Systematic Approaches to Cyber Insecurity

Daniel Goldsmith, Michael Siegel
MIT Sloan School of Management[1]
NE25-773, 5 Cambridge Center, Cambridge, MA 02142
617-258-7459
goldsmith@mit.edu; msiegel@mit.edu

Abstract

Recent developments have demonstrated that as the diffusion of cyber enabled technologies increases, so too does dependency on a cyber infrastructure susceptible to failure, outages, and attacks. While current efforts are underway to introduce new methodologies and techniques to manage risks, particularly localized risks (such as those at a particular firm), developing resiliency at the system level requires transformative thinking to increase collaborative situational awareness, improve our understanding of risk, foster strategic coordination, and define actionable plans at the sector level to address pervasive sector-wide risk. The overall goal of this research is to develop innovative management and operational approaches using experts, emerging data sets, policy analysis, and relevant theory, along with simulation-modeling, to enable real-world implementation of high-leverage opportunities to promote corporate resiliency to cyber threats.

Introduction

The cyber domain is experiencing tremendous changes, presenting both opportunities and challenges to individuals, corporations, and nations.[2] While ubiquitous computing is increasing the numbers of participants and the quality of their interaction in cyberspace, nefarious actors and the security vulnerabilities that plague our cyber infrastructure present serious economic and national security challenge. Government and private sector networks and information are being exploited by an array of actors and corporate intellectual property is being stolen from a diverse range of sectors. Over the past several years, malicious activity has grown more serious and sophisticated, with many observers concerned of large scale attacks that have the potential to impact millions of users.

In this paper, we propose an integrative approach to address a subset (though one tightly connected to the whole) of security issues by describing challenge of strengthening corporate resiliency—the ability of individuals, firms, and sector-wide coordinating mechanisms to reduce susceptibility to cyber risk and increase the capability to manage persistent vulnerabilities. The appeal of resiliency challenges associated with cyberspace lies in harnessing new techniques to link observable patterns of nefarious system behavior (such as information theft, distribution, and denial) of a system to macro- and micro-level structure and decision-making processes that cut

[1] This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

[2] There are dozens of definitions of cyberspace but for our purposes “cyber” is a prefix for electronic and computer related activities.

across multiple disciplines. In other words, this research aims to be tightly grounded in observations of real world cyber venues, but also will be associated with multiple theoretical frameworks of actor and group behavior. This multi-level modeling approach incorporates complex interactions among different major actors and entities in order to advance new frameworks of computational thinking for cyber-complexity. We see this paper as the first step in a collaborative, cyber-relevant research program aimed at developing new tools and methods to identify, measure, interpret, and analyze the critical challenges, as well as new frameworks to formulate and evaluate technical and behavioral responses to a challenging threat environment. The need for such a program was recently reported in the *National Cyber Defense Financial Services Workshop Report*:

> "The group concluded that high-impact, large-scale attacks that target the entire sector are theoretically possible and under analyzed. A continuing dialogue on defending against such attacks and how to effectively address them in cooperation with government would be productive and useful. The group also concluded that **banking and finance sector problems are unique and important and require basic research in modeling and analyzing large-scale interdependent financial systems** and in constructing inherently recoverable distributed computation." (NCDFWP, 2009) –**emphasis added**

It is important to note that the scope of the cyber threat has escalated in recent years from isolated effects, such as data-breach at a firm, to scenarios that involve complex linkages of systems and actors. For example, regarding the financial services industry, the recent credit crisis—in which firms were unable to fund positions that were drastically dropping in value, resulting in margin calls and liquidity crises—provides a template for potential scenarios or attacks that threaten the industry. It is possible that certain threat actors could create scenarios leading to similar crises, by, for example, creating failed trades that could not be resolved in time, or by developing erroneous trades that would have to be unwound. This could lead to capital requirements and risk management exposures that would need to be funded and covered, and that could drive prices sharply in unfavorable directions. If the situation was allowed to "snowball," risk exposure spirals could begin to de-stabilize and create a lack of overall confidence in the markets. This example shows how emerging patterns of interdependent risk and cyber security challenges can threaten corporate and sector stability in new and unprecedented ways.

The expected long-term results of this research include capabilities for projecting systemic effects corporate practices in cyberspace; tools for cyber and real world data that enable better analysis of risk; enhanced knowledge of threat actors' capabilities, intentions and motivations; potential policy and coordinating mechanism for cyber defense; robust principles for sector governance; models of cyber attack escalation and de-escalation as a basis for deterrence strategies; and a greater understanding of how computational simulation modeling can help address cyber challenges

This approach will address significant policy, management, and technology challenges, including:

- How can we best utilize modeling techniques to prevent pervasive failure of firms?
- How can we incorporate a range a useful academic research into a coherent framework to apply to relevant cyber challenges?
- What are likely counter intuitive and second-order effects of current or proposed policies that might actually increase risk (examples might include cloud computing, standardization, and growing interdependency)?

Loads and Capabilities in the Cyber Domain

Large portions of the economy depend on a cyber infrastructure assembled from readily available commercial information system components governed by a variety of practices, standards, and regulations. Much of this infrastructure is organized to tolerate random events, such as individual attacks against specific institutions, but analysts agree that systems could potentially fail under concerted attack. While financial institutions, for example, have developed approaches to manage operation risk, industry and government officials are becoming increasingly concerned that new approaches are required to address cyber threats, particularly in regard to understand the interdependencies and strategies for mitigating risks. For example, despite organizations best efforts, current cyber risk management approaches have often failed to meet their objectives and even have the potential to make the situation worse. (Hathaway, 2008)

Advancing the state of the art in secure and resilient sector cyber configurations will require a holistic approach that taps a range of approaches to identify pitfalls and solutions. This approach can be envisioned as a scale, in which each discipline or practice can help contribute value to inform on system loads, those activities and practices that *increase* the burden and risk to the sector, and system capacities, which *decrease* the burden and risk. The output of this framing is a series of high-leverage recommendations that maximize the relevant academic contributions from diverse sources. A notional framing of this challenge is shown in Figure 1.

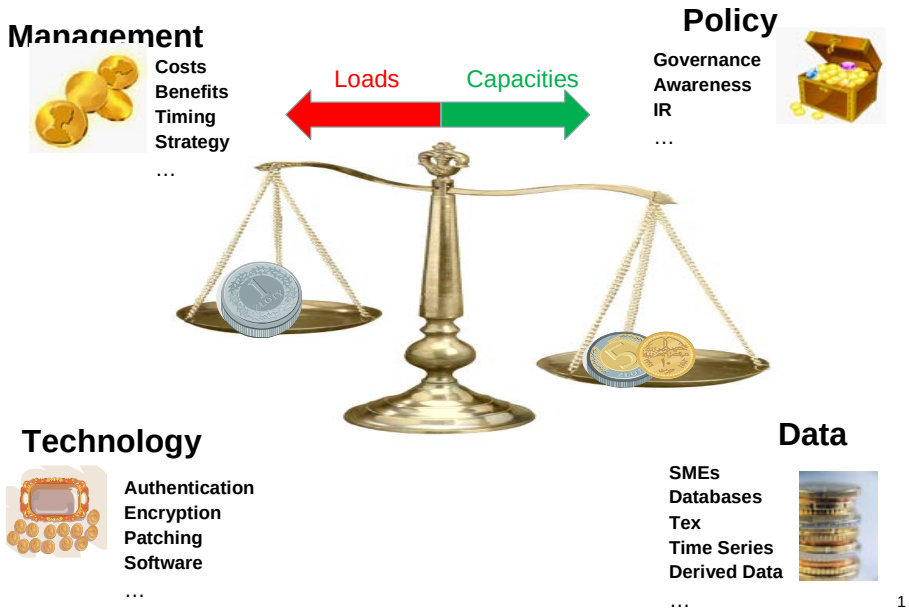

Figure 1: Holistic Framework for Interdisciplinary Approach

We highlight elements of this approach below:

- **Management**: The sector-wide management response to security threats has not kept pace with the sophistication and organization of those responsible for attacks. The United States lacks plans for the development of shared data on the frequency and severity of attacks. (The White House, 2009) One ramification of this is that

organizations that defend an attack do not share the knowledge of the attack, even though this knowledge could bolster the sector as a whole. Further, redundancy and waste occurs as each firm must individually develop and maintain security approaches.

- **Policy**: Designing an effective policy and legal responses to responding to cyber attacks presents enormous challenges. (Goldsmith & Wu, 2006) From a national policy framework, cyber challenges to the nation's economy are more urgent and difficult than ones presented by threats of nuclear, biological, and chemical weapons, yet the theoretical study of the policy and legal issues implicated by cyber attack is much less extensive and sophisticated than the theoretical study of these related threats. (Schmitt, 1999.)
- **Technology**: Software applications are complex, insecure, and can introduce vulnerabilities into a range of financial services operations. Patterns in acquisition requirements have shown preference for functionality and cost over security concerns. This has led to software development that neither focuses on nor supports security. Because financial institutions cannot be sure that their applications are 100 percent secure, they must develop and implement a range of technology approaches. (FSSCC, 2008)
- **Data**: Because of the interdisciplinary nature of cyber security, knowledge and relevant databases are often isolated and fragmented. We intend to harness datasets when available, such as CERT databases, FSTC and BITS collections, the National Vulnerability Database, and the MITRE dataset, among others, when available, In addition subject matter expert knowledge is required to be integrated to provide improved insights and understanding of challenges, threat, and opportunities. Data creating mechanisms, such as simulation modeling, are also helpful to link observable patterns of behavior of a system to macro- and micro-level structure and decision-making processes.

By harnessing work across these four areas, we seek to raise prominent challenges for cyber security, including:

- Improving data sharing across institutions
- Adopting industry wide metric, standards, and best practices
- Evaluating potential implications of technology shifts, such as cloud computing
- Addressing application and host security issues and potential compounding effects across the sector
- Understanding and addressing financial transaction system risk and resiliency
- Developing approaches to the human insider threat
- Improving the measurement of the value of security investments
- Understanding the state of security of critical suppliers
- Creating new security frameworks and "metaphors" to better communicate with users, administrators, and risk managers

A Framework for Cyber Security

We next provide a preliminary framework to address such a range of security issues. System dynamics has been used for a range of cyber security related issues, including user compliance (Dutta and Roy, 2008), insider threat (Rich, et al, 2005; Moore, et al, 2007), communicating information security practices (Hillen, Sveen, and Gonzalez, 2006). However, we explicitly drawn on and reframe previous modeling work in the health care sector, "Chronic illness in a complex health economy: the perils and promises of downstream and upstream reforms" by Jack Homer, Gary Hirsch, and Bobby Milstein, for our purposes. (Homer, Hirsch, and Milstein, 2007) We drawn upon this work for several reasons—just as the author's observe that "health care systems are organized in a way that makes them hard-pressed to respond to chronic illness," some cyber security experts believe that current wide-spread management practices are ineffective at dealing with persistent vulnerabilities. (Skoudis, 2009) In addition, the cyber domain similarly suffers from a misalignment of incentives and a lack of coordinating mechanisms to increase prevention (both at the host and network layers.) Therefore, we reframe the core of the stock and flow's from the chronic illness model into the cyber domain, as shown in Figure 2.

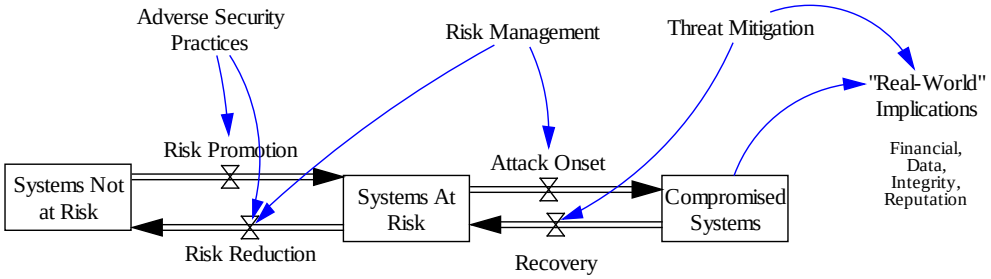

Figure 2: Stock and flow of cyber systems

The core of the model is the three stocks, which refer to different states of the sector's information technology infrastructure. These are: systems not at risk (those without identified attack vectors or in an otherwise secure state), systems at risk (those with identified risk vectors or zero-day exploits), and compromised systems (those existing with malicious code, such as malware.) The rate at which systems at risk change is controlled by a variety of security practices, including software choice, patching dynamics, user practices, and defensive routines. Once systems are at risk, they are susceptible to attacks resulting in infection, given different risk management practices. Compromised systems, if not mitigated, can lead to a range of adverse implications outside the computing domain, including financial, data, integrity, and reputation damages.

While data in the cyber domain is often difficult to measure and obtain, we can begin to overlay available data, such as the 2009 Verizon Data Breach Report, onto the key system variables. For example, in regards to the downstream flow of systems (the escalation of risk and infection), we find the following: a) regarding adverse security approaches, 67 percent of breaches were aided by significant errors (of the victim), b) regarding risk management, 64 percent resulted from hacking, and regarding threat management, 38 percent utilized malware. In sum, systems were

poorly handled, leading to increase risk exposure, were poorly managed, allowing hacking to occur, and once breached, allowed the injection of malicious code, increasing long-term threat.

We can use the same overlay on the upstream flows, the remediation of infection and reduction of risk. Regarding risk reduction, over 80 percent of the breaches had patches available for more than 1 year; regarding recovery, there was a 35 percent increase in the customization of Malware from 2007 to 2008, dramatically complicating recovery efforts; and regarding infected systems 75 percent of cases went undiscovered from weeks or months. In sum, systems were unnecessarily exposed to risk, faced growing complexity of attacks, and once infected were allowed to remain un-remediated, increasing the likelihood and severity of real-world loses.

We believe that this framework will show utility in the future as both a simulation model and as a method to integrate multiple perspectives. For example, from a management perspective, how can we best ensure compliance to existing security measures? From a policy perspective, how can we institute new methods of cost sharing or minimum levels of compliance? From a technology perspective, how can we use emerging technologies, such as the cloud, to reduce threat vectors? And from a data perspective, how can we better develop and implement metrics to improve understanding of performance?

Overlaying Dynamics

As an example using the core stock and flow structure above, we look at the key dynamics for cyber security of software patching (the installation of piece of software designed to fix problems or update a program. Traditionally, the patching problem, as viewed from the a vendor's perspective, was to determine the schedule to release patches to fix vulnerabilities in its software, while the problem from a firm's or user's perspective was how to update vulnerable systems with available patches. (Cavusoglu, Cavusoglu, Zhang, 2008) Patch management has been recognized as a crucial component of information security management, despite concerns about it implementation and effectiveness. As described in the Financial Services Sector Coordinating Council's 2008 Research and Development Committee's Report: "Information technology vulnerabilities emanate from two primary sources: (1) software flaws, and (2) inadequate patching and configuration practice."

Further, recent developments have put additional strains on the traditional patch cycle. When patches are released, nefarious actors work quickly to "reverse engineer" the patch and rapidly attack machines that are remain un-patched. Automated computer attack programs constantly search target networks, both on the Internet and on internal networks that attackers have already compromised, to search for systems configured with vulnerable software installed the way it was delivered from manufacturers and resellers. These default configurations are likely to be geared to ease-of-deployment and ease-of-use rather than security. (SANS, 2009) Once attackers have compromised systems, they can insert further malicious code and create "footholds," making it even harder to remove them from potentially sensitive systems. Therefore, in terms of system "loads" if software is not rapidly secured, the issuance of a patch can potentially worsen the overall security posture.

On the side favoring ‘capacities,’ certain interventions have the ability to lead to positive second-order effects that could further promote safety and stability. For example, in regards to patching, if machine configurations are standardized and tracked in a continuous manner, rapid patch deployment becomes possible, closing the window during which attacks can be launched. Once efforts to agree on standardized configurations are reached (such as efforts coordinated by MITRE regarding government configuration), firms within a sector could negotiate to buy systems configured securely out of the box using standardized images, which could be devised to avoid extraneous software, reducing the potential attack surface and the susceptibility to vulnerabilities. (Martin, 2005)

Below, we provide an example of patching dynamics by utilizing the framework to explain patching narratives. To do so, we add two new concepts: attacker capabilities and firm knowledge and awareness.

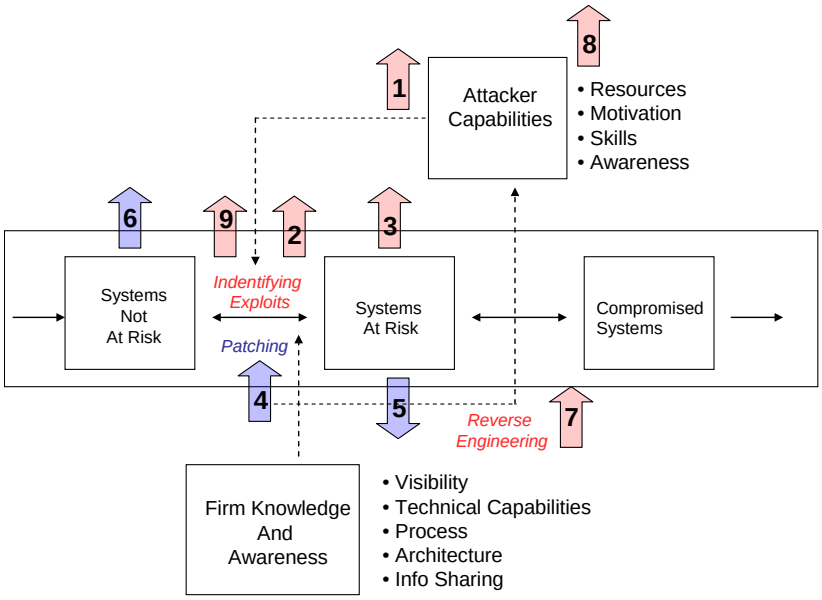

Figure 3: Patching Dynamics

As attacker capabilities increase (1), it is easier from these actors to develop and indentify exploits, new ways at putting systems at risk (2). Examples of exploits could include code vulnerabilities that enable sql injection or buffer overflows, increasing the stock of systems at risk (3). In response, a firm can patch these vulnerabilities, depending on firm knowledge and awareness (4) and the underlying availability of the patch (which we will assume for now.) This reduces the systems at risk (5) and increases secure systems (6). However, once the patch is realized, attackers can reveres engineer the patch (7) increasing their capability (8) and ultimately increasing the easy at identifying exploits (if the patch is not implemented rapidly.)

Next, we consider the additional downstream dynamics of the patching and exploit identification cycle.

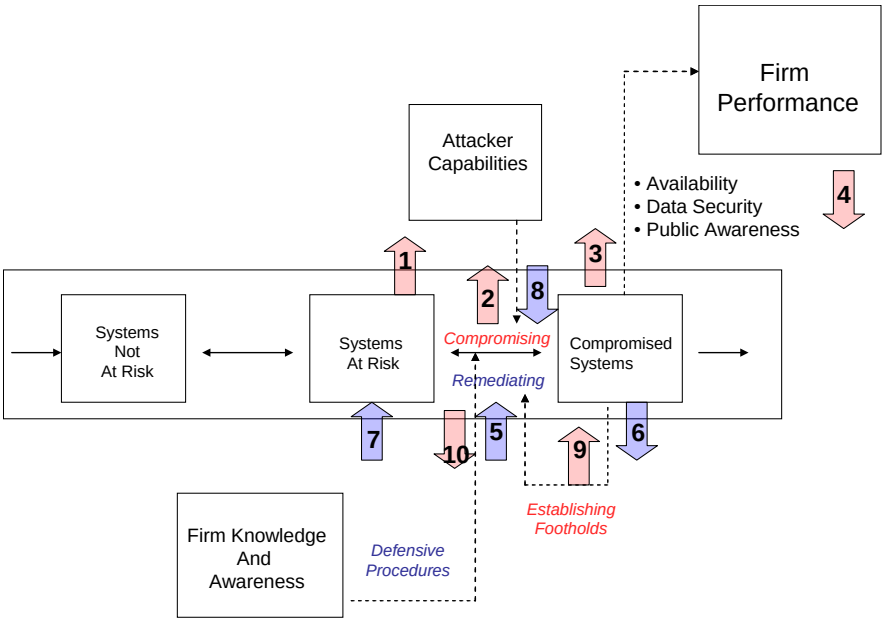

Figure 4: Downstream Dynamics

As the stock of systems at risk increases (1), compromising systems becomes easier (2), increasing the compromised system stock (3) and reducing firm performance (4). In response, firms can remediate (5) and reduce compromised systems (6), returning stems to a compromised (though potentially still at risk) state, and by identifying the attack vector making further compromising more difficult (8). However, if the firm does not act quickly, the attacker can establish footholds (9), making remediation much more difficult (10).

Finally, to briefly demonstrate these dynamics in a simulation we have initialized the three stocks (secure, vulnerable, and infected) to 100 percent base levels and have designed a series of simulation tests that mimic two real-world situations. (Figure 4) The blue line shows the initialized base case. The red and green lines show cases in which system vulnerabilities are introduced. These simulations can be thought of as recreating the Conficker worm, a computer worm first detected in 2008 which used flaws in the Windows operating system to co-opt machines.

In the red case, secure systems fail as more become vulnerable, but system security returns as firms are able to patch over time. This mimics a case in which industry relies on software that has latent security flaws, but is able to avoid infection by rapid patching and defensive routines taken by management to avoid infection. The green case has the same vulnerabilities introduced, but in this case industry is not able to rapidly address the vulnerable environment and a share of systems becomes infected.

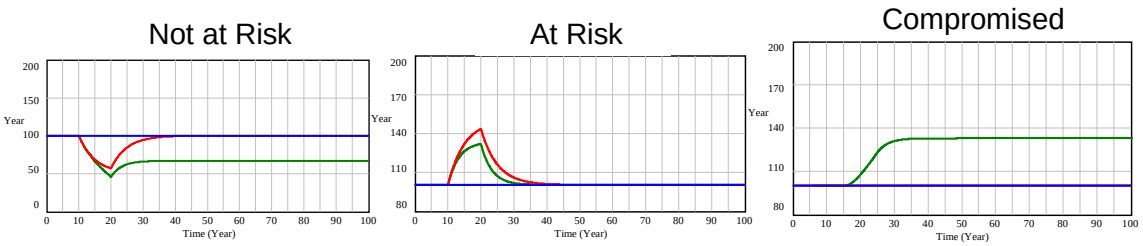

Figure 5. Simulation Output of Infection

Conclusion and Future Research Directions

Cyber security has been identified as one of the most pressing economic challenges of the 21st century, one that will require new thinking and collaboration to embrace solutions. We envision a unique approach to help advance knowledge and understanding of cyber related challenges, by a) developing creative simulation models and analytical frameworks to help address pressing cyber challenges in a holistic way, to ensure comprehensive solutions and broader impact; and b) reporting of salient and tangible financial services practices in cyberspace, such as: tools for cyber and real world data that enable better analysis of risk; enhanced knowledge of threat actors' capabilities, intentions and motivations; potential policy and coordinating mechanism for cyber defense; robust principles for sector governance; models of cyber conflict escalation and de-escalation as a basis for deterrence strategies; and a greater understanding of how computational simulation modeling can help address cyber challenges.

We believe the following steps will be helpful in addressing large-scale cyber challenges: 1) identifying and evaluating potential improvements (such as incentives for information sharing) and important areas of concern (such as interdependent risk) along with subject matter experts; 2) building formal simulation models for analysis and policy formulation; 3) testing the impacts of policy, management, and technology changes in low-cost modeling environments; and 4) engaging and reaching out to public, private, and academic audiences for the design and implementation of model-based strategies.

References

Cavusoglu H, Cavusoglu H, Zhang J. *Security patch management: share the burden or share the damage?* Management Science, 2008 54(4): 657–670.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, *Research Agenda for the Banking and Finance Sector*, September 2008

Goldsmith, J, and Wu, T. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press, 2006

Hathway, M. *Cyber Security: An Economic and National Security Crisis*. Intelligence Journal, Fall 2008, Vol 16, No. 2

Hillen S, Sveen FO, Gonzalez JJ.. Using dynamic stories to communicate information security. In Proceedings of the International System Dynamics Conference, Nijmegen. 2006.

Homer, Jack, Hirsch, Gary, and Milstein, Bobby. Chronic Illness in a Complex Health Economy: The Perils and Promises of Downstream and Upstream Reforms. System Dynamics Review 23, 313-343. 2007

Moulton, A., Madnick, S., and Siegel, M. *Context Interchange Mediation for Semantic Interoperability and Dynamic Integration of Autonomous Information Sources in the Fixed Income Securities Industry*. Proceedings of the Workshop on Information Technology and Systems (WITS), Barcelona, Spain, December 14-15, 2002 [CISL #2002-20]

Marshall, C and Siegel, M. *Value at Risk: Implementing a Risk Measurement*, Journal of Derivatives, Spring, 1997

Martin, B. *Transformational Vulnerability Management Through Standards*. The Journal of Defense Software Engineering, 2005.

Moore A, Cappelli D, Joseph H, Trzeciak R.. An experience using system dynamics to facilitate an insider threat workshop. In Proceedings of the International System Dynamics Conference, Boston, MA. 2007

National Cyber Defense Financial Services Workshop Report. *Helping Form a Sound Investment Strategy to Defend Against Strategic Attack on Financial Services*, October 23-29, 2009.

Rich E, Martinez-Moyano IJ, Conrad S, Cappelli DM, Moore AP, Shimeall TJ, Andersen DF, Gonzalez JJ, Ellison RJ, Lipson HF, Mundie DA, Sarriegui JM, Sawicka A, Stewart TR, Torres JM, Weaver EA, Wiik J. *Simulating insider cyber-threat risks: a model-based case and a case-based mode*l. In Proceedings of the International System Dynamics Conference, Boston, MA. 2005.

SANS. *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines*. 2009. http://www.sans.org/critical-security-controls/cag.pdf

Schmitt, J. *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*. Research Publications 1, Information Series, 1999.

Skoudis, Edward. *Information Security Issues in Cyberspace*, in Cyberpower and National Security. 2009

Sterman, J., N. Business Dynamics: Systems Thinking and Modeling for a Complex World. Chicago: McGraw-Hill/Irwin. 2000.

The White House, *Cyberspace Policy Review*, May 29, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Verizon Business RISK Team, 2009 Data Breach Investigations Report. 2009