KNOWLEDGE-SHARING IN VALUE-CHAIN NETWORKS: CERTIFYING COLLABORATORS FOR EFFECTIVE PROTECTION PROCESSES

G. Scott Erickson, Helen N. Rothberg, and Chris A. Carr

INTRODUCTION

Three major trends have come together at the start of the new millennium, raising the stakes for firms seeking to compete in the new economy. Initially, knowledge management (KM, also referred to as intellectual capital) poses the idea that every organization holds knowledge in the minds of its personnel that can be identified, collected, and managed for competitive advantage. Relatedly, modern internet technology has enabled knowledge management to be more easily accomplished while also taking the concept outside of the firm's borders. With advanced data management capabilities, instant communication throughout a network, and a mechanism to tie together disparate computer systems, cutting-edge firms are able to use the knowledge of their entire value chain as a competitive weapon.

The third major direction in business dampens this enthusiasm regarding knowledge management and e-business. Competitive intelligence (CI) has also grown apace over the past decade. Legitimate competitive intelligence activities pose a particular threat to internet-driven knowledge-sharing networks for a number of reasons, but the principal problem is more knowledge, in more heads, under less control, and in digital form. Competitive intelligence activities are on the rise and these types of systems are particularly subject to attack.

The question is what to do? On the one hand, knowledge management and e-business networks both offer a lot to firms seeking to differentiate themselves from competitors. On the other hand, such systems open firms up to competitive intelligence efforts from those same competitors. Can the systems be constructed so as to be useful, but to protect firms from CI incursions? Central firms in KM/e-networks obviously need to monitor what information is passed on to which suppliers, vendors, research or manufacturing partners, customers, etc. In order to keep control of the systems, however, and not arbitrarily favor one collaborator over another, we suggest that a certification system might be appropriate. Such a system would alert collaborators as to the steps necessary to qualify for various levels of participation within the network. Certification would also make the decision objective, hopefully lessening any tensions that may come from collaborators not immediately qualifying for higher levels of participation.

LITERATURE REVIEW

Knowledge management grew out of practice, with academics latching on to the topic only in the last few years (Edvinsson & Malone, 1997; Davenport & Prusak, 1998). The basic idea is that all organizations possess a certain amount of tacit knowledge, knowledge held by individuals that helps them or the firm perform better. If this knowledge can be made explicit,

captured by the firm so that it knows what knowledge assets it holds, the firm benefits (Nonaka & Takeuchi, 1995). Explicit knowledge can be organized and then further leveraged by distributing it to other employees who can, then, also perform better. Traditionally, KM is divided into three categories (Bontis, 1998). Human capital is individual knowledge about how to perform a job. Structural capital is knowledge about how to organize organizational resources (capital, labor, or even knowledge) to best effect. Collaborative capital is knowledge about how to deal with friendly parties outside the firm (suppliers, vendors, customers, etc.). Competitive capital has also been suggested by some—knowledgeabout competitors and how to compete with them—asan additional source of a knowledge asset (Rothberg & Erickson, 2001). As noted, the point of KM is to identify tacit knowledge assets in these various categories. If the firm can capture this tacit knowledge and make it explicit, the entire organization can benefit from it. The result is a firm managing its knowledge resources better than their competitors, leading to superior performance in the marketplace.

Into this KM mix has come the internet revolution of the past 6-8 years. Dotcoms are failing left and right and rapidly disappearing from view. Similarly, B2B exchanges are not showing the promise of a couple of years ago. But private exchanges continue to show some strength (Benoit, 2001; Harris 2001). It's no accident that systems firms IBM and SAP are still making money as a number of new economy stars are declaring record losses. A number of firms may have put off information technology investments during the new economy downturn, but investment is still taking place in proprietary systems that integrate a firm's value chain. As conditions improve, these investments will undoubtedly pick up as organizations seek to stay competitive with others in their industries. What an e-business network essentially does is establish communication links across the value chain (*The Economist,* 2000; *The Economist,* 1999). In some ways, the network is a newer version of ERP systems, but these go further. Initially, e-networks use the internet, resolving some of the

expense problems involved in setting up expensive electronic data interchange systems with all suppliers. For the price of an internet connection, anyone can now be part of the network. Secondly, e-business networks tend to incorporate more functions than is the case with pure ERP systems. The trade literature often now groups e-network functions into three categories: ERP, supply-chain management, and customer relationship management (CRM). ERP generally refers to organizing the resources of the firm to fill customer orders, perhaps including first-tier suppliers (as original ERP systems tended to do).

Supply-chain management has to do with integrating the entire supply chain to fill customer orders-- not only first-tier suppliers, but suppliers of suppliers of suppliers. Hand in hand with this is CRM, which electronically takes orders from customers, feeds them into the other parts of the network, and allows the customer to monitor the status of such orders. All of this is based upon the Dell model, in which an order is taken from a customer via the web and all parts of the company and its supply chain are immediately alerted as to part and resource needs. In real time, as the customer places the order, a supplier far down the chain knows immediately what the core firm, several links above it, requires and when.

E-networks are essentially just another tool for passing information throughout the supply chain-- a tool that makes life easier by allowing instantaneous, easy communication throughout this sometimes vast apparatus. In a number of ways, it is conducting knowledge management, even in its most basic form. Information from sales is immediately shared with the supply chain, and vice versa. Further, the system can be adapted to purer KM functions, using this type of system to collect and store knowledge from throughout the value chain, then making it available, as needed, wherever in the chain it might be needed. So customer likes and dislikes (collaborative capital) can be shared through this type of system with an R&D partner far upstream. Alternatively, an operator's knowledge of what works well on a particular piece of processing machinery (human

capital) could be shared downstream with a vendor who can price a product accordingly. KM is all about sharing knowledge, and e-networks are uniquely well-adapted to such purposes. The two fit together hand-in-glove, even when the e-networks are not established solely for the purpose of knowledge management. For both reasons, firms look to data exchange through such established mechanisms as a means to competitive advantage.

One interesting extension to this perspective has become a trend in core firms working on various operational activities with collaborators, in an attempt to bring collaborators' competencies up to the same level as seen in the central organization. The earliest stages of the trend were in quality as outside certifications of quality (ISO 9000, milspec) were initially used to validate the quality abilities of supply chain members. At a number of the larger firms, this tendency moved into proprietary certifications, as at the major auto manufacturers. Not only did firms such as Ford name Ford-certified suppliers, but they worked with closely-related firms to get them that certification. Similarly, GE worked on moving collaborators throughout its supply chain toward Six Sigma.

In recent years, this trend has extended to other activities, such as new product development and lean manufacturing. John Deere, for example, works directly with suppliers on reducing cycle time, lowering inventory, increasing on-time delivery, and other aspects of modern operations management (Ericksen, 2002). It's quite common in industry for extended enterprises to share expertise in managing aspects of the value chain. Incorporating knowledge management not only implicitly but explicitly into this structure makes a lot of sense. Core firms can and should take the initiative to install better knowledge management, processes throughout the extended network.

The fly in the ointment with this prospect is found in the growth in competitive intelligence activities over the past decade. CI, in legitimate circles, uses publicly available information, internal sources, and active

information-gathering to discern competitors' activities, processes, and strategies (Eells & Nehemkis, 1985; Meyer, 1987; Gilad, 1994; Gilad, and Herring, 1996). Illegal CI efforts also exist, of course, such as hacking and outright theft. This discussion will focus on legitimate activities, but recognize that the possibility of questionable CI just further strengthens the points made. Publicly available sources used by CI groups can include the business press, regulatory filings, patent filings, annual reports and other financial documents, and any number of other generally available information. Internally, CI takes advantage of employees hired in from competitors or other outside organizations, employees with contacts with outside organizations, and any other inside sources that have information regarding competitors. Finally, active CI functions include everything from infiltrating customer presentations, to simply calling up and asking for information. Dumpster diving, for example, is a typical aggressive CI activity practiced where legal.

CI can be organized in a number of different ways, but much like KM systems, competitive knowledge needs to be gathered from disparate sources, combined, and analyzed by someone with the skills to make sense of all the pieces of information. The point about CI is that its practice is expanding as firms find that such detailed knowledge of competitors can be useful in the marketplace. Into this environment comes KM/e-network structures that freely distribute information across an organization's entire value chain. Rather than individual tacit knowledge, targets within and without the firm theoretically have access to an organization's entire explicit knowledge base. The bottom line is more CI targets, each with a greater share of its network's knowledge base, inside and outside the core firm (and, therefore, less controllable), and holding the knowledge in an easily transportable, hard-to-track digital form. In such a circumstance, should firms take advantage of the promise of KM/e-networks or hold back on them so as to guard their proprietary knowledge assets?

THE ECONOMIC ESPIONAGE ACT OF 1996

Inside the firm, any company has a certain amount of control. Traditional intellectual property protection mechanisms such as patents and trademarks can be used on some knowledge assets. The problem occurs when trade secrets are used outside the firm, as in e-networks. What can a firm do to establish protection mechanisms for shared knowledge assets? One answer in the U.S. is found in the Economic Espionage Act of 1996 (EEA) (Carr, Morton & Furniss, 2000). The EEA was specifically adopted in order to combat perceived intelligence activities conducted by non-U.S. companies or, even governments. In practice, the terms of the legislation provides a number of unique opportunities for firms looking to use KM/e-networks systems. Initially, the EEA more formally defines what is and what is not a trade secret. Under the terms of the act:

> The term "trade secret" means all forms and types of financial, business, scientific, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, if:
> (A) the owner thereof has taken reasonable measures to keep such information secret, and
> (B)the information derives independent economic value, actual or potential from not being generally known to , and not being generally ascertainable through proper means by the public (18 U.S.C. § 1839(3), Supp. IV 1998).

As might be inferred from this statute, the definition fits knowledge management systems like a glove. Although not immediately apparent in terms of the traditional view of trade secrets, the knowledge as an asset

approach can help to establish the knowledge as something of economic value. As such, it is, then, protectable if the proper steps are taken to keep the information proprietary. The trick, then, is taking "reasonable measures to keep such information secret." Can this be done in a far-flung e-network involving everyone from customers to collaborators to suppliers to suppliers of suppliers? In taking reasonable measures firms need to recognize that although an e-network works best with the fullest sharing of information, it is incumbent on the core firm in any such network to have some system in place establishing how and to whom to release information. What would such a system encompass? As with supplier quality certification programs such as ISO 9000 (or, more pertinently, private certifications such as those at the major automakers) and environmental certification programs such as ISO 14000, an objective system with well-understood standards would work best in terms of meeting the law and ensuring that suppliers understand their status and what they need to do if they desire to improve it.

AN EEA COMPLIANCE CERTIFICATION PROGRAM

Several steps are necessary in order to establish knowledge as the trade secrets that a core firm in the e-network wants protected. Initially, before the knowledge is ever distributed to anyone, the firm must designate the information as valuable and an organizational asset. In this regard, the firm, in combination with a KM system, should conduct an audit of its valuable knowledge, determine the value, conduct a risk assessment to determine the likelihood of loss, and implement its own security measures, including everything from firewalls to softer mechanisms that incorporate common-sense measures that are described in the following (Fraumann & Koletar, 1999). Once the internal mechanisms are in place, the firm should take the following steps in terms of establishing a compliance system for collaborators. Earlier, we discussed how sharing expertise throughout the extended enterprise has been an increasingly common occurrence in

industry, and how such tendencies clearly could include knowledge management. As an additional extension, there is no reason not to include proper knowledge protection procedures among the shared expertise, and, indeed, to ensure that anyone participating in the virtual corporation can be certified as installing appropriate steps for knowledge protection.

What would this certification process include? Initially, any collaborator seeking to become part of the corporate e-network needs to establish that it has appropriate general security measures in place. These include such steps as the aforementioned firewalls, designating information "Confidential" or "Do Not Copy," controlling access with passwords or other means, implementing appropriate destruction practices, and employing encryption in communications (Carr, Furniss & Morton, 2000). As noted, these should be present in the core firm and become part of the assessment procedures of prospective partners. In addition, in terms of employees, a danger always exists in terms of those leaving the employment of a collaborator firm and going to a competitor. Firms often protect themselves with noncompete agreements, and these types of documents should be extended throughout the network. Although they often protect themselves, core firms in e-networks can overlook the possibility of employees of suppliers of suppliers of suppliers (as an example), with similar access to sensitive information, going to work for a competitor or a competitor's e-network.

As a result, not only the core firm but certified suppliers should establish that they have instituted noncompete, nondisclosure, and nonuse agreements. These are limited in their effectiveness as some states bar their enforcement (and EEA does not prevent employees from using their own "general knowledge, skills, and expertise") but they are important in terms of establishing the intent to keep knowledge secret. Further, collaborator firms should be able to show that they require departing employees to return sensitive documents, clean the drives on personal computers, and provide pre-clearance for future positions, allowing the previous firm to alert the

new employer not to use certain proprietary knowledge the employee may possess (Berkent Legal Services, 1997).

Compliance responsibility should exist at a high level of the firm, showing again that management of the knowledge is a high priority. Not only should the compliance standards noted above be clear, but an individual or team with sufficient authority should be charged with ensuring compliance throughout the collaborator organization. From a different perspective, the firm can also protect itself from being charged with violations of the EEA if it takes steps to ensure that knowledge coming into the organization (e.g. from newly-hired employees) is not tainted. The compliance officer or team should be able to determine the noncompete agreements applying to the new employee. Again, this type of procedure would be important in showing a professional approach to knowledge management of the collaborator organization itself, helping to ward off EEA problems and establishing proper controls on its own knowledge assets.

Collaborator firms, to show compliance with the spirit and intent of EEA, should also be able to establish that effective systems are in place to communicate the knowledge management standards throughout the organization (and, perhaps, on to the firm's own sub-network of collaborators). In assessing the effectiveness of both the standards and communication, participating firms also need to monitor compliance. Reasonable steps to discover and plug knowledge leaks should be documented and recorded in certification reports.

If e-networks intend to pursue outside firms for lifting trade secrets, they need to have their own response mechanism in place for handling these knowledge leaks. Further, as noted in the compliance subsection above, this response mechanism, to be fully-compliant, should also deal with violations of others' trade secrets by e-network members. If contaminated information does make its way into or out of the e-network, the core firm

and other collaborators should be able to show that procedures exist to discern violations and prevent further use of the knowledge.

In summary, these specific steps can be organized into an effective certification system for core firms in e-networks to use in assessing the ability of collaborator firms to participate fully in the knowledge management system. Indeed, the specific categories can be organized into a checklist for a certification/audit document used to assess prospective members' ability to adhere to the protection mechanisms of the core firm's e-network. Different degrees of compliance can be determined, resulting in "security clearances" determining how much of a network's knowledge assets a collaborator can be exposed to. As the collaborator implements more effective systems, it may acquire higher certification levels and the attendant business benefits that come from participation at the highest levels of an electronic value chain.

CONCLUSION

As firms move into the new reality that is e-networks and competition between global value chains, rather than simply between individual organizations, they need to give consideration to what gains them competitive advantage. In many ways, in the new economy, this competitive advantage can come from the most efficient use of knowledge assets. With modern communication and data storage/manipulation tools, knowledge management systems are a new and intriguing way in which to employ such assets. But with the growth of competitive intelligence activities, setting up the system is only an initial step in proper management of knowledge assets. Protection of the assets, keeping them proprietary and of value to the firm and network, can be a critical step in truly leveraging such competitive weapons. And protection concerns today do not end at the physical limits of the firm, they extend to the entire e-network that connects the value chain.

Consequently, we propose this rough outline of a certification system that can be used to assess the compliance of a firm and its e-network with the U.S. Economic Espionage Act. With compliance to EEA, the firm and its e-network can better establish their knowledge as assets and, then, protect dispersal to competitors. Further, with an objective certification process in place, existing and potential members of the network can be audited to gauge their level of compliance, giving core firms a basis on which to determine the degree of information-sharing to take place. Such steps allow the core firm to ensure its own compliance with EEA and, therefore, its ability to protect its own knowledge assets. In addition, the certification can help in determining how much access to the network's assets collaborators at various levels of compliance can be granted.

REFERENCES

Benoit, Bertrand. (2001, April 27). Dinosaur with a smile on its face. *Financial Times*, 13.

Berkent Legal Services, PC. (2000). *Protection of trade secrets, confidential information, and goodwill -- beyond the basics*. (http://www.berkent.com/art-tsc3.htm).

Bontis, Nick. (1998, March-April). Intellectual capital: an exploratory study that develops measures and models. *Management Decision*, 36(2), 63-76.

Carr, Chris, Morton, Jack & Furniss, Jerry. (2000, Winter). The economic espionage act: Bear trap or mousetrap? *Texas Intellectual Property Journal*, 8, 159-209.

Davenport, Thomas H. & Prusak, Laurence. (1998). *Working knowledge*. Boston: Harvard Business School Press.

The Economist. (2000, November 11). Inside the machine: A survey of e-management. 1-40.

The Economist. (1999, June 26). The net imperative: a survey of business and the internet. 1-40.

Edvinsson, Leif & Malone, Michael S. (1997). *Intellectual capital*. New York: HarperCollins.

Eells, Richard & Nehemkis, Peter. (1984). *Corporate intelligence and espionage*. New York: Macmillan.

Ericksen, Paul D. (2000). The Extended Enterprise: Aim for Mutual Gain and Competitive Advantage. *Target*, 16(3) (Third Quarter), 53-59.

Fraumann, Edwin & Koletar, Joseph. (1999, March). Trade secret safeguards. *Security Management*, 64.

Gilad, Benjamin. (1994). *Business blindspots*. Chicago, IL: Probus Publishing Company.

Gilad, Benjamin & Herring, Jan. (1996). *The art and science of business intelligence*. Greenwich, CN: JAI Press.

Harris, Nicole. (2001, March 16). 'Private exchanges' may allow b-to-b commerce to thrive after all. *The Wall Street Journal*, B1, B4.

Meyer, H.E. (1987). *Real world intelligence*. New York: Weidenfeld & Nicolson.

Nonaka, Ikujiro & Takeuchi, Hirotaka. (1995), *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. New York: Oxford University Press.

Rothberg, Helen N. & Erickson, G. Scott. (2001). Competitive capital: A fourth pillar of intellectual capital? In Nick Bontis (Ed.), *Organizational Capital, The Cutting Edge of Intellectual Capital and Knowledge Management (pp. xxxxx)*. Woburn, MA: Butterworth-Heinemann.

G. Scott Erickson is Associate Professor of Marketing at Ithaca College, Ithaca, NY, USA.

Helen N. Rothberg is Associate Professor of Strategy at Marist College, Poughkeepsie, NY, USA and Principal of HNR Associates.

Chris A. Carr is Assistant Professor of Law at California Polytechnic University, San Luis Obispo, CA, USA