Information Security in the Extended Enterprise: A Research Agenda

Scott Dynes
Center for Digital Strategies
Dartmouth College
Tuck School of Business, USA
sdynes@dartmouth.edu

Lutz M. Kolbe
Chair for Information Management, Institute of Information Systems
University of Goettingen, Germany
lutz.kolbe@unisg.ch

Ragnar Schierholz
ABB Switzerland Ltd.
Corporate Research
Switzerland
ragnar.schierholz@ch.abb.com

Abstract

Today most companies are closely knit together with and thus dependent on suppliers, allies, customers, and public authorities. Member companies in such an extended enterprise or "business network" are either forced or volunteer to meet certain security objectives as a whole. As a consequence, the business network needs to agree on a common strategy, joint processes and technical interfaces to meet regulatory or voluntary requirements from industry standards. Reality shows that – even if standards exist – they are not harmonized and access and reconciliation between partners is sometimes legally, if not technically impossible, or simply too expensive. The serious and economic assessment of risks, already tough on the internal scale, becomes almost an insurmountable obstacle when considering the entire business network. This paper's objective is to emphasize the importance of security in business networks for research and practice. Since there is little research available, it raises major questions to be answered by a future research agenda. A basic research framework is derived based on related research, an observation of the interdependencies of firms and a series of cases from different industry sectors. Finally, the paper discusses which factors and incentives might be catalysts for the adoption of such a framework by a single firm, business network, or even public welfare.

Keywords: Information Security, Risk Management, Business Network, Extended Enterprise

Introduction

The increasing reliance of the world economy on the information infrastructure has raised questions regarding security and robustness at all levels of the economy, ranging from small firms who are dependent on the internet for select business communication to large multinationals that are extensively networked with their customers and suppliers (Johnson 2005). Today most companies are closely knit together with and thus dependent on suppliers, allies, customers, and public authorities. Henceforth, we define this the "extended enterprise" or "business network".

One example is MasterCard, who had problems when a data processing partner had a security leak and exposed millions of credit card records. Another example is the bulk electricity system, a critical infrastructure. The 2003 blackout in North America has demonstrated how local security incidents can spread across a business network. A failure in one operator's system resulted in a communication failure to connected network control centers and thereby a spread of the failure across multiple operators' systems.

This paper takes a first step towards developing a research agenda to advance efforts in this very important area. The objective is to emphasize the importance of security in business networks for research and practice. Since there is little research available, it wishes to raise major questions to be answered by a future research agenda. A basic research framework is presented in section 5 based on related research (section 2), an observation of the interdependencies of firms (section 3), and a series of cases from different industry sectors (section 4).

Related research

Although companies begin to assess and to mitigate the risk associated with information technology (IT) within their boundaries, little has been done in research or practice to analyze the risk emergent from the complex interdependencies in an extended enterprise or critical infrastructure. Related research that forms a ground to start from comes from three different domains: business networking, risk management and information security management.

Business networking

Business networking (Österle et al. 2000) describes the interorganizational co-operation between companies. Considering current trends such as greater organizational distribution of companies, increasing outsourcing, and the consistent integration of customers and suppliers, business networking is becoming a central object in restructuring organizations (Fleisch and Wintersteiger 1999).

Business Networking extends the three-level business engineering model (Baumöl et al. 2005) to cover inter-organizational relationships. At the strategy level, business entities represent the nodes of the business network. Business entities are profit-responsible and market-directed; examples include corporate groups, business units, SMEs and profit centers. A business entity encompasses a business strategy (definition of objectives), a number of business processes (e.g. processes of the supply chain) which translate the strategy into practice, resources (such as its workforce, information, capital) and relationships to other internal and/or external business entities. The edges indicate the co-operation relationships (typically blanket agreements or mutual participations) between business entities. Process networks implement the business network. Co-ordination relationships (edges) synchronize the business processes (nodes) of different business entities. The issues arising at each individual level of business networking cannot be addressed independently of each other.

As organizations increasingly rely on the internet to enable supply chain and value chain processes, the failure of any firm's information network has an impact on the extended enterprise of suppliers, collaborators, and channel partners (Davis and Spekman 2003). Critical supply chain processes such as order fulfillment, manufacturing flow, and procurement (Lambert 2006) depend on vast transactional data; understanding the implications and vulnerability of this flow of information within and across the extended enterprise is a significant and under-researched topic. Like the interdependent risks faced by other business partnerships (Kunreuther 2002; Kunreuther and Heal 2003), we hypothesize that information flow risks across trading partners exhibit many important risk management challenges; disruptions in this flow of information has the potential to severely disrupt economic activity at national and trans-national scales.

Risk identification and management

All firms manage information security risk either explicitly or implicitly. An analytical approach (e.g. Gordon and Loeb 2002) identifies a minimum level of information security investment that is required simply to do business – to be credible with potential customers and suppliers.

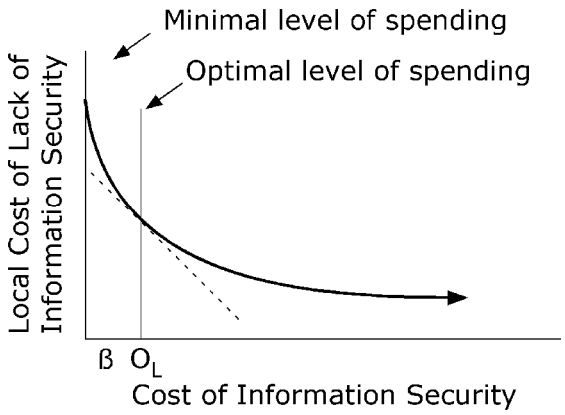

Figure 1 - Optimal level of local information security investment O_L. Within an organization, the optimal level of spending will occur when an increase in information security results in an equal decrease in costs due to information security lapses. After Gordon and Loeb 2002

The optimal level of cybersecurity investment is achieved when the marginal costs of increased information security equal the marginal decrease in the costs due to events such as virus attacks, hacking, break-ins, etc, as is shown in Figure 1.

Practically, in order for organizations to use such a method, they need to accurately know the costs incurred due to a lack of information security, their spending on information security, and have a good idea of what the marginal rate of return would be for a change in the spending. In reality, estimating many of these variables is difficult such as less tangible costs including the present and future costs of intellectual property losses or loss of future business due to brand damage.

An empirical approach (e.g. Dynes 2006a; Dynes 2006b; Dynes et al. 2005; Kumar and Tidas 2006) identifies not only risk within the firm, but also the risk to a business entity due to the interdependencies of technically mediated business processes. This approach explicitly recognizes that the ability of business sectors and critical infrastructures to provide products and services is dependent on the availability of the information infrastructure. An example would be RiskMAP, a process that explicitly maps IT risk to business risk (Watters 2007).

Information security management

A substantial amount of research effort already has been put into concepts for the management of information security as well as the underlying technology (Siponen 2005). Today there is an abundance of standards and guidelines for information security management and an organization has to choose which to comply with (Fumy 2004). Fortunately, if one looks closer at the standards and recommendations, it becomes clear that there are quite a number of common elements, which are conceptually equivalent even though different terminology and grouping of elements is used in different documents. The most prominent standard, ISO 17799, defines the 12 main categories. These are shown in Table 1.

Organizations trying to implement information security management in compliance with such standard requirements face various challenges. Among them there are the following:

- Quantifying risks is a complex task and the effort of doing so thoroughly is often hard to justify to management. Similar challenges arise when resources for information security operations need to be justified.
- Maintaining an accurate inventory of assets requires much effort and is often ignored, especially in emergency situations.
- Management of authorization is a complex issue; employees who are with an organization acquire broad privileges over time.
- Even though documented operational procedures exist, it is difficult and requires large efforts to ensure that they are being followed, especially in exceptional, unforeseen situations and emergencies.
- Security incident management allows an organization to learn from them and to improve but often raises negative press coverage and might raise attackers' awareness of the organization's vulnerabilities.

Table 1: Categories of Information Security Management Requirements

Risk assessment and treatment
Security policy
Organization of information security
Asset management
Human resources security
Physical and environmental security
Communications and operations management
Access control
Information systems acquisition, development and maintenance
Information security incident management
Business continuity management
Compliance

Firm and infrastructure interdependencies

Looking at existing extended enterprises we find an increasing dependency on technology to manage inter-firm relationships. Disruption of technical services will affect most firms, with effects ranging from severe at firms such as hospitals (which increasingly are holding patient records in digital form) and oil and gas companies (which are totally dependent on their digital process control systems) through disruptive at firms such as design houses, which use email to share designs amongst colleagues and to maintain a high level of contact with their customers, to of little or no consequence at what may be large numbers of very small suppliers (Dynes 2006b).

Technology also forms the core of many supply chain optimization efforts that spans from longer-term efforts such as forecasting of supply demand down to very short term efforts to optimize the placement of product on shipping pallets, and the placement of those pallets on delivery vans. This level of optimization increases productivity at the potential expense of flexibility in business operations.

Figure 2 diagrams an abstract value chain (suppliers, the firm, and its customers) for large manufacturing firms. In this figure, an important part of the supply chain relationship is the forecasts that are sent to important, high volume suppliers. These forecasts are very accurate for short time scales, and become increasingly inaccurate the further they look into the future. There will also be suppliers for which demand is not forecast; these are not shown.

In this figure, a possible supply chokepoint is denoted by **A**. Within the firm, there is the ability to internally produce the product using technology-dependent business processes; a possible chokepoint for internal production and delivery is denoted by **C**. Finally, there is the ability to ship completed product. In the figure are two classes of customers, large customers that order high volumes of products, and will provide forecasts for those demands, and small customers that will order small quantities of product at infrequent intervals. Two possible chokepoints in the ability of the firm to satisfy customers are denoted by **B**. Field studies have shown examples of each chokepoint, depending on how technology is used to optimize internal and external business processes (Dynes et al. 2005).

Figure 2 shows the interdependencies for a rather abstract view of the supply chain. In reality, the interdependencies within and across firms are much more complex. A recent study of an oil refinery showed that the greatest risks to the ability of the refinery to function came primarily from the utilities that supplied the refinery: water, natural gas, and other utilities. Without these the refinery would quickly shut down. In a hospital, each department can be viewed as a separate entity, connected with the other departments through an electronic medical record system. An internal failure of the network could have a major impact. Individual institutions in the financial industry are extremely interdependent and count on technology to enable all their financial transactions. When asked about what would happen if IP-based systems were to fail, one well-known banker responded by saying it would be a "snow day for the world".

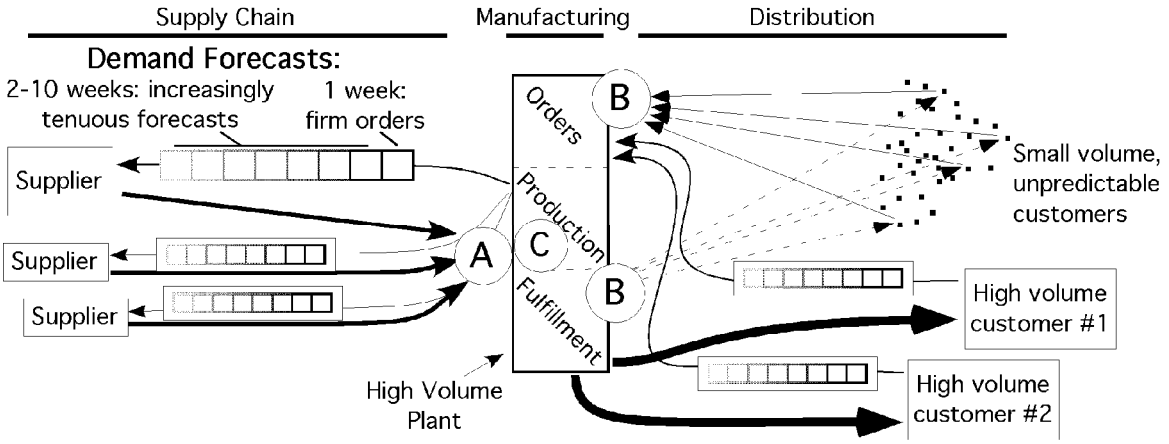

Figure 2. Schematic of high-volume plant value chain, showing suppliers, the 'plant' incorporating order processing, production and fulfilment, and distribution functions. Here, all suppliers are provided with forecasts of future demand; on the customer side high-volume customers who provide forecasting as well as smaller volume, occasional customers are represented. Three locations of possible interruption are denoted by A, B and C.

Insight from industries

In order to gain insight into a little understood and researched field, researchers have repeatedly suggested and successfully applied qualitative research methods such as case studies or expert peer groups (Benbasat and Zmud 1999; Myers 2002). In the following sections, a summary of challenges from three critical infrastructures are given.

Critical infrastructure and industrial process automation

The need for more research in the field of IT security for industrial control systems becomes ever more evident given the background of recent threats, including terrorist attacks. Recent findings show that the threat is reality rather than fiction (Amin 2002; Shea 2003). Further, as a result of introducing standard technologies including MS Windows and integration strategies for maintenance or control purposes, DCS and SCADA systems have become connected the corporate network; they are now as vulnerable to cyber attacks as the rest of the corporate network is (Dzung et al. 2005; Falco et al. 2004; Igure et al. 2006; Naedele 2005).

One example is oil and gas production on the Norwegian continental shelf (NCS). Here, two reasons speak for organizing the operations in an extended enterprise. First, oil and gas production companies traditionally have been operating their plants in segregated networks. Their staff typically has a strong mechanical or electrical engineering background and not much experience with regard to information security. Upcoming regulations and standards on information security (e.g. NERC CIP, ISA SP99) require such expertise; vendors of PCS typically have this expertise and can provide information security management as a service. Second, rising economic pressure forces the Norwegian oil and gas industry to increase efficiency of operations by leveraging technology enabled efficiency gains. To achieve this goal, the Norwegian Oil Industry Association (OLF) has developed the concept of integrated operations (OLF 2006). Since it is not economical for every operator to establish connectivity between on- and off-shore sites (e.g., remote control rooms and oil rigs) individually, the

Secure Oil Information Link (SOIL) has been put into place as a common network infrastructure. This off-shore system may be exposed to cyber security threats from the internet or enterprise networks of SOIL members if not proper information security management is in place. Automation system vendors have begun to use this infrastructure to offer their customers a wide range of remote monitoring and standard-compliant operations services.

However, some challenges similar to those mentioned in section 2 remain to be resolved:

- Management of authorization becomes a more complex issue the more organizations are involved. Even with remote monitoring and operations services, operator 's employees off-shore will still have to be able to access the system, e.g. to be able to act in emergency situations or in case of a failure in the connectivity to on-shore resources. This is hard when organizational boundaries have to be crossed.
- Authentication management becomes more complex when multiple organizations are involved, particularly when using stronger authentication methods such as public key infrastructures.
- Security incident management.
- Standards typically require information in transit to be encrypted, usually along the entire transit path. However, industry standards typically require operators of critical infrastructures to maintain a log of who performed which actions on the system, introducing additional monitoring steps whenever a connection crosses an organizational boundary.
- Maintaining an accurate inventory of assets must be part of the service offering if the goal is to provide standard compliant operations; this is important due to strict change management procedures.
- Different solutions for similar tasks exist which are incompatible with each other (e.g. for interactive user sessions solutions based on Citrix' ICA protocol or Microsoft's RDP can be chosen), forcing a vendor tot either require its customers to use one particular choice or the vendor must support virtually every choice his customer may require.

Manufacturing

We now turn to results from field studies that we have been conducting with manufacturing organizations. The basic form of these field studies was to identify a 'host' organization; we would travel to that host and conduct interviews around these issues. We would then ask the host organization to introduce us to a few of their key suppliers, we would then travel to these suppliers and conduct similar interviews. We present results from an electrical components organization and an automobile parts organization. The electrical organization served a combination of both high and low volume customers. The automotive organization was a tier 1 supplier to the automobile industry, meaning that its products went directly in to the finished product, rather than a sub-assembly. At the time of the field studies these organizations managed a substantial percentage of their supply chain using electronic communications (either EDI or a web portal); both were both involved in efforts to move all their supply chain communications to the internet. If successful, these organizations would be completely dependent on the internet for their normal supply chain management.

The host's suppliers were much more variable with respect to their dependency on the Internet. Most communicated with their suppliers using phone and fax, and were much less susceptible to interruptions of their supply chain due to Internet outages (Dynes et al. 2005). These tier-two suppliers were also less dependent on the Internet for communication with their customers as well. For these suppliers the major impact of an Internet event would not be supply chain or production disruptions, but in customer service via email.

Given this level of interdependency, what would be the impact of an internet outage on the ability to produce and deliver product? Consider the electrical parts manufacturer, which produced electrical products that range from small, very high volume items such as fuses and switches to large, very low volume items such as power-station transformers. Because of the long lead time required for parts that make up these large items, they must be ordered days or weeks in advance. An internet disruption the day an order needed to be placed would mean that the order would have to be placed by phone or fax. Since these were low-volume items, phone or fax ordering is entirely feasible.

The high-volume goods that this manufacturer also produces require frequent electronic communication of stock on hand and forecasting of demand with suppliers. A forecast to a supplier would typically reiterate this week's order and progressively ill-defined estimates of orders up to ten weeks out. This forecasting and the history between the suppliers and the manufacturer result in what one interviewee termed a "supply chain learned behavior". If the Internet were to fail, the suppliers would still deliver the needed supplies without any prompting from the manufacturer due to this 'learned behavior'.

The major impact of an Internet outage on the high-volume plants would likely be not a supply-chain issue, but an order fulfillment issue (Croxton 2002). Large customers would likely have forecasting and a 'learned supply chain behavior' in

place and shipments would be packed and shipped as expected. At the opposite end of the spectrum would be hundreds of smaller customers without forecasting; it is unlikely that the hundreds of faxes and/or phone calls for one or many products in various volumes could be handled Production and packaging would continue, but except for large customers these packages would accumulate on the shipping dock as the fulfillment system failed for smaller, ad-hoc orders.

This is shown graphically in Figure 2 by the point **B**, indicating the inability of the plant's order processing and fulfillment functions to cope with the volume of orders that would have been placed via the web, but are being phoned and faxed in due to the disruption of the Internet.

The automobile parts manufacturer adopted a different approach to supply chain management than the electrical parts manufacturer, which adopted a more just-in-time approach to supply chain management. While the auto parts manufacturer shares forecasting information with local suppliers of sub-assemblies, the manufacturer ran its own fleet of trucks to pick up these sub-assemblies. To increase efficiency the manufacturer was explicit about how items should be packed, and when they should be ready for pick-up. These suppliers would not prepare items for pickup or delivery unless they were explicitly told to do so by the manufacturer.

One outcome of this strategy was the lack of a 'learned supply-chain behavior': without communication supplies would not be delivered. From our analysis of the number of suppliers, the part counts and the frequency of ordering it is doubtful that these communications could be replicated via fax. As a result, there would be a restocking shortfall during an Internet outage.

On the customer side, the organization had a few very large customers that forecasted their demand; shipments to these customers would likely be limited by production rather than managing order communication. In the case of the auto parts manufacturer, the bottleneck would not be in the order processing and fulfillment functions, but at the point in Figure 2 labeled by **A**: the ability of the supply chain to effectively respond to stock shortages due to the supply chain timing and packing optimizations utilized.

Financial services

The financial services industry is in the middle of a structural change (Lehmann 2000). Increasing competition and customer demands require that financial services companies focus on core competencies in order to deliver better value to their customers. Consequently, companies that were formerly highly integrated have split into divisions or independent companies focusing on different parts of the value chain (Heinrich and Leist 2002). On the other hand, many customers demand a complete range of financial products in order to satisfy their financial needs "one-stop". This forces financial services companies to collaborate with providers of complementary products and services. Ultimately, networks of financial services companies ("financial services networks") emerge (Alt and Reitbauer 2005).

Privacy constraints are a major issue in almost all the financial service networks examined (Geib et al. 2006). The privacy protection laws in Europe are much stricter than in the U.S., making it more difficult for network partners to exchange customer data. Customer data is essentially bound to the company that collects it, and can only be used for the stated purposes. Special privacy laws prevent banks from sharing any customer data without a court order – even with their customers' permission. Consequently, partners may share data with banks, but banks cannot share data with partners.

Some product providers cooperate with several small and medium banks that act as relationship managers. They acquired their customers' consent to share personal data with the banks through their general terms and conditions, with only a few customers refusing to provide this consent. Due to privacy protection laws in Europe, only relationship managers are allowed to have access to all the personal customer information available in the network as they need it for comprehensive customer consulting (Fromholz 2000). These data are, of course, interesting for product providers as well for analytical customer relationship management, or to improve product innovation based on knowledge about customers. A solution to the privacy problem may be for relationship managers to make customer data anonymous before giving it to product providers. The latter can then analyze the anonymous data and build models to improve the product innovation and customer scoring of their products.

Figure 3 summarizes the findings from the analysis of financial services networks (Geib et al. 2006):

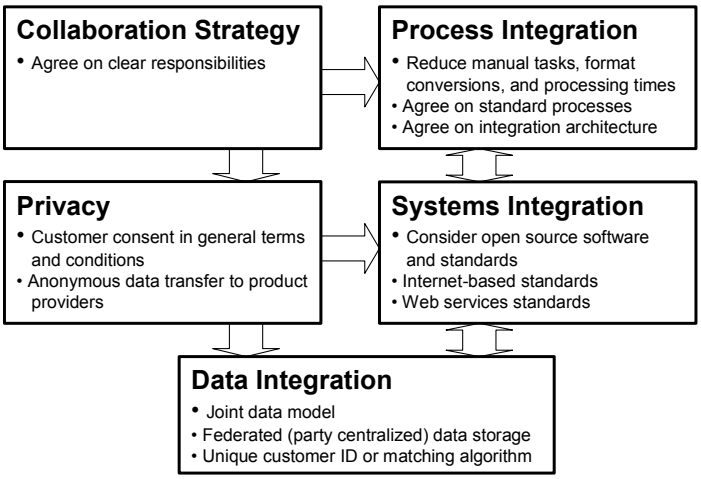

Figure 3: Requirements for business networking in financial services including customer data security issues

Building blocks and research issues for information security in the extended enterprise

Putting a box around managing the risk associated with increasing dependency on the information infrastructure is challenging. At a minimum, a risk framework would include the economic impacts of various cyber incidents in the extended enterprise, the resiliency of those extended enterprises, the incentives that are present for individual firms to manage these risks, and a definition of what constitutes an acceptable level of cyber risk from firm, sector and greater public good perspectives.

As the related research and the observations from different vertical industries show information security in the extended enterprise needs to be assessed on at least four levels:

- Strategy: It is clear from the above that information security is becoming a key enabler of corporate strategy. Information security risk should be viewed in this context, along with the risk referred from all the partners and suppliers in the extended enterprise. Information security strategy thus becomes a shared property of collaborative business entities, with common objectives and basic standards across all partners.

  Core research questions include:

  a. Conceptually, what is an appropriate level of information security for a particular business network: what level is the goal ("good enough")? If firms are adopting levels of information security perceived adequate for their local good, what more needs to be done to provide a level adequate for their extended enterprise? Their business sector? The greater public good? This is a key question that would integrate and provide focus to many ongoing efforts.

  b. How do business entities arrive at a consensus regarding their joint risk posture? In order to avoid free rider and negative externality issues, strategies must be developed to assure that in any agreement all entities benefit and are responsible.

  c. At individual entities, how is a business case for risk taking and mitigation developed?

- Processes: Processes must be aligned across partners and also assessed for business and security vulnerabilities. It becomes clear that processes as operational links between strategy and systems have a crucial function in translating strategic imperatives into systemic action.

  Core research questions include:

  a. How are inter-organizational business risk management process defined? Different entities will have different risk appetites, and prioritize risks differently; how can a shared vision be achieved?

  b. Who is responsible and accountable for what? While it may be assumed that each partner will manage their part of the effort, process transparency will likely benefit all parties.

c. Are inter-organizational processes at each entity really equivalent?

d. How can measurement and reporting be implemented?

- Systems: Once a common security strategy is in place and processes for active risk management across companies' borders are agreed on, the actual implementation of the business and risk processes will require systems level support. At this level, intra-firm interfacing and integration issues are obstacles to achieving the information security objectives the extended enterprise.

  Core research questions include:

  a. Are access rights and roles technically feasible across partners?

  b. Is it possible to audit systems to assure conformance with standards and regulatory requirements?

  c. What is an acceptable way for partners to assure the systems actually reflect strategy and process requirements?

- Culture: Risk needs to be identified and managed at 'design' time, not bolted on later as is often the case today. To make this change and meet the challenges laid out above requires a substantial cultural change, not only in the way individual entities think of internal information risk, but in the types of trust relationships entities have with each other.

  Core research questions include:

  a. Are business entities willing to share the level of information required for a successful effort? While entities may partner in certain contexts, they could be direct competitors in other contexts. How can entities efficiently compartmentalize information regarding processes and intellectual property

  b. Are the security cultures harmonized, e.g. when working with outsourcing partners abroad that may trade security quality for lower costs?

- Incentives: Even the best processes and systems that would allow firms to effectively assess and manage the information security risks they face in the extended enterprise will be useless unless they are adopted and utilized by firms. It follows that an essential building block is providing motivation for firms to adopt and put into practice the results of the preceding building blocks.

  Core research questions include:

  a. What motivates firms to adopt certain levels of information security? While there are studies that have detailed security investment practices in certain firms, it is clear that existing efforts are descriptive rather than prescriptive. Understanding the range of approaches is necessary for developing best practice guidelines that can be reasonably applied by a majority of firms.

  b. What is a proper role for government? Few experts or practitioners feel that government regulation is the best alternative as they agree that firms ought to be in the best position to know their risks. Despite this, there is a valid concern that firms are not doing enough to protect the critical infrastructures that are required by society, and such regulation may be needed to assure that information security risks across critical infrastructures are comprehensively managed.

An invitation to future research

Not only do the levels and their exemplary questions – as mentioned in the previous section - pose challenges for the business world, but by the same token open a field for academic research that spans different disciplines such as management, information technology and organizational science. The increased complexity of the networked enterprise – in most cases operating in different cultures and regulatory environments – prevents a quick solution and itself raises the need for future research. Incentives for meeting some level of information security are a key research area. All firms have incentives to adopt a level of information security sufficient for the firm's local good – to be seen as a credible business partner by customers or suppliers, or through regulatory mechanisms. For some sectors, the level of information security needed for the good of a

business sector (an aggregate of many extended enterprises) may significantly exceed that needed for the good of the firm. Are there sufficient incentives for firms to take the steps needed to meet that higher level of security? Looking at the bigger picture, it is an open question as to what level of information security is needed for the greater public good.

Acknowledgments

The effort by S. Dynes was supported under Award number 2000-DT-CX-K001 from the Office for Domestic Preparedness, Department of Homeland Security. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security.

References

Alt, R., and Reitbauer, S. "Towards an Integrated Architecture and Assessment Model for Financial Sourcing," FinanceCom05, IEEE, Regensburg, 2005, pp. 67-74.

Amin, M. "Security Challenges for the Electricity Infrastructure," *Computer* (35:4) 2002.

Baumöl, U., Österle, H., and Winter, R. (eds.) *Business Engineering in der Praxis*. Springer, 2005.

Benbasat, I., and Zmud, R.W. "Empirical Research in Information Systems: The Practice of Relevance," *MIS Quarterly* (23:1) 1999, pp 3-16.

Croxton, K.L. "The Order Fulfillment Process," *The International Journal of Logistics Management* (14:1) 2002, pp 19-32.

Davis, E.W., and Spekman, R.E. *The Extended Enterprise: Gaining Competitive Advantage through Collaborative Supply Chains* Financial Times Prentice Hall Books, 2003.

Dynes, S. "Information Security and Health Care – A Field Study of a Hospital After a Worm Event," Center for Digital Strategies Tuck School of Business, Hanover, MA.

Dynes, S. "Information Security Investment Case Study: The manufacturing Sector," Center for Digital Strategies Tuck School of Business, Hanover, MA.

Dynes, S., Brechbühl, H., and Johnson, M.E. "Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm," Workshop on the Economics of Information Security, Cambridge, MA, 2005.

Dzung, D., Naedele, M., von Hoff, T., and Crevatin, M. "Security for Industrial Communication Systems," *PROCEEDINGS OF THE IEEE* (93:6) 2005, pp 1152-1177.

Falco, J., Gilsinn, J., and Stouffer, K. "IT Security for Industrial Control Systems: Requirements Specification and Performance Testing."

Fleisch, E., and Wintersteiger, W. "Business Networking and Software Quality Management," 6th European Conference on Software Quality, ADV Handelsgesellschaft, Wien, 1999, pp. 56-70.

Fromholz, J.M. "The European Union Data Privacy Directive," *Berkeley Technology Law Journal* (15:Annual Review of Law and Technology) 2000, pp 461-488.

Fumy, W. "IT Security Standardization," *Network Security* (2004:12) 2004, pp 6-11.

Geib, M., Kolbe, L.M., and Brenner, W. "CRM collaboration in financial services networks: A multi-case analysis," *Journal of Enterprise Information Management* (18:6) 2006, pp 591-607.

Gordon, L.A., and Loeb, M.P. "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* (5:4) 2002, pp 438-457.

Heinrich, B., and Leist, S. "Nutzung und Entwicklung von Geschäftsmodellen - Ergebnisse des Kompetenzzentrums Bankenarchitekturen im Informationszeitalter," in: *Business Engineering,* H. Österle and R. Winter (eds.), Springer, Berlin et al., 2002, pp. 329-352.

Igure, V.M., Laughter, S.A., and Williams, R.D. "Security issues in SCADA networks," *Computers & Security* (25:7) 2006, pp 498-506.

Johnson, M.E. "A Broader Context for Information Security," *Financial Times*:September 16th) 2005, p 4.

Kumar, R.T., and Tidas, M. "Enterprise Information Security: Who should mange it, and how?," Workshop on the Economics of Information Security, Cambridge, England, 2006.

Kunreuther, H. "Risk Analysis and Risk Management in an Uncertain World," *Risk Analysis* (22:4) 2002, pp 655-664.

Kunreuther, H., and Heal, G. "Interdependent security," *Journal of Risk and Uncertainty* (26:2) 2003, pp 231-249.

Lambert, D.M. (ed.) *Supply Chain Management: Processes, Partnerships, Performance*. Supply Chain Management Institute, Sarasota, FL, 2006.

Lehmann, A.P. "Financial Services - Veränderungen von Märkten, Leistungen und Unternehmen," in: *Dienstleistungskompetenz und innovative Geschäftsmodelle,* C. Belz and T. Bieger (eds.), Thexis, St. Gallen, 2000, pp. 22-35.

Myers, M.D. "Qualitative Research in Information Systems," MISQ Discovery, 2002.

Naedele, M. "IT Security for Automation Systems," in: *Industrial Information Technology Handbook,* R. Zurawski (ed.), CRC Press, 2005.

OLF "Potential value of Integrated Operations on the Norwegian Shelf," OLF.

Österle, H., Fleisch, E., and Alt, R. "Business Networking: Managing the Transformation Towards Networked Enterprises," in: *Business Briefing: Global Electronic Commerce,* E. Cooper (ed.), WMRC, London, 2000, pp. 172-174.

Shea, D.A. "Critical Infrastructure: Control Systems and the Terrorist Threat," Report for Congress.

Siponen, M.T. "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods," *Information and Organization* (15:4) 2005, pp 339-375.

Watters, J. "Risk-to-mission Assessment Process (RiskMAP)," Process Control Systems Forum 2007 Annual Meeting, Atlanta, GA, 2007.