	China	Sandia National Laboratory, Lockheed Martin and NASA	Espionage
2007	China	U.S. computer networks (750,000 computers)	Denial of service
2007	Russia	Estonia's government web sites	Denial of service
2008	Unspecified	U.S. military network	Malicious code and zombie machines
2008	China and/or Russia	U.S. Presidential elections	Intrusion into email systems
2008	Russia	Georgia government and banking computer systems	Denial of service
2010	Unspecified	Iran uranium enrichment centrifuges	Sabotage
2010	Anonymous "Operation Avenge Assange"	Multiple western targets (public and private)	Denial of service

Despite warning signals from public and private sectors, doomsday and digital terrorist attacks have not yet caused the total collapse of western institutions. Nevertheless, threats of cyber warfare, virtual espionage, and "hacktivism" have materialized in the past two decades. Among the various challenges for national security practices, preventing and neutralizing attacks against the United States critical infrastructure at the hands of state and non-state actors is certainly a priority (NSCS, 2003). In that regard, Cavelty (2008) draws attention to the concern of adequately securing government and military systems as well as addressing vulnerabilities in critical infrastructures in the United States by scrutinizing the context of policy planning and international relations. Carr's (2010) examination of the concept of cyber warfare delves deeply into the vulnerabilities and political considerations of this new form of conflict (2010). Specifically, the author underscores the dangers related to cyber warfare and outlines future threats and cyber warfare strategies (prevention or defense). This work builds on previous assessments conducted by U.S. law enforcement agencies for internal purposes.

In 2005, the FBI published the results of its own computer crime survey. This exercise demonstrates the FBI's keen interest in preserving the security of the "nation's businesses." It provides a broad overview of the computer security problems facing U.S. businesses, how much financial damage these security breaches are causing, and the measures U.S. businesses are taking to protect themselves (FBI 2005). In addition to the 2005 survey conducted by the FBI, the Computer Security Institute (CSI) conducts a very thorough annual survey of the use of computer security software and the effects of computer crime in U.S. businesses (Peters 2009). More recently, 29 percent of respondents to a survey conducted by McAfee (2010) on worldwide prevalence of cyber attacks in critical infrastructures reported experiencing multiple large-scale denials of service attacks on a monthly basis with two thirds of those attacks impacting operations.

While there is an abundance of literature available on the subject of computer crime, very little is focused on maximizing efficiency in public agencies through analyzing current investigation models and strategies. Most of the research does not address the current state of computer crime investigation processes or how law enforcement and national security agencies work to effectively address cyber threats. Given that public authorities currently face a wide range of cyber threats, it's important to know: (a) the ways in which law

enforcement and national security agencies set investigation priorities; (b) the ways in which law enforcement and national security agencies achieve their organization objectives and goals throughout the investigation process; and (c) the operational definition of "success" as conceived by law enforcement and national security agencies.

Methods

This study employs primarily qualitative methods in research design and analysis. Document review served as the initial data collection tool. News stories taken from western media sources, reports produced by official agencies (including press releases), and public records of criminal cases reported by both law enforcement and national security agencies were reviewed for cyber investigation content. The information found in public reports and news media sources helped to identify specific cyber investigations and the corresponding federal agencies in charge of them. This data collection was useful in identifying the study participants (investigators) and preparing for interviews with them.

A second set of data was collected through semi-structured interviews with individuals employed by the Federal Bureau of Investigation (FBI), U.S. Secret Service (USSS), and Air Force Office of Special Investigations (AFOSI) who have extensive experience in cyber crime investigations. These organizations were purposely chosen for inclusion based on their responsibility for investigating cyber threats. Interviews were conducted with lead investigators (participants) and questions focused on the participants' professional backgrounds, points of view on how they measure success in their cyber-related investigative work, and their understanding of the differences/similarities between traditional crime investigations and cyber crime investigations.

In the United States, the FBI has investigative jurisdiction over all facets of computer crime. The Secret Service is also an important agency to include in the study due to their heavy involvement in financial crimes, a major subset of cyber crime. AFOSI was chosen as it was able to provide a distinctly different perspective, specifically that of internal counter-intelligence gathering from within the federal government. Though AFOSI is a federal law enforcement agency, its jurisdiction in law enforcement is limited to the Air Force and federal government agencies only. However, by playing a role of an insider in the US military apparatus, AFOSI facilitates computer counter-intelligence related to cyber threats. Consequently, this agency has a key role at the national security level.

Investigating cyber threats: preliminary findings

This section presents preliminary findings resulting from interviews conducted with cyber investigator participants working at the FBI, USSS, and AFOSI. More precisely, the analysis focuses on three key aspects explored during the interviews. Responses were examined as to the professional backgrounds of the participants and how those backgrounds do or do not shape investigation processes and tactics. The interviewees' responses were also culled for their perspectives on the investigation process, with particular emphasis placed on the starting point of the investigation, investigative discretionary power, and case attrition. Finally, this section reports the participants' responses regarding investigation outcomes.

Professional background, skills, and tactics

One of the interesting characteristics noted from our interviews is the fact that none of the individuals interviewed began their career as cyber investigators. In general, the participants have between seven and eleven years of experience in the field of cyber crime investigations, though all of them started as police officers. According to their responses, the skills acquired as a law enforcement officer are critical to their current work due to the feeling that the nature of the threats in the cyber space still requires traditional law enforcement tactics. According to the interviews, it seems that a background in traditional law enforcement,

combined with current work within the arena of national security, provides a valuable composite lens through which to recognize and negotiate the differences in the handling of traditional crime investigations and cyber crime investigations.

A finding reported by all interviewees was the necessity for traditional crime investigation techniques to remain an integral part of cyber crime investigations. Despite the technical nature of the crimes they are fighting, there is always a human element which is a major consideration in traditional crime solving. No matter how complicated and technological a computer crime may be, the perpetrator, the victim, and the investigator are still human.

Another reportedly critical aspect taken from traditional law enforcement techniques and featured in the response set is the ability to present investigative findings to a judge and/or jury. When a cyber-arrest is made and a prosecution begins, the preparation for court requires traditional tactics. The evidence and case against the accused needs to be presented in a form that anyone can understand and in a manner appropriate for a court of law. The members of the jury or the judge may not be as skilled in the realm of computers and information technology as the investigators are, making simplicity and clarity in presentation of evidence and investigative processes essential.

Investigation process

In a traditional investigation setting, it is widely understood that the solvability of a crime will be a critical element in the decision to conduct an in-depth investigation. Usually, the factors which determine the solvability of a case consist primarily of technical and physical evidence and other aspects such as the severity of potential damage or damage done. Though these investigative considerations are important in the case of cyber crime, they are not central. In fact, the two main considerations indicated by interview responses had to do primarily with threat elimination and the possibility of prosecution. Threat elimination relates to the level and scale of the crime itself, as well as the possibility of the investigation leading up the "chain of command" of a larger organization.

The possibility of prosecution refers to the decision of the Assistant to the U.S. Attorney in the relevant district "to be on board" with the cyber investigation case. U.S. Code, Title 18, Chapter 47, Section 1030 outlines the federal law regarding the amount of damage which must be done in order for federal prosecution to occur. This legal prerequisite represents a significant limitation to the investigative process and accounts for considerable case attrition in cyber investigations. If the loss is simply not great enough, a prosecution is not possible at the federal level. Even when the loss is sufficient for it to be considered a violation of federal law, the Assistant to the U.S. Attorney must be in agreement with the investigators to prosecute the case. According to the interview responses, if the cooperation between the investigators and U.S. Attorneys' offices is not established in the early stage of the investigation, much effort may be wasted.

In regards to the smaller cases of cyber crime, it appears that many cases which involve less damage are often left to local police to investigate and prosecute. However, not all smaller cases are left to the locals. For example the FBI may open a lower-order case if it is believed that the case will serve as the basis of an investigation into a larger organization. This notion ties in with the concept of threat elimination and its importance to federal investigators. The elimination of larger threats may begin at the lower levels, and the trail of investigations may lead the FBI or Secret Service up the ladder or hierarchy to a larger threat. The tactic of building an investigative ladder from the lower threats to the greater threats parallels the intelligence-led policing model. Interview responses point out that the cyber criminals that pose the greatest threat are often at the top of organizations which operate on an international scale. These top-level individuals present the opportunity for the largest amount of threat elimination through a single investigation.

In general, cyber investigations are handled on a case-by-case basis. According to the study participants, no two cases are approached exactly the same way. For example, AFOSI does not actively monitor systems in the Department of Defense (DoD), over which it has investigative jurisdiction. The investigation process begins when AFOSI receives specific requests from a federal agency, such as DoD. Once a request is received, AFOSI will begin to investigate the affected system and monitor it for continued breach attempts, if the system remains online. The FBI and Secret Service begin many investigations in a similar manner, through complaints or notification from private companies or government agencies. For all three agencies, the starting point of a cyber investigation is mainly reactive or in reaction to a complaint. This observation shows a critical departure from the ILP model which places an emphasis on proactive (rather than reactive) investigation initiatives.

Beyond the initial detection, cases evolve depending on the magnitude and nature of the threat detected. This is one of the core principles of combating high levels of cyber crime as reported in participant responses. A consistent reaction to the large number of cyber cases involving a lesser severity of damage was to not pursue the criminal at all. Rather, participants' responses representing all three agencies indicated that for crimes of a lesser degree, the reaction would be to simply strengthen the target, much like the problem-oriented policing in traditional crime. For AFOSI, this translates into making or advising changes in security measures or systems. For FBI and Secret Service, they each have established extensive partnerships with private businesses, especially large businesses and financial firms[1] allowing them to exchange information on threat patterns and crime prevention. Moreover, the Secret Service also benefits from partnerships with research institutions such Carnegie Mellon University and University of Tulsa[2].

Investigation outcomes

According to all the interviewees, the perception of success within their agencies was not solely oriented toward the arrest and prosecution of offenders. Statements made by individuals from all three agencies indicated an emphasis on the maximization of threat elimination with regards to cyber crime and counter-intelligence in the realm of national security. Threat elimination is very broad and encompasses a range of outcomes from efforts to single out ringleaders or more valuable targets, to strengthening potential targets in the private and government sectors. The definition of success in cyber crime investigations, as detailed in interview responses, revealed a policy and technique which mirrors the lessons learned from studying other strategic threats like organized crime and terrorism. In other words, when the success of an investigation is defined by the number of arrests and prosecutions, the likelihood of an investigator going after lesser offenders is greater, which results in a safer operating environment for the more dangerous and larger players in the cyber criminal world.

The participants' responses that emanated from a national security standpoint offer some different ideas of what success means. These responses reported the possibility of gaining counter-intelligence from a cyber threat as a measure of success in an investigation. When a system is infiltrated by a cyber criminal and it is determined to be a national security issue versus a criminal issue, then the possibility of a prosecution decreases significantly. In a national security matter, the priority becomes attribution, discovering the country or group the individual is from. If that can be done, then the presence and activity of the individual can be used as a valuable source of intelligence. As long as the value of the information gained outweighs the risks the intruder is causing, they may be allowed to continue their activities.

1 Interviewees specifically mentioned a critical collaborative effort established to protect these businesses: Infragard.

2 At Carnegie Mellon, Secret Service agents are embedded at the institution working with civilians conducting software engineering projects to further the development of the U.S. protective capabilities. At the University of Tulsa, a recognized 'center of excellence' by the Secret Service, agents collaborate with students and educators in efforts to further research on cell phone encryption systems.

Conclusion: Cyber investigation and intelligence-led policing

The federal government is currently planning to invest a vast amount of money and resources to protect public and private cyber infrastructures. Therefore, it becomes imperative to better understand the current and emerging investigation strategies and tactics that have proven effective in addressing this sort of crime. The potential for computer threats to do financial, and possibly even physical, damage has already materialized. In the face of such danger to the U.S. economy, public safety, and national security, it is crucial that the federal agencies protecting the country from cyber crime conduct their missions in the most efficient ways possible. This report presented preliminary findings to this end by identifying the basic measures of success and policing models currently in use by U.S. agencies. The identification of an element of intelligence-led policing in these models opens the door to further study into its effectiveness in investigating cyber crime.

During the interviews, participants described the top-down organization of computer crime on a world-wide scale. They made particular note of the relatively small number of hackers which are capable of the more damaging hacks and malicious programming, which involve only ten to twenty individuals at any given time. These high-level programmers maintain networks underneath them, keeping a strategic level of separation between the lower levels of the network and the top, thereby keeping the coders protected. Interviewees also mentioned that around ninety percent of major computer crime organizations take refuge overseas in order to avoid discovery and investigation. Cyber criminals seek out locations where they can operate with as little threat from the law as possible. One interviewee called individuals from Eastern Europe the current "masters of the universe" of computer crime. This global threat, similar to any other global threat, requires intelligence sharing and cooperation with foreign services to safeguard national critical infrastructures.

Despite the existing traces of intelligence collection and sharing combined with inter-jurisdictional collaboration, there is no evidence of a systematic application of an intelligence-led policing model to cyber investigation. This report has shown how the threat is characterized, highlighting the significance of its scope (national and international) and magnitude (volume and consequences). Despite the importance and the nature of the problem, which is comparable to the traditional threats of organized crime and terrorism to some extent, agencies addressing cyber threats seem to use a complaint-led model rather than an intelligence-led model. In addressing traditional serious crime, agencies having adopted ILP rely on both strategic and tactical assessments in order to prioritize threats and set investigation directions and requirements (Strang 2007). This differs from our participants' responses which indicate a reliance on national directives in order to prioritize threats.

Based on interview responses, it's unclear as to how much is done regarding the integration of local and regional agencies in the process of cyber investigations. For example, the "ladder" between federal and local agencies is not part of a systematic and procedural approach in cyber investigations, as it is in traditional investigations. The same observation can be made at the international level. Currently, it seems difficult for U.S. federal agencies to initiate international joint cyber investigations mainly due to the lack of harmonization in justice systems as well as varied levels of technological sophistication and investigative know-how (Lemieux 2008). Further study of the applicability of an ILP model to this type of investigative work may suggest ways for domestic and international police organizations to work around these barriers to cooperation in their mutual pursuit of cyber criminals.

Acknowledgments

I would like to acknowledge the research contributions of Brian Bales and Wilson Lee, two graduate students in the Master of Professional Studies in Security and Safety Leadership in the College of Professional Studies.

References

Carr, Jeffrey. Cyber Warfare. Sebastopol: O'Reilly, 2010.

Cavelty, Myriam. Cyber-Security and Threat Politics. New York: Routledge, 2008.

Federal Bureau of Investigation. "2005 FBI Computer Crime Survey. " (2006). Retrieved April 9, 2010 from http://www.digitalriver.com/v2.0img/operations/naievigi/site/media/pdf/FBIccs 2005.pdf.

Hinduja, Sameer. "Computer Crime Investigations in the United States: Leveraging knowledge from the Past to Address the Future." International Journal of Cyber Criminology. 1.1 (2007)

Internet Crime Complaint Center. 2010 Internet Crime Report. National White Collar Crime Center, 2011.

Kerr, Orin. Computer Crime Law. Eagan: Thomson-West, 2008.

Lemieux, Frederic. Information Technology in Criminal Intelligence Services: An International Comparative Perspective. In Leman-Langlois, S. (ed.) Technocrime. Columpton, UK: Willan Publishing, pp. 139-168, 2008.

Lemieux, Frederic. Normes et pratiques en matière de renseignements criminels : une comparaison internationale. Ste-Foy: Presses Universite Laval, 2006.

McAfee Labs. McAfee Threats Report: Third Quarter 2010. Santa Clara: McAfee Inc, 2010.

Mendell, Ronald. Investigating Computer Crime in the 21st Century. Springfield: Charles C. Thomas, 2004.

Peters, Sara. CSI Computer Crime and Security Survey. New York: Computer Security Institute, 2009.

Reyes, Anthony. Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors. Rockland: Syngress, 2007.

Strang, Steve. Project SLEIPNIR: An Analytical Technique for Operational Priority Setting. Ottawa: Royal Canadian Mounted Police, 2007.

Sussmann, Michael. "The Critical Challenges From International High-tech and Computer-related Crime at the Millennium." Duke Journal of Comparative & International Law. 9:451-490, 1999.

United States. Department of Homeland Security. "The National Strategy to Secure Cyberspace", February 2003, p.23 http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf, 10 Oct 2010.

United States. Department of Justice. Federal Bureau of Investigation."Cyber Division". http://www.fbijobs.gov/311132.asp, 23 March, 2010.

United States. Department of Justice. Federal Bureau of Investigation. "Cyber Crime". http://www.fbi.gov/about-us/investigate/cyber, 30 Oct 2010.

Healthcare Reform and Medical Data Security and Privacy

Patricia MacTaggart and Stephanie Fiore

Introduction

Health care delivery and administration are undergoing transformations that are dependent on and creating an expansive demand for health information technology (HIT). Evolving health delivery mechanisms include approaches beyond face-to-face encounters. Consumers and providers expect access to real time information at the point of clinical care. Administratively, payment methodologies demand consideration of demographics, use of quality metrics and reporting, and the use of performance incentives.

The need for clear guidance in health information technology is real. Decisions must be made balancing ease of use, privacy and security concerns of consumers/patients, practicality, costs and political will. The overall goal is finding the safest, most efficient methods for HIT implementation within an appropriate legal framework at the state and federal level.

Background

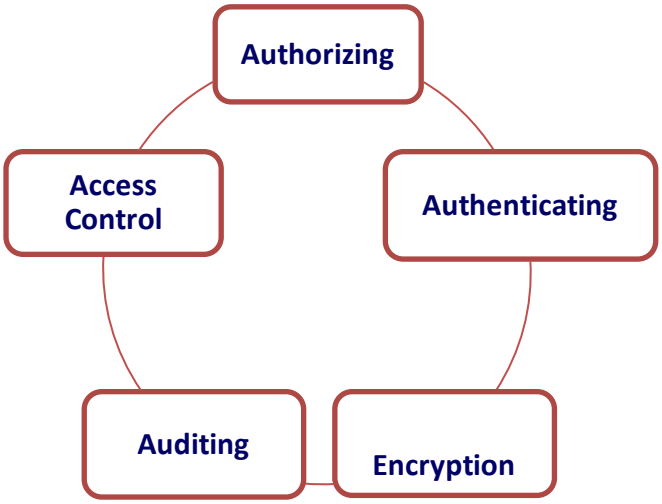
Health Information Technology is a "tool" to help providers, consumers, vendors, and stakeholders who are simultaneously entering this new and evolving environment. Consistency and collaboration between regulatory agencies, participants (physicians, other clinicians and patients), and stakeholders is necessary to fully utilize HIT to reach better health, better care, and lower costs.

One of the first steps is for patients and providers to understand the terminology of the changing HIT environment. Every day, new HIT terms and acronyms are created and their meanings change over time. For example, EHRs are electronic health records that go across health organizations, while EMRs are electronic medical records within one medical facility. More importantly, providers received "meaningful use" incentive payments for EHRs, but not EMRs. The American Recovery and Reinvestment Act[1] (ARRA) and the Affordable Care Act[2] created different forms of HIEs. ARRA HIEs are Health Information Exchanges, while Affordable Care Act HIEs are Health Insurance Exchanges.

HIT expands the potential for faster, safer movement of data, but also magnifies potential risks. HIT can enhance health data protection through encryption, role-based access and authentication when appropriately applied. E-Health information, absent of privacy and security safeguards, is at risk of disclosure through human error (laptop thefts and inadvertent data posting on the Internet) and disregard of personal information (breaches). The potential impact is not only invasion of privacy and finances, but also the risk of wrong medical decisions with life threatening results.

In response to the risks, security countermeasures to avoid or at least minimize security risks exist at various levels. They range from physical controls (locks on doors and computers) to administrative controls (staff security and privacy training) to technical controls (use of authentication and firewalls).

Figure 1: Security Controls



Key Critical Privacy and Security Policy Themes

There are numerous policy and operational issues related to privacy and security in the HIT area. Some are based on perceptions and others are based on reality, but to the consumer the impact is the same. Current key critical privacy and security themes are identified as follows:

Adequacy and Appropriateness of Current Privacy and Security Laws in an e-Health Environment

Privacy and security of health information is not a new set of concepts. Diverse federal and state laws and regulations exist that seek to address privacy and security, such as HIPAA Privacy and Security Rules, Privacy Act of 1974, 42 CFR Part 2: Confidentiality of Alcohol and Drug Abuse Patient Records Regulations,[3] Family Educational Rights and Privacy Act (FERPA),[4] Gramm-Leach-Bliley Financial Act,[5] Federal Information Security Management Act of 2002 (FISMA),[6] and Genetic Information Nondiscrimination Act of 2008 (GINA).[7] Policy makers must examine if current laws and regulations are still appropriate and necessary in an e-health environment. For example, 42 CFR Part 2 regulation related to confidentiality of alcohol and drug abuse patient records, was developed prior to a time when chemical dependency was considered a part of health care.

States and the federal government must also review their privacy and security laws to determine what is missing and what is no longer relevant because of the transformation of health care and evolution of HIT. Amendments may be necessary to accommodate changes that have resulted from the influx of HIT. A public demand for enforcement when breaches occur will dictate further development, clarification, and modifications to existing language. Two changes that have already had a significant positive impact are: 1) changes by DEA related to two-factor authentication for prescribing controlled substances that make e-prescribing more viable, and 2) Meaningful Use and Certification Criteria Stage 1 Privacy and Security measurements and provider attestation of a security risk assessment.

Consent

There are significant legal and consumer related considerations related to consent. The HIPAA Privacy Act[8] sets forth rules governing the use and disclosure of protected health information (PHI) by "covered entities" defined as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with a covered transaction, such as submitting a health care claim to a health plan.[9] HIPAA establishes the national minimum compliance framework, but states can and have expanded the legal provisions in areas of concern to their constituents. In addition, implementation and enforcement varies across states. Consent implementation issues relate to when and how often consent must be granted, the use of verbal or written consent, and the ability to consent to stay in (opt-out) rather than consent to stay out (opt-in). Legal requirements related to consent vary by the patient's age (adult or child), status (youth or emancipated adult), location of service (school or medical facility), type of service (behavioral health or substance use treatment), and purpose (secondary use of data or treatment). In addition, there are additional parameters related to disclosure and re-disclosure related to substance use treatment.

Implementation issues are complicated when certain services can be categorized different ways. For instance, pharmaceuticals used for behavioral health could be categorized as a pharmaceutical or a mental health service. The compliance requirements vary depending on the categorization.

Use of Data for Treatment

Data must be "near real-time," actionable, valid, and credible to be of value to providers. Data that does not easily and quickly provide accurate information has limited value. Factors that affect the transformation of data into practical information include the security of the data in storage and transmission, standardization of terminology and transmission, use of structured versus unstructured (free-text) data, access controls, and the potentiality of "gaps" in vital data because of legal or consumer barriers that may result in liability.

Use of Data beyond Treatment

While a breadth of patient concerns exist on the use of the data in the treatment of care, additional and broader concerns arise related to secondary use of data for functions other than clinical care. These include public health purposes, administrative functions, and quality improvement efforts. For example, access to eligibility and enrollment into public or private health care coverage is important for appropriate treatment and can decrease the administrative burden on consumers, but it can also be useful for focusing quality improvement efforts and measuring quality results. The existing policy issue is whether the data must be de-identified when used for a secondary purpose.

Identity Management

A sensitive privacy and security issue is the use of a unique patient identifier. Concerns range from increased patient privacy risks related to the ability to secure information about an individual, to fears of what it could lead to ("big brother effect"), to implementation related issues (connecting to existing records and cost when other alternatives might meet most of the needs). However, the cost of not implementing patient identifiers also has an impact as significant dollars and time are spent on identifying patients. It is a big expense to get accurate data to the provider at the right time, in a useable format, to assure efficient and effective health care delivery.

State Health Information Exchanges require a patient identifier for identity management. State Health Insurance Exchanges require the same, as do care providers. From an emergency room perspective,

information access saves money by reducing unnecessary testing and admissions, but more importantly, it helps physicians make improved decisions and save lives. Ensuring that accurate information about the specific individual is easily accessed is very important. This is a critical policy area where the solution is a balance between accessibility to critical information, while avoiding inappropriate access or use of personal information.

Operational Requirements

As with any new area of development, there are known requirements and unknown areas to explore. Providing quick and consistent guidance regarding operational requirements will make implementation and ongoing use feasible for large and small users alike. Security questions remain regarding strength of authentication; when, with whom, and how to use digital credentials, and types of transactions to be authenticated.

Critical to execution is intra- and inter- state consistency through mechanisms such as uniform laws, model acts, regulatory action, and reciprocity laws. One source for uniformity is the National Health Information Network (NHIN) DURSA agreement. The NHIN DURSA agreement provides standardized language related to responsibilities regarding privacy and security controls linked to malicious software, privacy and security rules, breach notification and action, oversight of technology, and compliance with laws.

Discussion

The technical architecture and capability to address privacy and security issues exists. The ability to segment and manage data is technically feasible; however, the demands on technology are complex, costly, and dependent on the granularity (consent by data type) required. For example, access controls can be based on different variables (user, role, location, and group) or be rule-based. The rule-based provides greater flexibility moving forward, but it also requires a complete understanding and agreement on the legal and policy framework, the technical and operational business rules and guidance, and sufficient human and financial resources to assure correct implementation and ongoing compliance.

Implementation demands the technical capacity to identify and separate sensitive health information, differentiate information according to type (HIV), data source (school), and patient. One of the most difficult, heterogeneous populations to address is adolescents. To assure adolescents' health care needs are not ignored or disenfranchised, the HIT infrastructure must have the ability to address variations in state laws regarding minor consent and definitions of "emancipated." The system must also segment adolescent health records to avoid unauthorized disclosure through tagging all data related to a procedure to which a minor has consented, recording the related minor consent status in a structured field, and transmitting minor consent status and information tags. To add to the complexity, providers serving teens in foster care may release "confidential" HIV-related information to an authorized foster care agency, without permission, but are not required to do so.[10] Foster care agencies, however, must release any HIV-related medical information of which they have knowledge to prospective foster or adoptive parents, but also safeguard this information from disclosure to others.

Conclusion

As HIT evolves and health care reform moves forward, decisions will need to be made on when to enforce existing or create new policies, especially those guiding privacy and security. Providers must adjust workflow related to obtaining and managing consent. Consumers and patients will need to understand the vast changes to their own health care delivery and administration, and conflicting interests will need to be balanced to get to a sustainable, reformed health care and information technology system. Throughout these advancements, patient privacy and security must remain at the forefront of every decision as they are essential to keeping the system credible, trusted, and operating.

References

[1] American Recovery and Reinvestment Act of 2009. (Public Law 111-5).

[2] Patient Protection and Affordable Care Act of 2010. (Public Law 111-148 & 111-152).

[3] 42 C.F.R. Part 2 (2009). These regulations were promulgated pursuant to the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Pub. Law 91-616, 84 Stat. 1848, and the Drug Abuse Office and Treatment Act of 1972, Pub L. No. 92-255, 86 Stat. 65. The rulemaking authority granted by both statutes relating to confidentiality of records can now be found at 42 U.S.C. § 290dd-2 (2006).

[4] The Family Educational Rights and Privacy Act (*FERPA)* of 1974 (20 U.S.C. § 1232g; 34 CFR Part 99).

[5] Gramm-Leach-Bliley Financial Modernization Act of 1999. (Public Law 106 – 102).

[6] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

[7] GINA §§ 102, 201, 203, 122 Stat. at 894, 908-909 (codified at 42 U.S.C.A. §§ 300gg-1, 2000ff-2 (West 2009)).

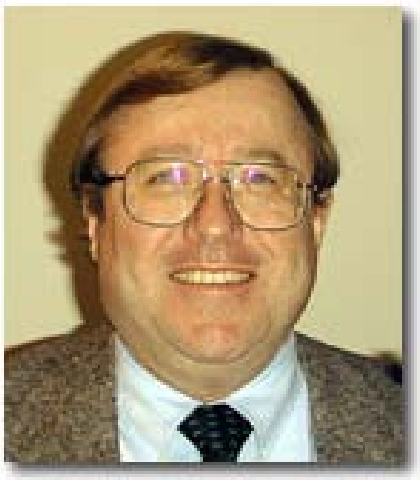
[8] Health Insurance Portability and Accountability Act of 1996. (Public Law 104-191).

[9] 45 C.F.R. § 160.103 (2009).

[10] http://www.five-rivers.org/privacy-policy.asp

Joseph J. Cordes

Columbian College of Arts and Sciences
Trachtenberg School of Public Policy and Public Administration
cordes@gwu.edu



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

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

Ross A. Lumley

School of Business
Information Systems and Technology Management Department
rlumley@gwu.edu

Dr. Ross Lumley is an Assistant Professor of Information Systems and Technology Management in the School of Business at The George Washington University. He received a Ph.D. in Management Science from the University of Texas at Dallas, a Master of Science in Management Science from the University of Texas at Dallas, and a Bachelor of Science in Electrical Engineering and Computer Science from the University of California at Berkeley. Dr. Lumley's forty years of experience in industry spans a wide variety of roles involving all aspects of information systems development as a developer, consultant, research fellow, and project manager. His areas of expertise are in security, performance engineering, enterprise architecture, advanced networking, mobile networking applications, large scale computing for Internet applications, virtualization, cloud computing, and virtual environments for collaboration. Dr. Lumley has published articles on performance engineering, high availability applications, areas of virtualization with open source technologies and building private cloud computing platforms directed toward the classroom and new paradigms in technology curriculum. Dr. Lumley has created the Cloud Computing Research Laboratory at The George Washington University Science and Technology campus in Ashburn, VA. He has presented his research outcomes in major regional, national, and international conferences.

Diana Burley

Graduate School of Education and Human Development
Department of Human and Organizational Learning
dburley@gwu.edu

Diana L. Burley is an Associate Professor in the Graduate School of Education and Human Development at The George Washington University. Dr. Burley joined GW in 2007 and during her tenure at the university she has served as the inaugural Department Chair of the Human and Organizational Learning Department and as Director of the Executive Leadership Doctoral Program. Prior to joining the GW faculty, she served as Program Officer in the Directorate for Education and Human Resources at the National Science Foundation (NSF). At NSF, she managed multi-million dollar grant programs designed to increase the capacity of the U.S. higher education enterprise to produce professionals in scientific fields. Her area of expertise at NSF was in computer science education. Based on her work, she was honored by the Federal Chief Information Officers Council and the Colloquium on Information Systems Security Education for outstanding efforts towards the development of the federal cyber security workforce. She currently serves as Vice Chair of the Association for Computing Machinery Special Interest Group on Computers and Society. Dr. Burley holds an M.S. in Management and Public Policy, an M.S. in Organization Science, and a Ph.D. in Organization Science and Information Technology from Carnegie Mellon University.

Julie J.C.H. Ryan

School of Engineering and Applied Science
Department of Engineering Management and Systems Engineering
jjchryan@gwu.edu

Julie J. C. H. Ryan is an Associate Professor and Chair of Engineering Management and Systems Engineering at George Washington University. She holds a B.S. degree from the U.S. Air Force Academy, M.L.S. in Technology from Eastern Michigan University, and D.Sc. in Engineering Management from the George Washington University. Dr. Ryan began her career as an Intelligence Officer, serving the U.S. Air Force and the U.S. Defense Intelligence Agency, focusing on communications and computer issues. She followed that service with a period of activity in industry, working for companies such as TRW and Booz-Allen & Hamilton. She has been in academia since 2001. Her areas of research interest are in information security and information warfare research. She was a member of the U.S. National Research Council's Naval Studies Board from 1995-1998 and currently sits on the Standing Committee for Technology Insight-Gauge, Evaluate & Review (TIGER). She is co-author of the book "Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves" (McGraw Hill 2000).

Charles L. Glaser

The Elliott School of International Affairs
Department of Political Science
cglaser@gwu.edu

Charles L. Glaser is a professor in the Elliott School of International Affairs and the Department of Political Science, and Director of the Elliott School's Institute for Security and Conflict Studies. His research focuses on international relations theory and international security policy. Professor Glaser's book, *Rational Theory of International Politics* was published by Princeton University Press in 2010. His research on international relations theory has focused on the security dilemma, defensive realism, the offense-defense balance, and arms races. His recent publications on U.S. nuclear weapons policy include "Counterforce Revisited" (with Steve Fetter) in *International Security* (2005), and "National Missile Defense and the Future of U.S. Nuclear Weapons Policy" (with Fetter) in *International Security* (2001). Professor Glaser's work on American Cold War nuclear weapons policy culminated in his book, *Analyzing Strategic Nuclear Policy* (Princeton 1990).

Professor Glaser holds a Ph.D. from the Kennedy School of Government at Harvard University. He received a B.S. in Physics from MIT, and an M.A. in Physics and an M.P.P. from Harvard. Before joining the George Washington University, Professor Glaser was the Emmett Dedmon Professor of Public Policy and Deputy Dean at the Harris School of Public Policy at the University of Chicago. He has also taught political science at the University of Michigan, was a visiting fellow at the Center for International Security and Cooperation at Stanford, served on the Joint Staff in the Pentagon, was a peace fellow at the United States Institute of Peace, and was a research associate at the Center of International Studies at MIT.

Jeffrey Rosen

The George Washington University Law School
jrosen@law.gwu.edu

Jeffrey Rosen is a professor of law at The George Washington University and the legal affairs editor of The New Republic. His most recent book is *The Supreme Court: The Personalities and Rivalries that Defined America*. He is also the author of *The Most Democratic Branch*, *The Naked Crowd*, and *The Unwanted Gaze*. Rosen is a graduate of Harvard College, summa cud laude; Oxford University, where he was a Marshall Scholar; and Yale Law School.

Professor Rosen's essays and commentaries have appeared in the New York Times Magazine, The Atlantic Monthly, on National Public Radio, and in The New Yorker, where he has been a staff writer. The Chicago Tribune named him one of the 10 best magazine journalists in America, and the L.A. Times called him, "the nation's most widely read and influential legal commentator." Professor Rosen lives in Washington, D.C. with his wife Christine and two sons.

Neal Sikka

School of Medicine and Health Sciences
Department of Emergency Medicine
nsikka@gwu.edu

Dr. Sikka is a Board Certified Emergency Physician at The George Washington University Hospital and Director of the Section of Innovative Practice at the GW Medical Faculty Associates. He serves as the Co-Director for both OnSite Medical Access and Global Health Services. He also oversees the GW Medical Transport Service and is the ED Information System Physician Application Manager.

Dr. Sikka has been a faculty member of the Department of Emergency Medicine since 2003 and is a Fellow of the American College of Emergency Physicians. His interests lie in medical informatics, telemedicine, mobile health, travel and tourism medicine, and innovative medical practice and design.

Frederic Lemieux

College of Professional Studies
flemieux@gwu.edu

Frederic Lemieux is an Associate Professor of Sociology and the Director of Police Science and Security & Safety Leadership Programs. He received his Ph.D. in criminology from the University of Montreal in 2002. Dr. Lemieux's research has focused upon social control and policing. He is currently conducting studies on transnational drug trafficking enforcement and the function of criminal intelligence as a formal social control tool. Dr. Lemieux has also published various journal articles examining crime control during major disasters, criminal intelligence agencies, and police cooperation. He has published four books, *Militarization of the Police Apparatus* (2005), *Norms and Practices in Criminal Intelligence: An International Comparison* (2006), *Homeland Security Handbook* (2007), and *International Police Cooperation: Emerging Issues, Theory and Practice* (2010).

Patricia MacTaggart

School of Public Health and Health Services
patricia.mactaggart@gwumc.edu

Patricia MacTaggart, M.B.A., M.M.A., is currently a Lead Research Scientist at The George Washington University (GW), where she instructs graduate students in health information technology (HIT) policy, quality and state health policy. She is also an Adjunct Associate Professor in the Department of Health Policy and Management at the University of North Carolina at Chapel Hill Gillings School of Global Public Health.

Ms. MacTaggart has been a public servant for almost 30 years including serving as Minnesota's Medicaid Director. She provides technical assistance to state and federal agencies regarding health information technology, quality and Medicaid/CHIP. Past president of HIMSS-NCA, she is a current member of the national HIMSS Public Policy Committee.

Stephanie Foire

School of Public Health and Health Services
sfiore@gwu.edu

Stephanie Fiore is a full time Research Assistant for The George Washington University Department of Health Policy. She is currently completing her M.S. Health Policy degree with a concentration in Health Information Technology. Presently, she is working on multiple projects which include creating a plan for the development and implementation of a health information exchange for the state of Alabama, building recommendations for the technical architecture of an HIT system for the state of California, and executing various initiatives relating to the HITECH Act and the Affordable Care Act.

About The George Washington University

Our University actively engages Washington, D.C., and the world. Our location in the heart of Washington places us at the core of U.S. government, policy, and law. We sit where the worlds of science, technology, media, and the arts converge. Our students and faculty have the unparalleled opportunity to study and work alongside leaders and practitioners in every discipline, to take part in the interchanges that shape our community and the world.

Our History—The George Washington University was created in 1821 through an Act of Congress, fulfilling George Washington's vision of an institution in the nation's capital dedicated to educating and preparing future leaders. Today, GW is the largest institution of higher education in the District of Columbia. We have more than 20,000 students—from all 50 states, the District, and more than 130 countries—studying a rich range of disciplines: from forensic science and creative writing to international affairs and computer engineering, as well as medicine, public health, the law and public policy. GW comprises three campuses—Foggy Bottom and Mount Vernon in Washington, D.C., and the GW Virginia Science and Technology Campus in Ashburn, Va.—as well as several graduate education centers in the metropolitan area and Hampton Roads, Va.

Our Commitment—Our mission is to provide an environment where knowledge is created and acquired and where creative endeavors seek to enrich the experiences of the global society. With ten schools and colleges and nearly 100 research centers and institutes, our students receive hands-on experience as they explore nearly any avenue of personal interest. The depth and breadth of our academic programs, the exceptional qualifications of our full-time faculty, the unmatched experiences of our adjunct faculty and the strengths of our research initiatives allow our students, our faculty and our staff to look at the world beyond the classroom. They allow us to prepare the next generation of leaders.

The George Washington University
2121 I Street NW
Washington, DC 20052
http://www.gwu.edu/
TEL (202) 994-1000

About the School of Engineering and Applied Science

GW's School of Engineering and Applied Science officially opened in 1884, as the first school of science and engineering in the District of Columbia. Originally known as the Corcoran Scientific School, the school focused on a limited range of engineering disciplines, granting degrees in civil, mechanical and mining engineering. However, the school rapidly grew, becoming The George Washington University School of Engineering in 1928. With the onset of WWII, the engineering school assumed an important role in educating young military officers and became a leader in rocket and ordnance research, In 1956, the school secured a building of its own—Tompkins Hall, equipped with modern mechanical, civil and electrical engineering laboratories, and in 1962, it acquired its current name—the School of Engineering and Applied Science.

Today, SEAS is home to undergraduate and graduate programs in biomedical engineering, civil and environmental engineering, computer science, electrical and computer engineering, engineering management and systems engineering, and mechanical and aerospace engineering. SEAS maintains several state-of-the-art research facilities, where our faculty and students work in partnership with public and private sector organizations. Targeted SEAS growth areas include nanotechnology, biometrics and bio-inspired engineering, high-performance computing, transportation safety, computer security and information assurance, and crisis, risk and knowledge management.

School of Engineering and Applied Science
725 23rd Street, NW
Washington, DC 20052
http://www.seas.gwu.edu/
TEL (202) 994-5613

About the Cyber Security Policy and Research Institute

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. CSPRI's mission is to encourage, promote, facilitate, and execute interdisciplinary research in these areas, including the exploration of the norms, governance issues, and operating systems of cyberspace.

Outside of GW, CSPRI works with government and private organizations to study the impact of rapid technological change on business, government, and the infrastructure security problems caused by the convergence of data and organizations in a networked world. It carries out studies and hosts seminars that move stakeholders towards rational and informed discussion of critical changes in communication, commerce, education, government, science, and entertainment facilitated by the Internet, a global venue that has blurred traditional political and organizational boundaries, made time zones irrelevant, and erased language barriers.

GW is federally designated as a National Center of Excellence in Information Assurance Education and as a National Center of Excellence in Information Assurance Research. CSPRI is the home for two major information assurance and computer security scholarship programs funded by the Defense Department, the Department of Homeland Security, and the National Science Foundation; since 2002 it has administered over $9 million in related grants.

Cyber Security Policy and Research Institute
707 22nd Street NW
Staughton Hall Room 304
Washington, DC 20052

TEL (202) 994-5613
EMAIL cspri@gwu.edu
http://www.cspri.seas.gwu.edu/