Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Understanding Cyber Complexity: Systems Modeling and the Financial Services Sector

Daniel Goldsmith

Sloan School of Management
Massachusetts Institute of Technology

Michael Siegel

Sloan School of Management
Massachusetts Institute of Technology

February 2010

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Understanding Cyber Complexity: Systems Modeling and the Financial Services Sector
February 2010

Daniel Goldsmith and Michael Siegel
MIT Sloan School of Management

I. Introduction

Recent developments within the financial services sector 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 and emerging data sets available from the financial services industry along with simulation-driven technologies to enable real-world implementation of high-leverage opportunities to promote financial services resiliency.

The appeal of the analysis of sector resiliency challenges associated with cyberspace lies in harnessing new techniques to link observable patterns of behavior of a system to macro- and micro-level structure and decision-making processes that cut 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 while capturing non-linear causal relationships. By understanding how non-linear causal connections among actors create different propensities for risk and resiliency, we can advance new frameworks of computational thinking for cyber-complexity.

We have utilized *System Dynamics Modeling* (SDM), an approach for modeling and simulating complex physical and social systems. The core of the modeling strategy is to represent system structure in terms of stocks, flows, and the causal mechanisms that govern their rates of change. Feedback loops are the building blocks for articulating the causality represented in these models. In this domain, the interaction among the various modular sectors (*i.e.*, technical, social, economic, regulatory, and cultural) can be used to explain overall system behavior, such as identifying the sources and recognizing the evolution of cyber threats.

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

- How can we best utilize modeling techniques to prevent pervasive failure of the sector?
- 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)?

II. Research Description

This paper is the first step in a collaborative, cyber-relevant research program to investigate the threats and opportunities arising in the financial services industry. The program derives from the need for new tools and methods to identify, measure, interpret, and analyze the critical challenges facing the industry and new frameworks to formulate and evaluate technical and behavioral responses. As reported in the recent *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**

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 funding 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 one example shows how interdependent risk and cyber security challenges can threat industry stability in new and unprecedented ways.

Our prior research utilizing multi-methodology simulation modeling has been effective at addressing a variety of complex environments, including predicting and mitigating threats to country stability (Choucri, 2007; Morrison, 2008) and changing wide-scale operations in health care environments (Akiyama, 2007). The current and expected results of this research include capabilities for projecting systemic effects of financial services 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.

III. Exploiting Interdisciplinary Methodologies to Address Industry Challenges

Large portions of the financial services industry's functions 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 industry analysts agree that systems could fail under concerted attack. While financial

institutions 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. Previous research has examined financial services operations and risk from a variety of perspectives, including data integration and risk measurement. (Moulton, Madnick, and Siegel, 1998 & 2002; Marshall and Siegel, 1997)

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.

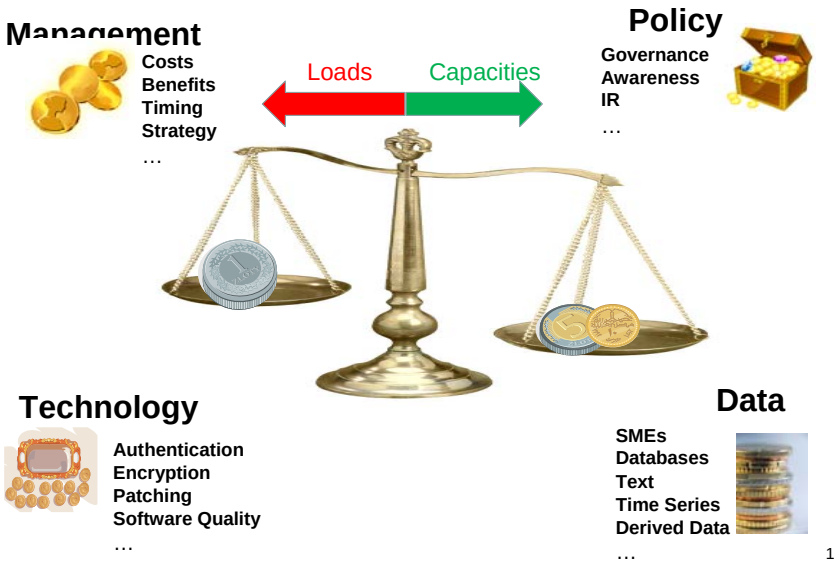

Figure 1: Holistic Framework for Interdisciplinary Approach

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 the financial services industry and investigates and aims to inform on specific industry topics include:

- 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

Further, we investigate the ways in which suggested policies interact with each other, as well as the surrounding environment, to control overall sector stability. For example, despite organizations best efforts, cyber risk management approaches have often failed to meet their objectives and even have the potential to make the situation worse. (Hathaway, 2008) The reason is that risk management efforts can lead to unintended consequences that subvert the original intentions of the effort: security and resiliency may fail to rise to any meaningful level, or they go up in the short term only to go back down in the long term.

An example of this dynamic concerns software patching; when patches (a piece of software designed to fix problems or update a program) 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, if systems are not rapidly secured, the issuance of a patch can potentially worsen the overall sector's security posture.

On the side favoring 'capacities,' certain interventions have the ability to lead to positive second-order effects that could further endogenously 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)

These two dynamics—system destabilizing and system supporting—demonstrate the complex, non-linear, and intertemporal nature of security interventions. We therefore choose our research methodology to enable representation of these effects.

IV. Methodology

To accomplish the goals described in the Introduction, we employ System Dynamics Modeling (SDM), an approach for modeling and simulating complex physical and social systems. The SDM approach is based on identifying individual causalities and how they *combine* to create, non-linear feedback loops that are the causes of the counter-intuitive outcomes. This approach can greatly leverage the deep, but often isolated and fragmented, knowledge about complex challenges (such as cyber security) that is generated from empirical observations, the written record, or from Subject Matter Experts (SMEs). Doing so can leverage diverse materials and provide improved insights and understanding of the dynamics and behaviors of systems under diverse conditions. As such, system dynamics is a method that contrasts sharply with the many quantitative approaches that are based on "driving forward by looking through the rear-view mirror." While there are advantages in relying upon the use of past data to predict the future, there are also serious disadvantages that must be guarded against.

This approach is intended to help bridge the gap between data and knowledge, by providing a coherent framework within which to gather, organize, and analyze a variety of types of data (i.e. time series, expert generated), and ultimately simulate quantifiable models to generate robust system knowledge..

The core of the modeling strategy is to represent system structure in terms of stocks, flows, and the causal mechanisms that govern their rates of change. Feedback loops are the building blocks for articulating the causality represented in these models. In this domain, the

interaction among the various modular sectors (i.e., social, economic, technical, and cultural) can be used to explain overall system behavior, such as identifying the sources and recognizing the evolution of cyber threats. (Sterman, 2000) The appeal for the analysis of cyber-enabled challenges associated with the financial services industry lies in SDM's capacity to link observable patterns of behavior of a system to macro- and micro-level structure and decision-making processes. In other words, models will be tightly grounded in observations of real world cyber venues, but also will be associated with multiple theoretical frameworks of actor behavior.

This multi-level modeling approach incorporates complex interactions among different major actors and entities while capturing non-linear causal relationships. By understanding how non-linear causal connections among actors create different propensities for risk, we can use the model to explore policy alternatives and identify high-leverage options to mitigate risk. Our own uses of system dynamics modeling have allowed us to determine the method's *unique capabilities* to the understanding of the generation of the propensities for risk and resiliency, and to predict future patterns due not only to the central features of this method, but also because of added, specific and unique capabilities of SD. These include:

- *Objective input*: Ability to utilize data to determine, with precision, parameters affecting the causality of individual cause-and-effect relationships.
- *Empirical grounding*: Ability to interface with the other methods for estimating relationships (such as econometrics) or the nature of content (such as content analysis) in the integration of quantitative foundations for model parameters
- *Subjective (expert) judgment*: Ability to represent and model cause-and-effect relationships, based on expert judgment, even when detailed data does not exist.
- *Intentions Analysis*: Ability to identify the long-term unintended consequences of policy choices or actions taken in the short term
- *Tipping point analysis*: Ability to identify and analyze "tipping points" – where further incremental changes lead to significant impacts.
- *Transparency*: Ability to explain the reasoning behind predictions and outputs of the SD model.
- *Modularity*: Ability to organize SD models into collections of communicating sub-models (e.g., terrorism recruitment, economic development, religious intensity, regime stability)
- *Scalability*: Ability to use the modularity to increase complexity without becoming unmanageable.
- *Portability*: Ability to utilize the same basic SD model in different regions of the world without requiring re-specifications.
- *Focusable*: Ability to increase details in specific areas of the SD model to address specific (and possibly new) issues that emerge from the outcomes, behaviors, or predictions that are made.

We present a causal diagram below in Figure 2 to illustrate several of the characteristics of system dynamics.

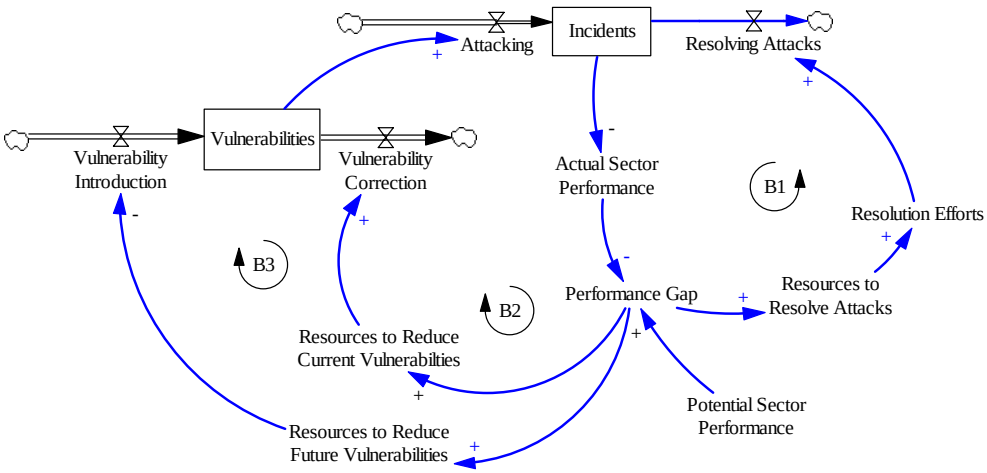

Figure 2. Vulnerability and Incident Causal Diagram

The casual diagram captures three dynamic narratives concerning security dilemmas and potential responses. Its purpose is to show the temporal dynamics involved with targeting different aspects of the financial system for policy responses. The flows, denoted by straight arrows with valves, are the rate at which variables (vulnerabilities and incidents) accumulate. Also shown in the figure are the system stocks, denoted by a rectangle, which are computed as the integration of the stock's inflows less its outflows. Linking the flows are feedback arrows, labeled with a "+" for a positive polarity (more x leads to more y) and a "-" for a negative polarity (more x leads to less y.)

To unpack the dynamic responses, we begin with an initial concept: the co-evolution of systems (i.e. technology platforms), vulnerabilities (i.e. latent software flaws), and incidents (i.e. attacks, data loss). As systems develop, they increase potential vulnerabilities (at a rate that is controlled in part by system quality.) Over time, these 'latent' vulnerabilities can be exploited, increasing the number of incidents (such as attacks) which have manifestations for users. These conflicts reduce the utility of systems and create a gap between the potential (feasible) performance of the sector and the actual (constrained) performance. The existence of a gap signals the need for corrective action.

The performance gap can create pressure for policies to reduce the gap in several different ways.

- Reducing the current stock of incidents (loop B1)
- Reducing the current stock of vulnerabilities (loop B2)
- Reducing the introduction of vulnerabilities (loop B3)

The policies above are all aimed at reducing the utility gap and solving cyber challenges, but do so in fundamentally different ways and at different speeds.

- Resolving Incidents (Loop B1): This loop captures the logic of responding to cyber incidents by direct resolution. The actions represented in this loop could feasibly be acted upon quickly. Incidents are a salient indicator of cyber threats, and therefore the time to

react will likely be shorter. Coordination costs may also be lower than other responses, depending on the number of actors required to respond. However, B1 may involve *significant and reoccurring costs* because the address only the manifestation of sector challenges.

- Resolving current vulnerabilities (Loop B2): This loop captures the logic of addressing existing vulnerabilities in the cyber system. Efforts corresponding to this loop may represent a more *systematic response to cyber challenges*, though there are *significant barriers to engaging these actions*. Vulnerabilities are harder to detect and "count" than incidents and may be more tightly engrained with the overarching cyber system, requiring greater coordination from a greater number of actors. Therefore, it is likely that responses along the logic of B2 will have a greater delay than those in B1.
- Reducing future vulnerabilities (Loop B3): This loop captures the logic of a fundamental shift in cyber systems to reduce or eliminate the creation of vulnerabilities. Policies captured in this loop would involve systematically rethinking cyber systems and sector interaction. This loop conceptually has a *high "ceiling" for effectiveness*, but would likely require *large degrees of coordination* (as well as technology development) and may *involve lengthy delays*.

Finally, it is important to note that these loops exist within a resource context, and each loop corresponds to different claims on resources. Depending on the cues organizations and individuals respond to, the economics will favor different loops over time. This framing represents a unique and distinctive cut into evaluating sector wide approaches, one that focuses on temporal dynamics and feedback.

V. Case Study: Advancing the State of the Art in Designing and Testing Secure Applications

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." Below, we provide an example of a system dynamics model to address these vulnerabilities, which are placed in a larger context, including organizational and sector response strategies. The model in Figure 3 provides a framework to address the application security questions above as well to explore other issues described below:

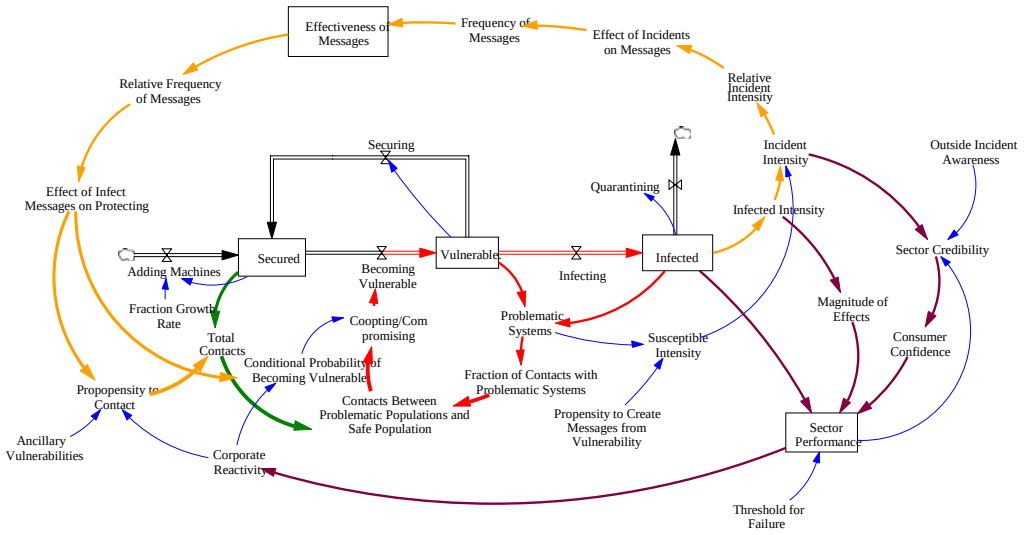

Figure 3. Example of System Dynamics Simulation Model

Figure 3 is a simplified representation of a simulation model[1], with each color denoting a different feedback loop. The model is described below:

- **Main Stocks and Flows**: The core of the model is the three stocks, which refer to different states of the sector's information technology infrastructure. These are: secured (at low or no risk), vulnerable (at an exposed level of risk, such as those with software possessing identified risk vectors), and infected (existing with malicious code, such as malware.) These states are linked together by flows, by which systems grow, become vulnerable, become infected, and are secured or quarantined. *The key issue here is the feedback controlling these rates.*
- **Vulnerability Feedback**: These loops, shown in red and green, show how secure systems come in contact with vulnerable or infected machines and become co-opted into more problematic states. *The key issues here are the rate of contact (which can be thought of system interdependency) and the rate of infection (controlled by corporate resilience to attack and infection.)*
- **Effectiveness Measure Feedback:** This loop, shown in yellow, shows industry response to infection through the transmission of messages about threats. As the frequency of messaging increases, so to does industry effort to reduce both the contact rate and the probability of becoming infected. *The key issues here are at what rate messages are generated (does the sector have good visibility into the current state of systems?) and how effectively are these messages converted into defensive action.*
- **Sector Performance Feedback:** This loop, shown in purple, depicts the outsider response to cyber challenges via industry performance. For example, if infected machines increase in magnitude, leading to greater cyber incidents, this will have a negative effect on consumer confidence and sector credibility, hurting overall industry performance. In response, the industry can attempt to increase corporate reactivity to cyber as another

[1] The simulation model uses fourth-order differential equations and consists of approximately 75 variables. Behind each variable shown in the figure is either a parameter or an equation.

path to reducing the infection rates. *The key issues here are the rate at which cyber attacks occur, the financial magnitude of this effects, and outsider's visibility into these events. Also important is the ability of the sector to coordinate responses.*

Figure 3 shows the framework for a simulation model to quantify these feedbacks. While not fully shown for space reasons, the simulation model is initialized with stylized parameters (with additional variables to allow for quantification) to run a series of tests. 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 recover 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 (via the messaging loop) and defensive routines taken by management to avoid infection (via the sector performance loop). 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.

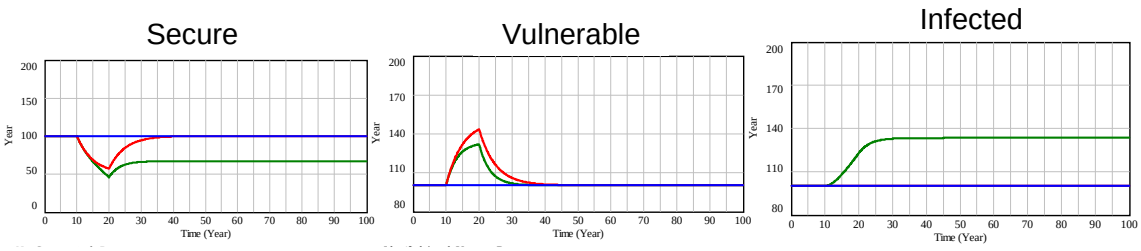

Figure 4. Simulation Output of Infection

Next we examine the cost ramifications of the three cases (Figure 5) by looking at the costs generated from the vulnerable and infected stocks, as well as the total. While costs in the red case (industry relies on software that has latent security flaws, but is able to avoid infection by rapid patching) are higher due to more proactive management of the vulnerable machines than in the green case, they are lower from the infected stock. As a result, on the whole, the red case in less expensive.

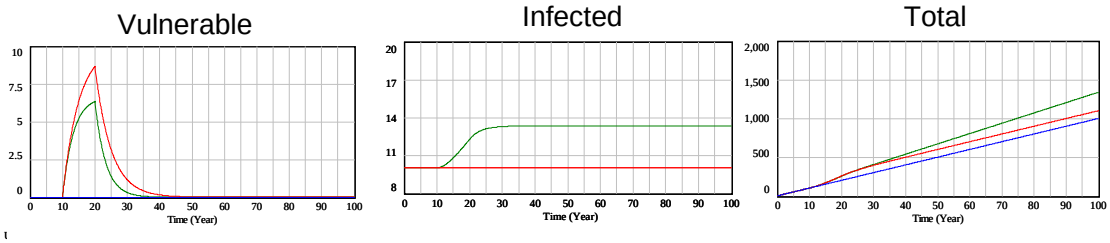

Figure 5. Simulation Output of Cost

This relatively simple simulation is designed to demonstrate several features of our approach, the ability to:

- Run scenarios showing different security approaches and the cost ramifications.
- Identify tradeoffs between approaches
- Show root-causes of behavior because of feedback

IV. 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 sector 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; 4) engaging and reaching out to public, private, and academic audiences for the design and implementation of model-based strategies; and 5) developing approaches to transfer management techniques, models, and associated tools to relevant organizations.

References

Akiyama, M., Goldsmith, D., Siegel, M. *Improving Hospital Operations Using Bar-Code Capture Data and System Dynamics Modeling Techniques*, System Dynamics Conference, Cambridge, MA, January 2007

Choucri, N., Goldsmith, D., Madnick, S., Morrison B., Siegel, M. *Using System Dynamics to Model and Better Understand State Stability*. System Dynamics Conference, Cambridge, MA, 2007

Choucri, N, Goldsmith, D. and Mezher, T. *Framework for Modeling Technology Policy: Renewable Energy in Abu Dhabi*, Conference Proceedings of the 2008 International Conference of the System Dynamics Society, July 20 - 24, 2008, Athens, Greece

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

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]

Moulton, A., Madnick, S., and Siegel, M. *Context Interchange on Wall Street," Proceedings of the International Conference on Cooperative Information Systems*. (CoopIS'98), N.Y., 1998

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.

Morrison, B., Goldsmith, D, Siegel, M. *Grappling with Dynamic Complexity in Military Planning: The System Dynamics Approach*. International System Dynamics Conference, Athens, Greece, 2008

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.

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.

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.

Appendix A: Unpacking the Dynamics of Systems, Firms, and Sectors

This appendix pulls together several narrative threads around the issue of systems, firms, and sectors. It is intended to pull together causal linkages and feedback for several issues cutting across technical and organizational boundaries, including: Attack Vector Identification, System Compromising, Attacker Dynamics, Firm/Sector Dynamics, and Market Dynamics and Vendor Response.

It builds the narratives around a framework which includes a firms IT systems (either not compromised, those with identified attack vectors, and those compromised), the firm and sector performance, firm knowledge and awareness, attack capabilities, and vendor resilience and responsiveness.

Figure A1.

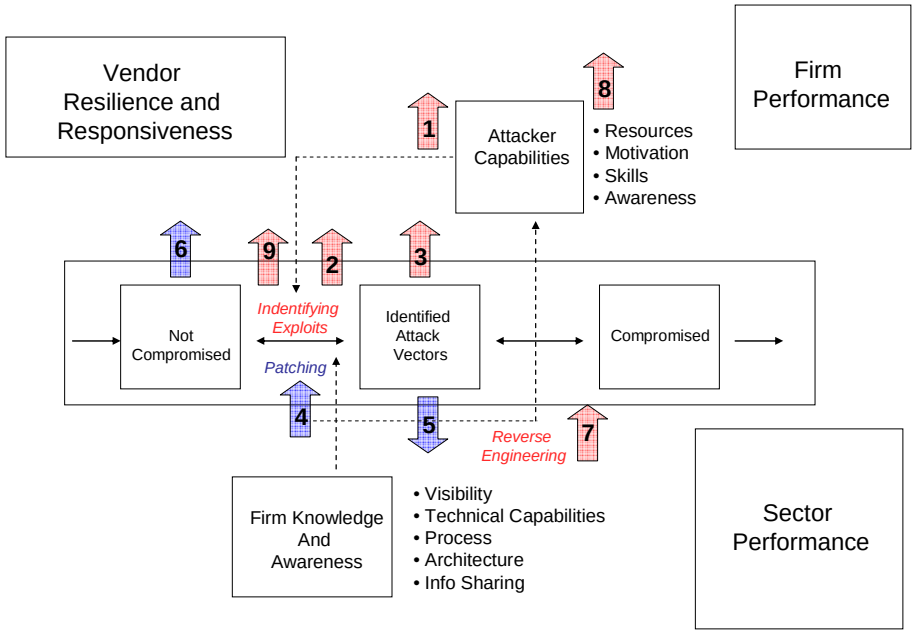

Figure A1. Attack Vector Identification

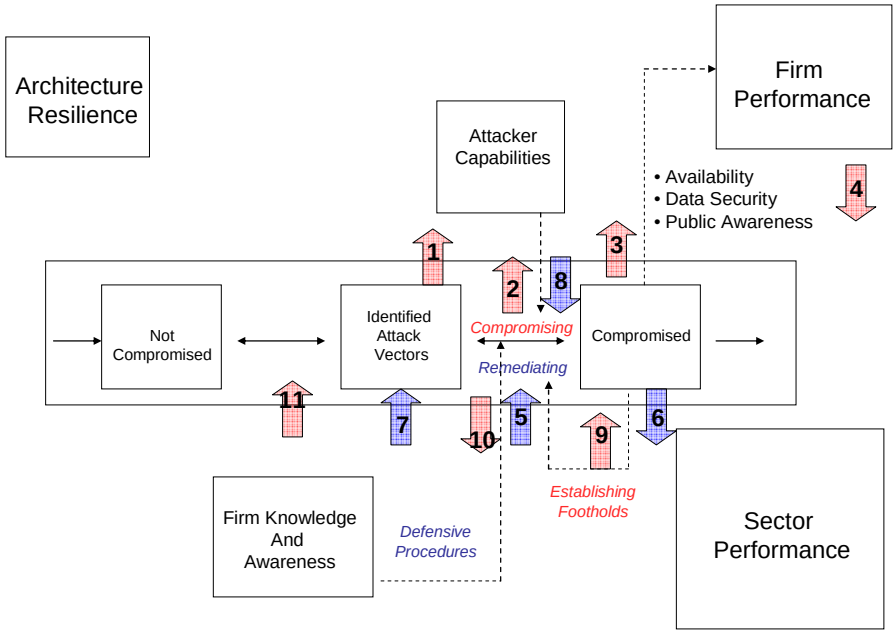

Figure A2. System Compromising

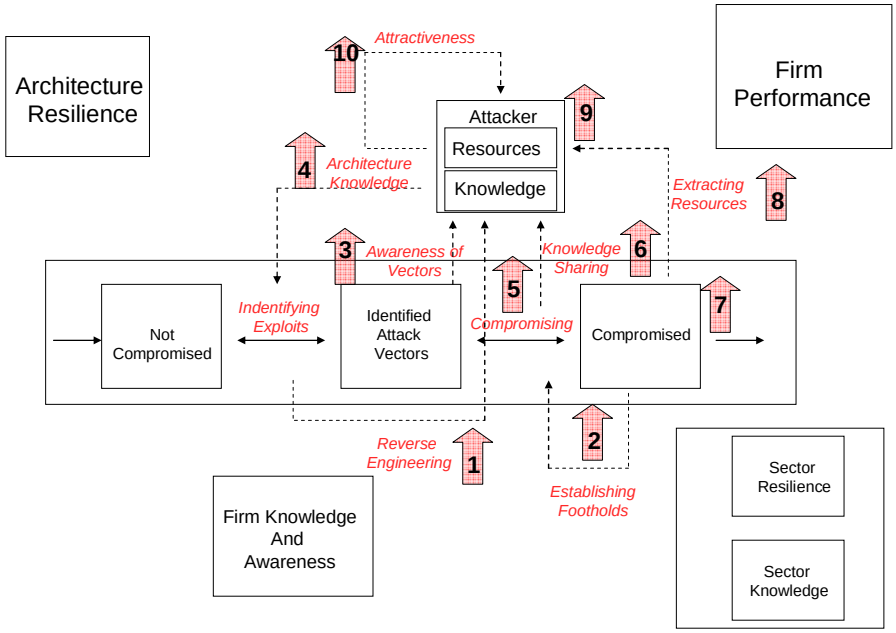

Figure A3. Expanded Attacker Dynamics

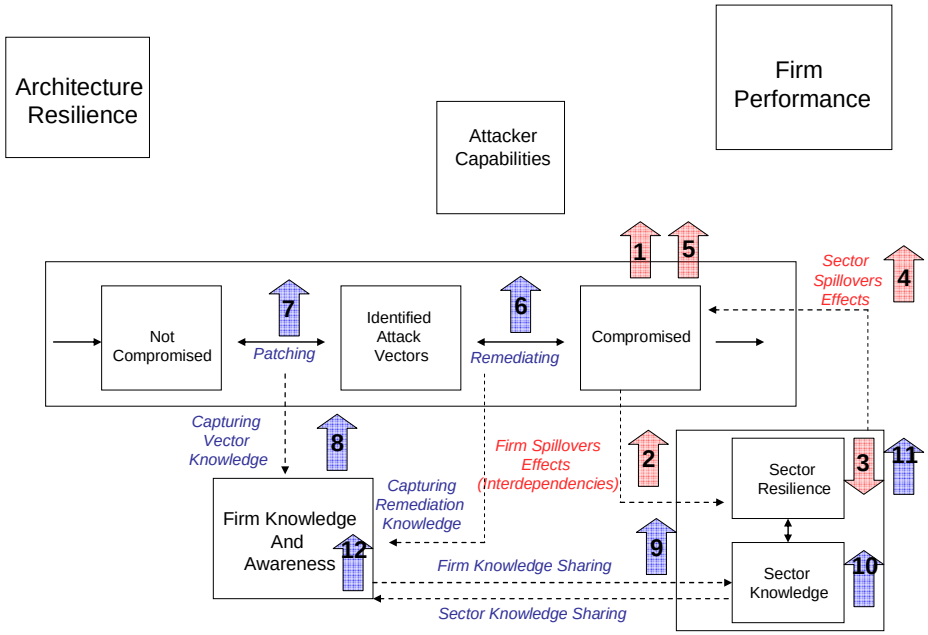

Figure A4. Firm/Sector Dynamics

Scrubbing and Architecture Resilience

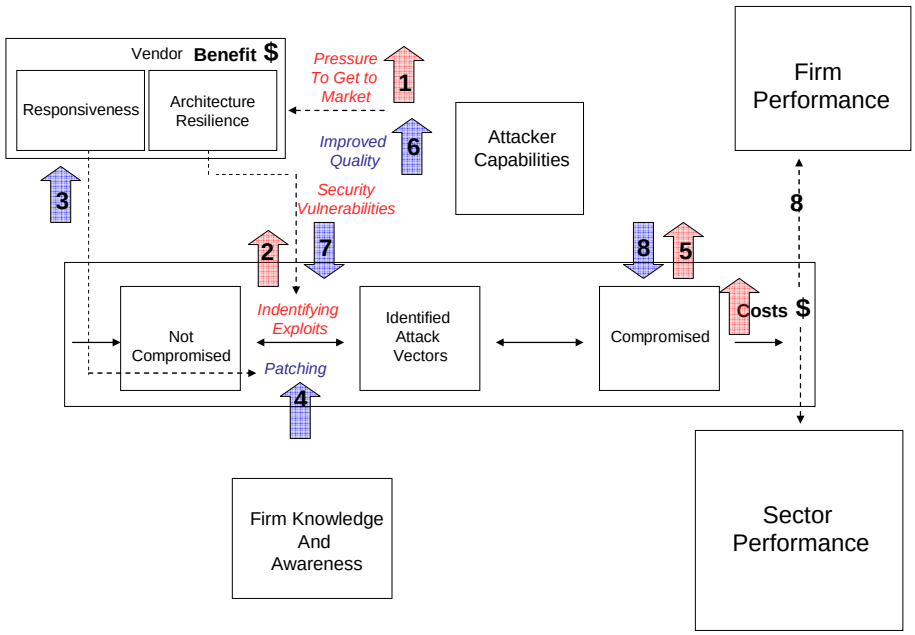

Figure A5. Market Dynamics and Vendor Response