Are Your Secrets Safe? Knowledge Protection in Strategic Alliances

Patricia M. Norman

Businesses, particularly in high-tech industries, are entering into a growing number of alliances for a variety of compelling reasons. Through alliance partnerships, they may gain competitive advantages such as greater speed to market, lower costs, and shared risks. They may gain access to outside knowledge and capabilities ranging from product development and technology to management and marketing. However, a partner may also be seeking access to a firm's internal knowledge and capabilities. Thus the firm may find itself facing what Quintas, Lefrere, and Jones (1997) call the "boundary paradox"—alliance partners seeking knowledge and capabilities from external sources, while simultaneously facing the risk of exposing their own vital internal knowledge.

A classic example of this kind of risk occurred during the development of the Apple Macintosh from 1982 to 1984. Apple engaged Microsoft to develop spreadsheet, database, and graphical applications for the Mac. As a direct result, Microsoft acquired critical knowledge about Apple's GUI (Graphical User Interface) products that enabled its engineers to develop the Windows operating system. Eventually, Apple recognized that it was losing its distinctive advantage in the marketplace and brought a lawsuit against Microsoft. But it was unsuccessful, and Microsoft was later awarded a registered trademark for the name "Windows."

What is the long-term risk to a business in the event that alliance partners gain access to and actively use its core knowledge in a competitive challenge? More specifically, how can a firm protect its core competencies—the knowledge and capabilities considered essential to its competitive positions in the marketplace?

KNOWLEDGE PROTECTION MECHANISMS

A firm must protect its critical knowledge in at least two respects. First, there is knowledge that is directly relevant to the alliance and is being used and/or directly contributed in a purposeful manner. The firm must decide what parts of that knowledge must remain within its own private domain, as well as *how* to ensure that it is actually protected. Second, there is the danger of inadvertent or "indirect" sharing of knowledge and capabilities. A partner could easily gain access to information through physical presence on-site to participate in joint design or testing activities. Or its representatives could engage in numerous informal conversations with the firm's employees.

Certain structures and processes can be used to prevent partners from observing, understanding, acquiring, or imitating a firm's critical knowledge and capabilities.

Knowledge protection mechanisms can be grouped into three major categories: (1) human resources; (2) legal structure of alliance agreements and contracts; and (3) alliance processes. **Figure 1** shows specific protection mechanisms for each category. These mechanisms may be implemented either bilaterally or unilaterally. Bilateral mechanisms are usually put in place through mutual compliance with established alliance processes and structures. However, most firms also employ mechanisms that are devised and implemented solely for the firm's own use.

Before discussing the various knowledge protection mechanisms firms use, it should be mentioned that the extent to which firms will need to employ them varies depending on alliance and partner characteristics. Trust is one of the most important characteristics that will influence the need to protect knowledge. When a partner is more highly trusted, fewer or less stringent mechanisms are needed to control potential opportunism. Even with high trust, however, some level of protection is prudent. "One U.S. high-technology company's Japanese partner," report Yoshino and Rangan (1995), "learned about a highly sensitive research project from a notice concerning an internal research meeting posted on a company bulletin board." Thus, even when high trust and good chemistry exist, companies must always remain aware of sensitive knowledge and information.

Figure 1
A Framework for Classifying Knowledge Protection Mechanisms

Areas	*Categories*	*Knowledge Protection Mechanisms*
Human Resources	Top Management Support	Actions by top management • Identify core capabilities • Stress protection of core capabilities • Provide resource for protecting core capabilities
	Alliance Management	Actions by focal firm managers in alliance • Stress protection of core capabilities • Appoint a focal firm information manager
	Human Resource Management	Human resource management in focal firm • Educate personnel about proprietary data • Establish reward/evaluation program for protection of core capabilities • Consult designated individuals when circumstances are unclear • Report contacts with partner employees
Legal Structure	Patents	• Obtain patent to prevent imitation
	Contractual Mechanisms	• Specify proprietary information • Specify what information and capabilities can be shared • Specify what information and capabilities cannot be shared • Provide consequences if a partner accesses off-limits information • Provide consequences if a partner uses proprietary information in the wrong way • Sign nondisclosure agreements (NDAs) • Bar employment to partner employees • Ensure that information or technology shared with partner is covered by patents
Processes	Information Flows	• Limit to one person (gatekeeper) • Limit to a few people (communication stars) • Exclude certain information deemed off-limits
	Partner Access	• Perform certain alliance activities separately from partner • Limit partner's access to facilities • Limit partner's access to non-alliance personnel

Human Resources

The area of human resources encompasses the protection of knowledge by people at various levels in the firm. The three key areas include top management, alliance management, and HRM (including the day-to-day alliance members and other employees).

Top Management. Though usually not involved in the day-to-day operation of alliances, senior managers often play a significant and vital role in alliance negotiation and oversight. While their role in protecting critical knowledge and capabilities has not been widely discussed, the following list enumerates several logical responsibilities.

1. First and foremost, top management must identify the firm's core capabilities. A related and vitally important role is to decide what information can and cannot be transferred. In some instances, top managers may not make these decisions themselves but instead must ensure that adequate management processes exist so that appropriately designated individuals can make timely decisions. If these decisions are not made and clearly communicated, alliance members and other employees may inadvertently share information that could later hurt the firm's competitive position.
2. Top management must create awareness of the issue by personally stressing the importance of protecting the company's critical capabilities.
3. Top management should ensure that necessary resources are allocated for protecting knowledge and educating the work force.

Alliance Management. This HR category includes managers directly involved in the day-to-day operation of a cooperative effort. Alliance managers can endorse and strengthen top management's emphasis on protecting core capabilities. They may also appoint, or personally act as, information managers. The role of information manager is usually an additional duty assumed either by the overall

alliance manager or by another key manager in the alliance (such as the business coordinator or the lead engineer). In the absence of a common name, we have chosen to refer to this role as "Alliance Information Manager." The AIM may perform any or all of the following activities:

Monitoring and surveillance. The AIM carefully scrutinizes critical knowledge used in the alliance and ensures that it has been classified accurately and that alliance members and other involved employees are properly informed and educated about knowledge issues.

Compliance. The AIM must continuously ensure that employees are actually following the guidelines and procedures established by the knowledge protection system.

Consulting/advising. The AIM may also act as a consultant in cases where employees feel that the circumstances surrounding knowledge protection are vague or unclear.

Human Resource Management. The HR function in a firm can support the knowledge protection effort in several ways. One way is to provide education and training programs aimed specifically at protecting knowledge. For personnel directly involved in an alliance, these programs are usually conducted in conjunction with the alliance manager. For personnel indirectly involved or not expected to be involved but who may come into occasional contact with partner employees, the HR function must ensure that they understand the importance of maintaining confidentiality. Likewise, reward and incentive programs for protecting core capabilities can be structured and implemented through the HR division. Using performance appraisals to evaluate employee achievements in protecting critical knowledge also falls within the responsibility of the HR division.

While the actions of top management, alliance management, and HRM are vital, information leakage frequently depends on the choices made by individuals who work with the alliance on a daily basis and come in regular contact with alliance partners. Any point of contact between a firm's employees and its partners' employees represents an information flow where critical knowledge could be inappropriately communicated. So the education of employees about what information is sensitive and proprietary is of paramount importance.

Employees at the working level have several personal responsibilities in protecting sensitive knowledge. The first is being aware of and complying with corporate procedures on knowledge protection. Second, when it is unclear whether information should be shared, employees should consult with designated individuals such as the AIM. Third, some companies require employees to report any contact with alliance partners if they believe an information issue exists. For example, such a report would be advisable if the employee believed an alliance partner was "fishing around" for critical knowledge that had been deemed off-limits.

Legal Structure

Firms also turn to legal mechanisms to protect knowledge. These may include patents and contractual mechanisms.

Patents. Patents are used primarily for the purpose of providing legal protection for inventions and processes. If other parties do not obtain the proper authority to use a patented product or process, the patent holder may pursue legal remedies that prevent those parties from using and/or selling the product or process. The patent holder may also be awarded monetary damages for the infringement. Several issues are associated with using patents to protect critical knowledge. One is that patents do not cover all categories of competitively sensitive knowledge, so overreliance on them may still leave a company vulnerable. Another concern, particularly relevant to high-tech industries such as electronics and semiconductors, is that the patent process discloses information that may enable some competitors to "invent around" the patent. Patents have historically been more effective in such industries as pharmaceuticals and chemicals, where the physical composition of patented products makes them difficult to imitate without violating the patent.

Contractual Mechanisms. A variety of contractual and legal mechanisms may be imposed to protect specific knowledge from unwanted appropriation (shown in Figure 1). For example, contracts can explicitly identify information that has been designated as proprietary. They can spell out what information and capabilities are to be shared, as well as expressly identify information and capabilities that are *not* to be shared. A more active approach imposes contractual or legal penalties if an alliance partner deliberately accesses or uses information inappropriately. For instance, a contractual clause may specify monetary penalties or contract termination for violations of knowledge protection agreements.

It should be noted that alliances usually result in a certain amount of "natural learning" as a consequence of working together. In fact, learning is often desired and adds to the success of a partnership. Thus, merely acquiring knowledge is not necessarily a "violation"; the acquisition of a certain amount of knowledge is predictable and expected. However, violations do occur when alliance partners reuse knowledge in a direct, intentional way that was prohibited by the alliance contract. Examples of such violations include (1) an alliance partner establishing itself as

a direct competitor by using illegally acquired information to build its own product and (2) disclosing protected alliance information to outside parties.

One widely used approach for implementing contractual protection requires each individual alliance member to sign a nondisclosure agreement (NDA). Each member is then bound by the agreement to protect designated information from disclosure to outside parties. Another protective mechanism uses employment limitations in which companies are prohibited from offering jobs to the employees of an alliance partner. These limitations are usually specified for a given time period and often apply only to selected employees who have been involved in the alliance or have obtained relevant knowledge.

Processes

According to Galbraith and Kazanjian (1986), processes affect the "direction and frequency of work and information flows" within a firm. Extending this observation from a single firm to multiple firms in an alliance arrangement, processes are vitally important because they determine how work is done and how people interact. In other words, processes are critical determinants of the information, skills, and capabilities that flow between partners. Control of processes is therefore another way to protect critical knowledge in an alliance environment. Examples of processes that are relevant to alliances include planning, problem-solving, decision-making, determination of product requirements, development of technical designs, integrating and testing products, and so on.

A subtle but important distinction should be made here. There are processes and information that need to *be protected,* and there are processes that help *ensure that such protection occurs.* The information to be protected generally involves two major categories: (1) technical knowledge associated with such processes as designing, testing, and manufacturing a product; and (2) strategic knowledge associated with business decisions such as future product mix and cost structures. The processes that help protect this knowledge are generally associated with communication, information flows, and people. Thus, the knowledge protection mechanisms associated with controlling processes fall into two major categories: information flows and partner access.

Information Flows. When using any of the example processes mentioned above, alliance partners must share information to get things done. So another potential approach to protecting knowledge focuses directly on who is allowed to exchange information as well as what information may be shared. A relatively cautious, conservative approach regarding who may exchange information is to funnel all information and communication through a single individual known as a *gatekeeper.* This practice reduces unintentional, incidental disclosures that occur when partners overhear and observe technical details merely because they have access to a firm's people and facilities. In keeping with the more cautious approach to protecting knowledge, information flows may be strictly limited only to what is directly relevant to the alliance and absolutely necessary to support successful integration of each partner's contribution. These cautious practices make it more difficult for an alliance partner to gain enough information to successfully imitate complex capabilities.

However, the cautious approach brings potentially serious disadvantages, particularly for product development alliances. If time is of the essence, limiting information flows through a single individual will likely slow communication and decision-making and result in bottlenecks and schedule delays. Alliance members performing daily technical tasks may find that they have insufficient information or that the information comes too slowly. There may be less synergy and exchange of ideas for improving design concepts. Moreover, when information is closely held, there may well be more problems when the partners attempt to integrate the various subsystems into one cohesive product.

Extending the gatekeeper concept, a somewhat more flexible approach would employ the use of several "communication stars" rather than a single gatekeeper. Communication stars are boundary spanners who have well-developed external and internal networks that allow them to acquire and share information from outside the firm. They are the people typically sent to conferences, seminars, and trade shows. However, in an alliance these communication stars could also easily become the conduit, as well as the safeguard, for information that goes out of the company to any alliance partners.

Communication stars differ from the AIM in two important ways. First, any alliance will have only one AIM, but may have a number of communication stars. Second, a designated AIM is responsible at a higher level for the procedures used to protect information, whereas communication stars are the primary individuals who are actively engaged in exchanging information with the alliance partners on a daily basis.

Partner Access. Other procedural decisions may affect an alliance partner's access to critical knowledge. A firm may isolate critical information by performing certain activities without the partner. Roehl and Truitt (1987) report how General Electric, in its alliance with the French company Snecma, modularized their jointly produced

engine so that certain critical technologies were not shared. GE produced critical components as "black boxes," and Snecma never had the opportunity to examine those technologies.

In addition, firms can limit partner access to both facilities and non-alliance personnel. Limiting partner access to company facilities prevents the partner from observing how the firm conducts business and thus inadvertently gaining access to information that is not intended to be part of the alliance. Similarly, whenever the alliance involves periods of physical collocation, partner employees will have the same opportunities for learning and observation, so access to facilities must be planned, monitored, and controlled. Non-alliance personnel may be unaware of what information is to be shared and what information is off-limits to the partner. Limiting partner access to these people is another mechanism for protecting knowledge. Although partners will, of course, gain access to some information that is not intended to be part of the alliance through observation and inadvertent release, limiting their opportunities to observe critical operations and to have informal discussions with non-alliance members is a way to reduce knowledge leaks.

A KNOWLEDGE PROTECTION STUDY AND ITS FINDINGS

To explore knowledge protection among partners, the author conducted a study of alliances in four high-tech industries. The data reported here were collected through personal interviews of 22 managers who were involved in 25 alliances. **Table 1** shows the number of managers and alliances from each industry segment. The names of the companies are fictitious because they were guaranteed anonymity. Alpha Computers is a division of a large computer firm. Beta Electronics is a small, independent division of a large, diversified company, and is involved in a high-tech segment of the electronic components industry. Gamma Pharmaceuticals is a large drug company. Delta Telecommunications is a small firm that designs and makes telecommunication equipment. Each of the firms is currently engaged in a number of alliances. In addition, two of them have extensive experience with alliances that are now completed.

The study participants were first asked open-ended, general questions in the following two categories: (1) the core capabilities of the company or division; and (2) what techniques and practices were used to protect these capabilities and whether each of these methods was equally effective. Finally, managers were asked to numerically rate the effectiveness of specific knowledge protection mechanisms and to provide information about the use of these methods. After the interviews, responses to written surveys were obtained from managers involved in 46 alliances in three of the aforementioned high-tech industries: computers, electronics, and telecommunications. These managers numerically rated the effectiveness of several knowledge protection mechanisms. **Table 2** shows the number of alliances from each industry.

Table 1
Summary of Interviews

Firm	*Number of Alliances*	*Number of Managers*
Alpha Computers	11	10
Beta Electronics	6	7
Gamma Pharmaceuticals	5	3
Delta Telecommunications	3	2

Table 2
Summary of Surveys

Industry	*Number of Alliances*
Computers	18
Electronics	14
Telecommunications	14

Note: One manager responded for each alliance.

Unfortunately, all knowledge protection mechanisms were not created equal. Some methods, such as NDAs, have been used extensively and were historically assumed to provide reasonable protection. However, the respondents in this study revealed that NDAs have some serious shortcomings. Because "traditional" wisdom does not always ensure a sufficient level of protection, the research findings are organized according to the mechanisms that were considered most effective and those considered least effective. **Table 3** on the next page groups the most and least effective mechanisms into broad categories. The average ratings from the interviewees and the survey respondents are shown.

Most Effective Mechanisms

In reviewing Table 4, it is notable that all but two of the most effective mechanisms were concerned with making company personnel aware of the need to protect certain knowledge and identifying what knowledge needed protecting. The other mechanisms that were rated as highly effective involved walling off critical knowledge. An important characteristic of all these methods is that they allow the firm to protect knowledge in a manner that still allows it to be open to the upside and benefits of knowledge sharing. They preserve the opportunities for spontaneous learning and changes.

As one manager noted, protecting critical knowledge and competitively sensitive information ultimately depends on the choices made by people in the firm. Thus, it is not surprising that many of the managers discussed mechanisms that involved raising individuals' awareness of the need to protect certain knowledge and providing specific guidance on what to protect. Awareness of the need for knowledge protection begins at the top of the organization. When senior managers make knowledge protection a priority, they

Table 3
Effectiveness of Knowledge Protection Mechanisms

		Interview Rating	*Survey Rating*
Most Effective	*Awareness of Protection*		
	• Top management focus on protecting capabilities	4.2	3.9
	• Education about proprietary data	4.2	4.1
	• Information manager	3.9	3.6
	• Contract specifying proprietary data	3.9	4.3
	• Contract specifying what information can be shared	3.9	4.3
	• Clearly marked documents as to level of criticality	NR	NR
	• Top management identification of core capabilities	3.8	4.1
	• Alliance management focus on protecting capabilities	3.8	4.0
	Walling Off Critical Knowledge		
	• Performing certain functions without partner	4.0	4.1
	• Excluding certain information deemed off-limits	NR	4.1
Effectiveness Depends on Firm/Industry	*Patents*		
	• Obtaining patents on critical inventions and processes	NR	3.8
Least Effective	*Punitive Contractual Measures*		
	• Barring employment offers to partner employees	2.8	3.8
	• Consequences for accessing off-limits information	3.5	3.5
	• Nondisclosure Agreements (NDAs)	NR	NR
	Undue Hindrances to Integration		
	• Limiting partner access to non-alliance personnel	3.4	3.4
	• Not sharing critical capabilities with partner	3.5	NR
	• Limiting information flows to a gatekeeper	3.5	3.0
	After-the-Fact Personnel Actions		
	• Rewards/evaluations that consider protection	3.5	2.6
	• Reporting contact with partner employees	3.5	3.1

NR=not rated

send a signal to employees at lower levels that it is an important activity. Their role, however, goes beyond just raising awareness. Top managers must set the stage for effective knowledge protection and ensure that the firm has identified its core capabilities and knowledge. Without a clear identification of what is at the core, different individuals may make different decisions about whether or not to protect the same knowledge. At Alpha Computers, managers from different functional areas identified diverse core competencies. A marketing manager, for example, was willing to share information that an engineer considered critical and would not share. By contrast, everyone at Beta Electronics, regardless of functional area, identified the same core capabilities and agreed that knowledge related to these capabilities should not be shared with outsiders.

Alliance managers reinforce top management's emphasis on knowledge protection. Employee awareness is likely to be raised if consistent messages are sent from top levels of the organization as well as from alliance management.

A common theme that emerged during the interviews was the importance of educating personnel interacting with partners about what information to share and what not to share. Through education, personnel not only became generally more aware of the need for protection, they could be given specific guidance. People need to know the relationship bounds.

Contractual mechanisms that specifically identified what proprietary data and information could be shared were rated more effective than contractual measures aimed at preventing knowledge leaks or punishing a partner. These more effective mechanisms are important not because they allow for legal action or enforcement, but because they are key educational tools for the firm's own employees. They provide specific guidance about what can and cannot be shared with a partner.

Another theme was to involve only those people who were needed in an alliance. This limits potential exposure and makes the job of managing information flows much easier. Not all non-alliance personnel "have the sense to know" what should and should not be shared. In dealing with this problem, one firm appointed a "business coordinator" (the equivalent of an information manager) who was responsible for tracking information flows and ensuring that other alliance personnel understood which information was critical and to be protected. Other firms reported that the alliance manager was expected to fulfill a similar role.

Respondents found that the use of a single gatekeeper posed several problems, so they imposed a variety of alternative mechanisms to control the flow of information. In many development projects, sensitive information was available only to company personnel with a need to know. Moreover, each firm had processes for classifying and disseminating information. They differed, however, on how formal the processes were and how carefully they were followed. At a minimum, firms marked information as proprietary. Beta Electronics had a comprehensive system for classifying and disseminating information.

Data on core technical processes were labeled "strictly confidential" and were tightly controlled; copies were limited, and the information was shared only with necessary internal personnel. General information such as strategic plans for product development were labeled "confidential" and were not disclosed outside the firm.

A final mechanism that was widely cited as very effective was to perform certain activities without a partner. This allowed firms to wall off critical capabilities from the purview of their partners. Roehl and Truitt (1987) suggested a similar strategy that is especially applicable when the work revolves around technological knowledge. In this study, Delta Telecommunications was able to encase its critical technology in a black box that was then integrated into the final product. Walling off knowledge, however, was not limited to technological knowledge. Firms in this study also walled off other critical knowledge, including market applications and financial information.

Mechanisms Whose Effectiveness Varied by Industry

Study participants cited the protection offered by existing patent and copyright laws. However, they pointed out that patents are much more effective and thus a more important source of knowledge protection for the pharmaceutical industry than for many other industries. As mentioned earlier, pharmaceutical products are more difficult to imitate based on information disclosed by the patent process. However, in some industries (electronics was specifically mentioned), patents disclose enough information that competitors may be able to "invent around" them, as discussed earlier. One manager at Gamma Pharmaceuticals thought that, partly because of the heavy reliance on patents, companies in the pharmaceutical industry are not as guarded as those in other industries.

Least Effective Mechanisms

When managers were asked how their firms protected proprietary or competitively sensitive knowledge, the overwhelming first response was nondisclosure agreements. NDAs made people feel more comfortable in sharing information with a partner. Without an NDA, firms tended to share less. Despite the pervasive use of NDAs, however, many managers questioned their effectiveness. With an NDA, one is trusting one's partner to abide by it. If a violation occurs, significant damage is already done. Another problem raised by some managers was that violations may not always be detected. In light of these problems, a number of managers suggested that NDAs are best used, in the words of one, "as a tool to more explicitly state what is proprietary and what can be shared." Reliance on NDAs to protect critical knowledge adequately may create a false confidence in many instances.

Another topic that elicited much discussion during the interviews was the flow and control of information. Although a gatekeeper can provide tight control on information flows, a number of drawbacks were raised. First, in many types of alliances, such as when firms are jointly developing a product, such a limitation may not be feasible. Second, as information is passed through a gatekeeper, the meaning may get changed. In one firm, an engineer had experienced problems when technical information had been passed through a gatekeeper who was focused more on the business side of the project than the technical side. The engineer recalled the childhood game of "telephone" in which a message is initiated and passed through several people, invariably being altered in some significant way by the time it gets back to the initiator. So it can be with a gatekeeper who does not have relevant knowledge. In addition to changing the message, this filtering process may sometimes slow down the development process by causing communication to take longer. Because of these drawbacks, single gatekeepers were rarely used. Instead, firms imposed a variety of other mechanisms to control the flow of information, rated in Table 3 as the most effective mechanisms.

Protection mechanisms that were rated among the least effective can be grouped into three categories: punitive contractual measures, methods that unduly hinder integration with a partner, and after-the-fact personnel actions. Note that the contractual measures rated as relatively more effective were aimed at educating company (and partner) personnel about whether or not certain information was to be shared, whereas the punitive contractual measures were responses to partner misdeeds. A number of negative consequences are likely when firms resort to punitive contractual provisions. For one thing, writing detailed contracts is time-consuming and expensive. But more important, a partner may perceive these actions as a lack of trust, thereby causing the relationship to deteriorate. Moreover, lengthy contract restrictions are often perceived as bureaucratic and may stifle creativity. Finally, enforcement of these mechanisms means that a violation has already occurred and the damage to the firm is done.

Using gatekeepers, not sharing knowledge, and limiting access to non-alliance personnel were not seen as effective mechanisms. Although they may protect company-specific knowledge, they severely limit a partner's ability to interact and create synergies from joint activities. Thus, partners are less likely to enjoy the full range of

benefits an alliance can offer. Moreover, they tend to be applied broadly to all information and communications rather than selectively to particular items and capabilities that must be protected.

The final group of least effective mechanisms includes using rewards and evaluations that consider knowledge protection and requiring employees to report contact with partner employees. Both these mechanisms involve actions taken after personnel have had contact with partner personnel. They may be viewed as efforts to control employees. But employees seem to respond better to efforts to educate them so that they are equipped to make wise decisions when faced with whether or not to allow a partner access to critical knowledge.

Other Findings

Another interesting finding from the interviews conducted for this study was that the techniques a particular firm used to protect knowledge did not always vary greatly for its different alliances. Although it was expected that there would be a fit between the perceptions of the need to protect knowledge and the actions taken to achieve that level of protection, the managers suggested that this may not always be the case. In every firm, certain knowledge protection mechanisms were applied to all alliances regardless of the partner or the circumstances. Practices became institutionalized with repeated use, or as they developed to address problems arising during an alliance. NDAs were the most universal technique. Moreover, each of the firms had certain practices or procedures related to information flows.

This finding emerged from the interviews and was not initially hypothesized for the study. Literature on institutional theory and organizational learning both provide plausible explanations for how actions taken to protect knowledge may become institutionalized. From an institutional theory perspective, Scott (1987) maintains that they become taken for granted as "the way things are to be done." According to Meyer and Rowan (1977), specific, rule-like prescriptions often emerge that become "highly institutionalized and thus in some measure beyond the discretion of any individual participant."

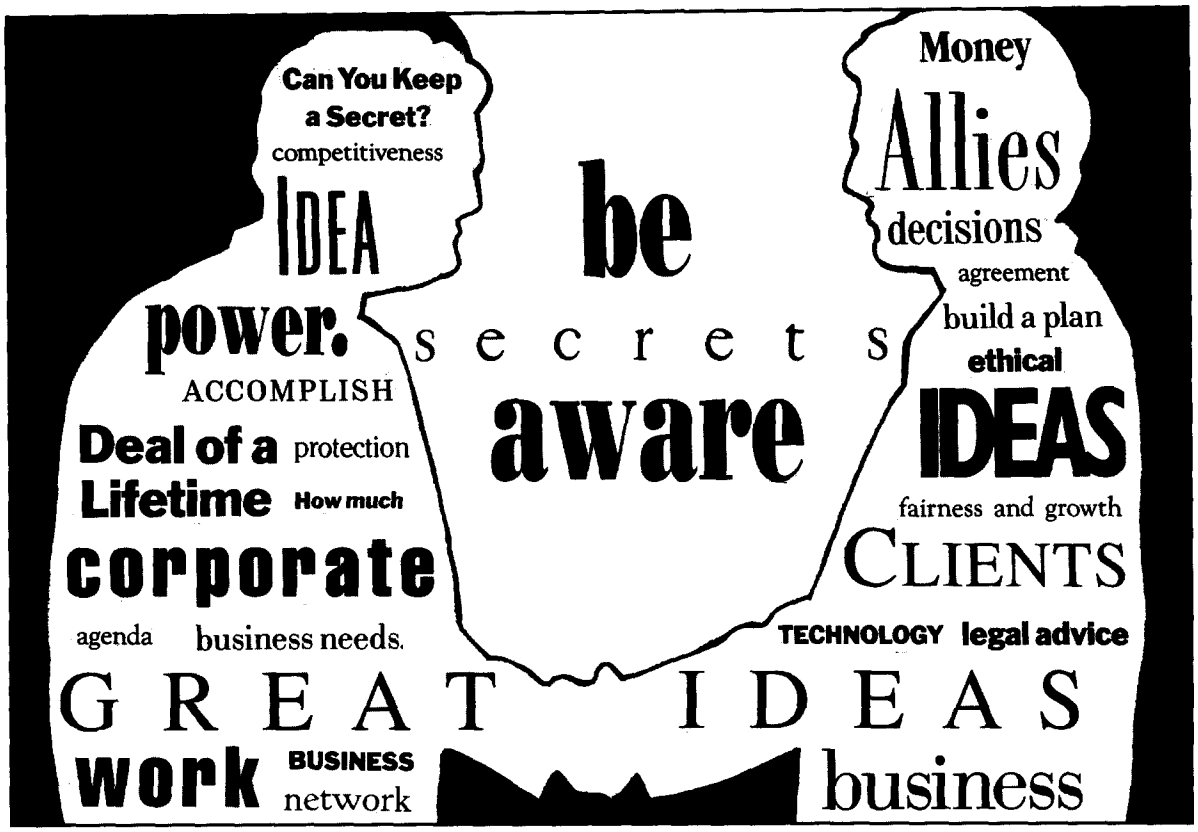
A complementary explanation is that firms learn about knowledge protection as they gain more experience with alliances. This learning can take place in a number of ways. First, firms may learn from the success or failure of techniques they have applied. Second, they may learn how their partners protect knowledge and imitate their techniques. Third, managers may learn through informal contacts with managers outside the firm, articles published in professional journals, or consultants who make recommendations based on their experience with and knowledge of other companies and alliances.

Experiences at Beta Electronics also suggest that despite this tendency to apply knowledge protection mechanisms universally, there were changes in how strictly some were applied over the life of an alliance. Information that was originally off-limits to partners was shared as the deadline for completing the product design approached. How freely it was shared, however, did depend to some extent on the manager's perceived need for knowledge protection. This perceived need was most influenced by such factors as the extent of competitive overlap, how much trust had developed, and whether the knowledge in question had been identified as core knowledge by the firm.

Almost all of the managers interviewed agreed that the level of trust in a partner was a critical factor that influenced how much they believed their knowledge needed to be protected from that partner and the degree to which they took actions to protect it. Two alliances at Delta Telecommunications, each with a different firm, illustrate this relationship. In each alliance, Delta was contributing a portion of the jointly developed product as a black box to its partner. In one case, the partner asked only for data related to the interface so that the product could be integrated; over time, Delta came to trust this partner. The partner in the other alliance was immediately aggressive about seeking information related not only to the interface, but also to the design in the black box. Delta became suspicious of its intentions and was never able to develop trust within the alliance. As a result, Delta was much less open and more formal in structuring communication and information flows.

Knowledge may be embedded in products, processes, and people. When critical knowledge is embedded in products or processes that can be readily segregated from other alliance activities, then product knowledge can be protected by building it into a black box that a partner cannot see, and process knowledge can be protected by performing activities separately from the partner so that the process cannot be observed.

The most difficult aspect of protection, however, seems to be the knowledge held by individuals and groups within a firm. When it comes to such knowledge, the results of this study suggest that effective protection has less to do with restricting actions or carefully prescribing punishment than with educating the employees who are to interact with the alliance partner(s). Partners that openly share knowledge are likely to enjoy the most successful alliances. Educating employees instead of restraining their interactions with



partners helps preserve the benefits of interactions while also protecting the firm's knowledge.

Identifying and developing core competencies is a central role of top management. To protect a firm's core competencies adequately, however, two steps are necessary beyond this role. First, top management must ensure that all employees understand the firm's core competencies. While this is important for future competency development, it becomes especially critical when firms are engaged in alliances. Individual employees are likely to interact with partners. If the firm's core competencies are not already known, they will be unable to make informed choices about knowledge sharing during an alliance.

Clearly identifying core competencies can be a double-edged sword. If knowledge is made more explicit, it may be easier for partners to understand and acquire. But identifying core competencies does not necessarily mean articulating and documenting the knowledge itself. Rather, it means making it clear to employees what those competencies are, labeling and protecting this knowledge if it is written, and putting boundaries around it. The boundaries may be physical (imposed around equipment, products, processes, or facilities) or mental (placed around certain knowledge in employees' minds).

Second, top managers must ensure that education is provided for alliance personnel. Educating personnel is a key factor in effectively protecting knowledge without limiting the benefits to be gained from alliances. There are two crucial issues in gaining the most effective performance from alliance members: staffing and training. Choosing the right people as "working" members of an alliance is critical to its success and is especially relevant to successful knowledge protection. The most effective protection techniques were ultimately associated with adequate knowledge and good decision-making on the part of these working alliance members. Employees involved in alliances must be committed to the firm's mission and have the ability to exercise good judgment in making independent decisions. They should focus on creating new knowledge in conjunction with partner employees, but must understand when it is necessary to protect critical data.

The fact that knowledge protection techniques become institutionalized has a number of implications for managers. Because techniques are being used in cases where they may not be needed, firms can suffer a number of adverse effects. This is particularly true in cases where less protection is warranted by the circumstances. First, alliances that use more knowledge protection than really needed will incur the associated administrative costs of those actions. Second, firms that are overly protective with partners may damage their relationship and thus the potential of their cooperative efforts. Third, carefully prescribing actions can limit an alliance's flexibility.

Finally, the relatively short-term objectives for successful alliances must be delicately balanced with the long-term health of the corporation. Not having protective processes and mechanisms exposes a firm to potentially devastating losses. Yet mindless institutionalized overprotection will undermine the potential gains from alliances. Hopefully, the findings of this study will help in striking a better balance. ❐

References and Selected Bibliography

M.A. Cusumano and R.W. Selby, *Microsoft Secrets* (New York: Free Press, 1995).

J.R. Galbraith and R.K. Kazanjian, *Strategy Implementation: Structures, Systems, and Process*, 2nd ed. (New York: West Publishing, 1986).

J.W. Meyer and B. Rowan, "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology*, September 1977, pp. 340-363.

P. Quintas, P. Lefrere, and G. Jones, "Knowledge Management: A Strategic Agenda," *Long Range Planning*, June 1997, pp. 385-391.

P.S. Ring and A.H. Van de Ven, "Structuring Cooperative Relationships Between Organizations," *Strategic Management Journal*, October 1992, pp. 483-498.

T.W. Roehl and J.F. Truitt, "Stormy Open Marriages Are Better: Evidence from U.S., Japanese and French Cooperative Ventures in Commercial Aircraft," *Columbia Journal of World Business*, Summer 1987, pp. 87-95.

W.R. Scott, "The Adolescence of Institutional Theory," *Administrative Science Quarterly*, December 1987, pp. 493-511.

M.Y. Yoshino and V.S. Rangan, *Strategic Alliances: An Entrepreneurial Approach to Globalization* (Boston: Harvard Business School Press, 1995).

Patricia M. Norman is an assistant professor of management at Baylor University, Waco, Texas.

This research was supported by the Cato Center for Applied Business Research at the Kenan-Flagler Business School, University of North Carolina at Chapel Hill. The author is grateful to Rich Bettis for assistance in conducting the interviews and to Mike Farr for his help on the article.