Interdependence of Security and the Extended Enterprise
(I-SEE SIG)

A New Special Interest Group at the MIT Center for eBusiness

Associated Faculty: Arnold Barnett, Gabriel Bitran, John Carroll, Nazli Choucri,
Steve Graves, Benjamin Grosof, Richard Larson, Don Lessard,
Stuart Madnick (Coordinator), Michael Siegel, Yossi Sheffi, Richard Wang, Roy Welsch

June 2005

MOTIVATION

This Special Interest Group is motivated by several separate, but interrelated, observations:

- Businesses have become increasingly global and interdependent – the traditional enterprise has become the "extended enterprise."
- Disruptions, even though rare, any where in this "extended enterprise" can have dramatic and often unexpected impacts upon all the organizations involved. For example, an action at an Ohio power plant (whether accidental or by terrorist) can bring down the electric power for almost half the USA.
- In recent years, acts of terrorism, besides undermining the national security of our country, have introduced new and dangerous disruptions to business and society.
- Although we often think of National and Homeland Security from a governmental and military perspective, businesses play an extremely important role for many reasons:
  - Businesses can suffer tremendous disruption
  - Much of the USA infrastructure (such as transportation, power systems, financial systems) is run by the private sector
  - We have much to learn from each other: Business has much to learn about dealing with these issues from government and academia; Government has much to learn about dealing with these issues from business and academia; and Academia has much to learn from Business and Government.

This SIG is intended to serve several interrelated functions:

- **Perform research** related to I-SEE, including articles for both academic journals and business publications. Current and potential research topics can be seen in below, along with MIT faculty interests. A possible preliminary research plan is presented below.

- **Develop courseware** (including case study materials) and **deliver courses** related to I-SEE both for traditional graduate degree programs as well as short courses for executives in both industry and government in order to better educate and prepare managers for a more complex and inter-related world with respect to the security of the extended enterprise. For example, several Sloan alumni taught an MBA course on "Business and National Security" in Spring 2004 (see Appendix

V.) The major sections of the course were: (1) What has Changed? (2) Supply Chain Security, (3) Cyber Security, (4) Financial Tracking, (5) Working with Washington, (6) Investing in an Uncertain World, and (7) Lessons Learned.

- **Facilitate discussions**, seminars, and symposium amongst academia, government, and business on these important topics.

PRELIMINARY RESEARCH PLAN

A major challenge for business and government is deciding with some measurable degree of confidence how much and what they should invest for protection against extreme and rare events. This will require a way to address events that are often not independent and, without proper protection, can result in catastrophic loses. Although our initial focus is on terrorism and national security, these events could include cyberfraud, natural disasters, even rapid invasion of a market by a competing technology or business model.

We propose research in four inter-related areas (the four M's): Monitor, Measure, Model, and Mitigate risks.

Monitor Risks. Risk is usually associated with something bad happening (downside risk) but it can sometimes provide opportunities – such as the aftermath of the death of a political leader (e.g., Yasser Arafat) or a major natural disaster (e.g., a tsunami) can open up new opportunities (e.g., new approaches to peace in Middle East or Indonesia and Sri Lanka). By constantly monitoring events and having flexibility in our processes, we can be in a position to take advantage of shifts in our favor (opportunities). Risk is almost never one dimensional and the complexity of and linkages between global corporations, information systems, and supply networks means high dimensional multivariate systems approaches will be required.

The National Research Council report on 9-11 noted that "*[A]lthough there are many private and public databases that contain information potentially relevant to counterterrorism programs, they lack the necessary context definitions (i.e., metadata) and access tools to enable interoperation with other databases and the extraction of meaningful and timely information*.[1]" There are technologies being developed at MIT, called context mediation, which provides novel approaches for addressing these problems. We plan to study and explore the use of these technologies, especially in providing support for counter-terrorism intelligence information gathering.

The "nightmare scenario" among security professionals is not a nuclear holocaust or a dirty bomb. Instead, it is an attack in which the target does not realize it is under attack until it is too late. Fast detection of such an ongoing disruption is a key to resilience. As an example, one of the main differences between Nokia's and Ericsson's response to the fire at Philips is the speed with which Nokia detected the problem and internalized its consequences, and thus sprung into action. It is critical that there be government or company processes that can lead to fast detection, enabling it not only to respond quickly to disruptions but also respond quickly to day-to-day changes in the marketplace.

Mechanisms are needed to continually monitor and assess possible risks at multiple business levels. At the highest level, monitoring the risks of disruptive innovation and terrorism are important areas needing further research. Document search and retrieval

technologies and the analysis of text data will be important and require additional research in data mining aimed at risk monitoring.

Measure Risks. Historical data, scenario simulations, and expert judgment are used to develop models for uncertainty. However, these models are often converted into risk measures based on variances and covariances (for dependent events). Recently, the finance community has come to realize that variances often do not provide adequate risk measures. Experience with financial risk measurement shows that using variances or covariances may underestimate (and in some cases overestimate) the actual risk by a sizeable factor. The emphasis is now on extreme behavior which is often measured using value-at-risk, shortfall, etc. in the upper tail and lower tail separately. These new forms of risk measurement should be useful tools to assess risk in situations that go beyond financial or third-party risk. More generally, supposedly adequate financial diversification based on covariance structures has proved to be inadequate in extreme stress (meltdown) situations. New research is focused on developing diversification algorithms using tail correlation measures.

One area outside of finance where new risk measures are being applied has been in the area of supply chain management. Optimal supply chain policies can often be very fragile and extreme events can cause chaos. New risk measures, like shortfall, offer the promise of less fragile supply chains in situations that can threaten the entire enterprise. We plan to extend these ideas to other risk situations at various levels in the corporation.

High-dimensional risk data with complex dependencies and nonlinear interactions will require new analytic approaches. Identifying structure and interactions in such situations would normally require unrealistically large amounts of data. Recent work on dimensionality reduction (which, on one hand, is free from rigid structural assumptions about the underlying model and, on the other hand, does not require large amounts of data) shows great promise. This will also allow better visualization of multivariate and multilevel risks along with key risk drivers.

We can augment available data in another way. Focusing on more extreme events means we will, most likely, have less historical data available that reflects exactly the situations we are considering. This will mean developing methods to combine similar, but not identical, rare events. This is becoming established practice in the use of data from clinical trials and research to extend these Bayesian modeling methods is needed to see if they can be applied over a much broader range of situations. Bayesian methods can also be used in other ways to substitute for the lack of data by incorporating prior information and expert opinion.

Model Risks. In other situations we will need to assess the cost of flexibility based on newer risk measures and more sophisticated determination of the risks involved. Even in less complex cases, developing models that would search for optimal flexibility strategies under certain constraints (cost, time to market, etc.) would be useful and will help parameterize flexibility. This will also allow for sensitivity analysis and stress testing to determine how best to invest additional resources and what adjustments to make as risk scenarios change.

There are ironic examples where addressing and mitigating risk for small parts of a larger system can lead to increased risks for the larger system[2]. We need to understand why and when this occurs and investigate methods to model larger and more complex risk situations.

[2] There was a recent article about Electric Power Systems that expressed an interesting premise that incremental steps to improve safety has led to bigger disasters!

In its Preface, the 9/11 Commission Report stated: "*We learned that the institutions charted with protecting …national security did not understand how grave this threat can be, and did not adjust their policies, plans, and practices to deter or defeat it*" (2004: xvi). The importance of this was also highlighted in the Wall Street Journal[3] when they noted "*Early US decisions in Iraq (during pre-conflict) is haunting current efforts (during post-conflict)*." Given current realities and uncertainties "better preparedness" can be achieved by identifying, controlling and managing the elusive linkages and situational factors that fuel hostilities and terrorism. We propose to explore capabilities provided by anticipatory technologies that help model and better understand the complex dynamics shaping and precipitating conflict worldwide. Initially we will focus on linking pre- and post- conflict situations by drawing upon the power of system dynamics, augmented by new technologies for integrated information analysis, in conjunction with the development of conceptual and computational ontologies capturing the diversity, intensity, and dynamics of the conflict domain.

Another possible component of these risk models is likely to be real options. Just as financial risk measurement ideas (shortfall, etc.) are starting to impact supply chains and product development, financial options theory is now being applied in order to assess and quantify the options explicitly involved in choices related to robustness and flexibility. As we attempt to scale risk management from the tactical to the operational and on to the strategic level, we expect new research opportunities to arise in real options as well.

The ability to model and estimate the costs and degree of confidence related to robustness, flexibility, etc. will allow the government and corporations to assess the amount of risk they should assume and the amount they should pay others to assume.

Mitigate Risks. There are at least three basic ways to deal with risk (and more may arise as the research progresses). We can: (1) reduce uncertainty, (2) enhance systems to respond by strengthening the system against shock, or (3) make the system more flexible so that it can adjust to shock. For example, we could control uncertainty using demand management, protect passively by building in robustness to known potential variation, or protect actively by creating flexibility that managers can use to react to uncertainties.

This will depend on the enterprise level being considered. At the product and process design stage, enabling flexibility can mitigate risk, often at low cost. Forecasting customer behavior in many industries has become increasingly unreliable. If forecasting does not work well, then building flexibility into production processes and manufacturing plants can allow production shifts at far lower cost in the future. One manager recently said that if we can't predict, at least we can survive. The catch, of course, is that there is an upfront cost to building in this flexibility. GM found that, after a careful analysis of what the critical flexibility enablers were, the upfront cost was so low given the large cost of a new model and associated production facilities that it did not require an overly detailed assessment of risk and reward—it just made good sense. It may be possible to develop flexibility analysis tools that will make the real cost of flexibility easier to analyze and show that it is far more cost effective than generally thought.

Often a companies' fortunes in the face of business shocks depends more on choices made before the disruption than it does on actions taken in the midst of it. Companies can build in flexibility throughout their supply chains, based on proven design principles and the right culture – balancing security, redundancy, and short-term profits. Investments in resilience and flexibility not only reduce risk but can create a competitive advantage in the increasingly volatile marketplace. Companies can increase security, reducing the likelihood

[3] April 19, 2004.

of a disruption, with layered defenses, the tracking and analysis of "near-misses," fast detection, and close collaboration with government agencies, trading partners, and even competitors. An important factor is resilience—the ability to bounce back from disruptions—by building in redundancy and flexibility. For example, standardization, modular design, and collaborative relationships with suppliers (and other stakeholders) can help create a robust supply chain and a corporate culture of flexibility, with distributed decision making and communications at all levels, can create a much more resilient enterprise.

"Mitigation" usually conveys the notion of incurring some additional cost (like an insurance policy) to try to reduce the negative impacts of some risk. This view is too limited in two ways:

(1) At one time, many thought that "quality" and "cost" were trade-offs, i.e., one could have higher quality at higher cost or go for less cost with lower quality. As Total Quality Management (TQM), and other efforts, showed – it was often possible to simultaneously increase quality while decreasing costs (especially by reducing waste materials and redundant labor). Similarly, we envision that there are opportunities to simultaneously increase the security of our organizations without increasing costs – possibly even reducing costs in some cases.

(2) As noted earlier, sometimes opportunities are created by unexpected events. We want our organizations to be resilient and flexible enough to seize such "up side" possibilities.

When we look at the scope and complexities of the extended enterprise, the ability to reduce uncertainty, enhance systems to respond most effectively by strengthening the system against shock, and make the system more flexible and resilient so that it can better adjust to shock and take advantage of opportunities becomes even more important.

Additional Comments on the Research Effort. In addition to gaining a general understanding of the issues described above, we need more theory to ground our measures and models, perhaps a framework about risk and security that can address particular content areas such as: computer security, borders, transportation, financial stability, interorganizational information systems, data mining, system simulation, gaming and scenario development, design for flexibility and resilience, etc. In particular, we need better ways to organize large enterprises to be more flexible. We look forward to inter-organizational collaborations and information exchanges, especially in organizational learning, i.e., how we learn from successes and failures.

We all understand that in thinking about terrorism, we are up against a "modern" form of organization, i.e., a loosely-organized, modular, flexible, bottom-up, networked organization that has a lot of innovative capability and resilience. It's like the Colonial snipers and the British troops – as long as the British troops march along in their redcoats in predictable formations, even a small and weak force can slowly inflict considerable damage. Our society is very efficient and interdependent, that is both our advantage and our vulnerability. We have to maximize that advantage and minimize the vulnerability – as proposed in these research efforts.

ASSOCIATED FACULTY

The list below indicates some of the faculty with interested related to I-SEE. They have all seen this proposal and provided some of the materials:

GABRIEL BITRAN (Sloan): His research interests are in the design and delivery of service systems, coordination and integration in supply chain management, and pricing of goods and services.

JOHN CARROLL (Sloan & ESD): John Carroll's recent work focuses on industries that manage significant hazards, such as nuclear power, petrochemicals, and health care. Carroll has examined the relationships between leadership, management philosophies, teamwork, mental models, safety culture, and human performance improvement.

NAZLI CHOUCRI (Political Science Dept): One particular project that she is involved in is using System Dynamics to model and better understand the causes and outcomes of conflicts. She also is working on multi-dimensional threats to national security and alternative strategies for reducing vulnerabilities.

STEVE GRAVES (Sloan & ESD): Stephen Graves develops and applies operations research models and methods to solve problems in manufacturing and distribution systems, and in service operations. Currently, he is focusing on supply chain optimization, strategic inventory positioning in a supply chain, and production and capacity planning for various contexts.

BENJAMIN GROSOF (Sloan): Benjamin Grosof has been working on using semantic web rules for policy, including authorization/security/privacy policy, and including monitoring/exception-handling/problem-resolution requirements for policy compliance (e.g., with financial regulations), and analysis of risk management economic advantages.

RICHARD LARSON (Civil Engineering & ESD): He was worked on operations research as applied to services industries, especially urban service systems (esp. emergency response systems), logistics and workforce planning. His first book, Urban Police Patrol Analysis was awarded the Lanchester Prize of the Operations Research Society of America.

DON LESSARD (Sloan): Don Lessard studies international corporate strategy and finance with a special emphasis on risk and knowledge management. His current research focuses on globalization strategies in network industries and the linkage of strategy on risk management in major projects. He has published extensively on risk management, global strategy, international corporate finance, and the debt crisis.

STUART MADNICK (Sloan & ESD): Two particularly relevant current projects are (1) Modeling the causes and outcomes of conflicts (with Nazli Choucri, see above), and (2) Technologies to aid in gathering and aggregating data from disparate sources to better assist counter-terrorism measures (with Dr. Michael Siegel.)

YOSSI SHEFFI (Civil Engineering & ESD): Yossi Sheffi just finished a book (which will come out towards the end of 2005) on supply chain resilience. It was the result of a CMI research effort and it looked at many cases of supply chain breakdown (due to terrorism, fires, earthquakes, strikes, whatever) and how companies responded. The book is aimed at developing ideas on supply chain resilience and how to build flexibility into supply chains.

RICHARD WANG (Center for Technology and Industrial Development): Richard Y. Wang is a pioneer and internationally known leader in the data quality field. He is the lead Principle Investigator of the MIT Information Quality Program and Co-Director for the MIT Total Data Quality Management (TDQM) Program.

ROY WELSCH (Sloan & ESD): Roy Welsch is an expert in applied statistical methodology in manufacturing, ebusiness, and finance. He also looks at hybrid process control, credit card

scoring models, data mining for the analysis of massive data sets, robust methods and design, value-at-risk models, and optimization for financial time series.

CURRENT RESEARCH PROJECTS

Prof Gannon, Madnick, Moulton, Siegel, Sabbouh, Zhue: "Semantic Information Integration in the Large: Adaptability, Extensibility, and Scalability" – There is a pressing need for effectively integrating information from an ever increasing number of available sources both on the web and in other existing systems. A key difficulty of achieving this goal comes from the pervasive heterogeneities in all levels of information systems. Existing and emerging technologies (web, ODBC, XML, and web services) provide essential capabilities in resolving heterogeneities in the hardware and software platforms, but they do not address the semantic heterogeneity of the data itself. A robust solution to this problem needs to be adaptable, extensible, and scalable. In this research project we identify the deficiencies of traditional approaches that address this problem using hand-coded programs or require complete data standardization. The Context Interchange (COIN) approach overcomes these deficiencies by declaratively representing data semantics and using a mediator to create the necessary conversion programs using a small number of conversion rules. The capabilities of COIN are demonstrated using an intelligence information integration example consisting of 150 data sources where COIN can automatically generate the over 22,000 conversion programs needed to enable semantic integration using only six parametizable conversion rules.

Prof Madnick, Moulton, Siegel: "Context Mediation Demonstration of Counter-Terrorism Intelligence (CTI) Integration" – Context mediation provides the means to formally document the semantics of the data used by each source and to automatically generate the necessary conversion procedure to put the data into any required form. To experiment with the use of context mediation for counter-terrorism intelligence, we developed a fictional scenario with surrogate data comparable to some types of data that might be used in actual practice. The scenario involves events, people, and places located primarily in "Great Britain. The people and events are entirely fictional, but not unrealistic. The places are real, in the sense that they can all be located on a map, though there is nothing to suggest that the places chosen have any relation to action tactual terrorist activity. Our experiment produced very useful data, and our analysis shows that indeed context mediation has an important role to play in counter-terrorism.

Prof Choucri, Mardnick, Siegel: "Research Initiative to Understand & Model State Stability: Exploiting System Dynamics" – This project focuses on the use of systems dynamics modeling techniques to help understand, measure and model the complex dynamics shaping state stability, initially for two regions. The researchers have specifically considered the impacts of unanticipated disruptions, such as a tsunami and its aftermath, on the dynamics of the two regions. For each region, a detailed country model is delivered, including 3-5 futures predictions in the 6-12 month range, along with an analysis of conditions and causal links between predicted futures plus corresponding mitigated options.

Prof Madnick, Siegel: "Towards Total Security Quality Management (TSQM): Definition and Measurement" - We propose to draw upon the experiences and theories developed by the TQM and TDQM research efforts to produce operational measures and metrics, and related tools to assess levels of security in modern enterprises. These would include a definition of what constitutes good security, and a statistical model for measuring this at individual firms or departments. Realistically, multiple iterations and experiments with organizations will be needed to refine these measurement tools. However, we believe

that a useful initial set can be developed in the short term as we define and measure "total security quality management" in the extended enterprise.

PROSPECTIVE RESEARCH PROJECTS

Prof Gabriel Bitran: "Mining System Security" – I am interested in studying risk issues in mining systems. Typically such systems include several mines, mineral improvement plants, railroads, trucking and Shipping operations. The potential for accidental and planned disruptions is enormous and the consequences very costly. The inability to operate the mines can jeopardize national security and economic stability.

Prof Nazli Choucri, Prof Stuart Madnick, and Dr Michael Siegel: "Modeling Stability of States and Implications of Instability" – Given current realities and uncertainties "better preparedness" can be achieved by identifying, controlling and managing the elusive linkages and situational factors that affect state stability and fuel state decay – and hence create new threats to our nation's security. We propose to explore the use of system dynamics modeling techniques to develop anticipatory technologies that help understand, measure and model the complex dynamics shaping and precipitating state failure.

Prof Benjamin Grosof: "Defining and Executing Security Policies" – A key component of security is defining and executing policies for security authorization, reporting, and handling of violations. There often have problems in regard to coherence, integration, transparency, training, compliance assurance, change management, and overall costs. Recently we have made theoretical breakthroughs in interoperability and modularity of generic rule-based policy specification and processing. We are interested in applying these advances to radically improve security policy management, by addressing the above problems – in short to improve quality, agility, and life cycle costs.

Prof Stuart Madnick, Dr Michael Siegel, and Dr Richard Wang: "Measures and Metrics of Enterprise Security" – There are many important similarities between the TQM efforts (of the 1950s onward) and the increasing concerns about the cost and quality of security in enterprises today. An important early step in the TQM effort was to more precisely define what "quality" meant, especially in a holistic sense. In order to make serious progress towards improving enterprise level security, we propose to draw upon the experiences and theories developed by the TQM and MIT TDQM[4] research efforts to define the concept of enterprise "security" and develop effective ways to assess and measure it.

Prof Richard Larson: "Vulnerability Analysis of Firms to Loss of Key Professionals" – Research questions: Which set of professionals is most problematic? Rankings? How to mitigate against this risk? Loss of professionals could be due to illness, voluntary change of jobs, natural disasters, and acts of terrorism including kidnapping.

Prof Stuart Madnick and Dr Michael Siegel: "Intelligent Intelligence Information Integration" – Counter-terrorism intelligence analysis requires fitting together fragments of information drawn from a variety of heterogeneous sources. When some data is represented in one way while other data is represented another way, an additional level of complexity is introduced. The MIT Context Mediation Technology (CMT) offers a new means to solving those semantic problems with greater flexibility and reduced costs for constructing and maintaining conversion software. We propose to explore extensions to this technology to facilitate counter-terrorism intelligence analysis and related information challenges to the extended enterprise.

[4] The Total Data Quality Management (TDQM) effort started in 1991 at MIT.