# Identifying Risks and Building Trust in Global Supply Chains

Bonnie W. Morris
College of Business & Economics
West Virginia University
PO Box 6025
Morgantown, WV 26506-6025
bmorris@wvu.edu
304 293 7851

"Trust is fragile, hard to build, and easily lost."[1]

## Introduction

At West Virginia University, we are engaged in a program of research related to the role of continuous auditing in identifying risks and building trust in a number of contexts. One of the main focuses of our work is on the use of continuous auditing to build trust in supply chains.

Global supply chains are subject to two significant sources of risk: Damage to the telecommunications infrastructure, which is the backbone of the supply chain, and errors or attacks on the reliability, integrity, or availability of the system that are carried out through the supply chain itself. Our interest is in the latter.

## Background

Global supply chains are complex webs connecting firms around the world. Supply chain interactions are not just about exchanging purchase orders and invoices. Many organizations link production planning, inventory management, engineering design, logistics and distribution, and payment systems to their procurement and order processing systems. The goal is to improve customer service by being more responsive, reducing costs and improving efficiency.

The development and use of electronic supply chains will increase. Large powerful customers will demand that their vendors participate. The automotive industry is an excellent example. The Big Three U.S. automakers not only require their first-tier suppliers to participate in electronic trading, they also have begun to mandate participation by second and third-tier suppliers.

All distributed networks are inherently risky. The Internet is the largest distributed network and is subject to many risks, but even private networks have increased risk due to the number of access points. As the number of organizations participating in supply chains increases, the exposure to extreme losses grows. The exposure relates to reliability, integrity, and availability. For example, InformationWeek reports that Covisint, the automotive industry exchange, is

[1] Keen, Peter G. W. (Editor), Craigg Ballance, Sally Chan, and Steve Schrump. (1999). *Electronic Commerce Relationships: Trust By Design.* Prentice Hall. Upper Saddle River, NJ: p 6.

handling 100 million supply-chain procurement transactions per month between the automakers and 2,000 different suppliers.[2] This volume is approximately equal to the entire procurement for one automobile company. The Covisint exchange affects the entire automotive industry.

There is always a trade-off between control and access. The more distributed the network is, the more points of access and the less control the organization has. Giving customers greater access via the supply chain may increase customer satisfaction, but it reduces control. Giving vendors access may improve inventory management, but it reduces control.

Risk analysis should lead to decisions about investment in security measures and changes in business practices. Calculating the return on IT investments is difficult under any circumstances, but even more so for IT security investments in a networked environment. The interconnectivity of supply chain participants means that the security of any participant can be jeopardized by weaknesses in security and business processes at any of its trading partners. The impact may affect more than just one pair of trading partners. Due to the networked nature of the supply chain, there is a significant risk that security breaches that affect the reliability, integrity or availability of the system will propagate through the entire supply chain.

The inadvertent disclosure or theft of intellectual property or other confidential, proprietary information such as customer or vendor data can be catastrophic for a business. The potential seriousness of such threats is demonstrated by the results of the 2001 CSI/FBI Computer Crime and Security Survey.[3] Although it was not a scientific survey[4], the magnitude of the losses reported is noteworthy. The greatest category of loss was due to disclosure or theft of proprietary information. One respondent estimated the value of lost proprietary information from one single incident at $50 million. Perhaps more significant than the direct monetary loss is the loss of reputation and trading partner trust.

## Control and Audit

Control and audit are often thought of as bureaucratic overhead to be minimized. It is more productive in this environment to think of control as an element of quality—the quality of the security and business processes. Security and control can be market differentiators.

In the supply chain environment, Trading Partner A has incomplete information about the quality of security and business practices of Trading Partner B. Independent third party audits add value by creating mechanisms for trust among trading partners. Audit has value to Trading Partner B because it is a means of signaling the high quality of its security. Increased trust lowers transaction costs.

Continuous auditing provides additional information. Periodic audits provide information about the quality of security and control at a point in time. There is uncertainty about compliance with established procedures during the interim. Continuous audit provides continuous monitoring of *compliance* with policies and provides substantive evidence of the *effectiveness* of the controls. Finally, audits provide an insurance effect. When independent auditors provide assurance about

---

[2] Konicki, Steve. "Covisint Handles 100 Million Supply Transactions Monthly." Feb. 25, 2002 http://www.informationweek.com/story/IWK20020225S0010 .

[3] Power, Richard. "2001 CSI/FBI Computer Crime and Security Survey." *Computer Security Issues & Trends.* Vol VII, No. 1. Computer Security Institute.

[4] It was a convenience sample with a likely significant self-selection bias due to a 14% response rate.

any business activity, they assume some risk. The consumers of the audit have recourse against the auditors (see Andersen and Enron).

## Research Directions

The handling of intellectual property, including information that is transmitted as an attachment to support requests for payment, is a particularly interesting issue. Consider a subcontractor, perhaps an engineer, who is to receive progress payments on project. The subcontractor submits with the invoice a statement of the specific tasks completed to date. That information may very well include sufficient detail to compromise either the vendor or customer's intellectual contribution relating to processes, design, or products. The development of controls for reducing that vulnerability and the development of audit procedures for assuring the protection of that information is an interesting research area.

There are also a number of general research issues that we are investigating.

- Metrics—direct measurements of system activity that can be compared to an a priori or historical standard to deviations from the norm and changes over time.

- Analytics—identification of logical or empirical relationships that can be used to flag transactions for further review.

- The use of case-based reasoning to detect low probability, high impact events.