IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4250

Securing Intellectual Property In IS Layoffs

Norman Pendegraft and Jerry Wegman
Associate Professor, Department of Business, University of Idaho, Tel: (208) 885-7157, norman@uidaho.edu

INTRODUCTION

The most important asset of many companies is their intellectual property (IP). Customer lists, computer code, and information about new products are all IP. According to Nichols et.al. (2000) preventing the disclosure to competitors of IP is a major IS security problem. They assert that the major source of such disclosures is insiders such as disgruntled employees or former employees. Poorly handled layoffs may provide the incentive and the opportunity for employees to disclose IP to competitors at great cost to the firm.

Until recently the major HR problem facing IS managers was the shortage of qualified workers (Murray 2000). Recent events have changed this. According to Rosencrance (2001) during the first 9 months of 2001 over 130,000 jobs were cut at computer based companies. Layoffs have received considerable attention in the trade press (Duffy 2001, Georgia 2001). Despite this little has been written to guide managers faced with IS layoffs. For example, Brown (2000) devotes a chapter to hiring and retaining IS workers but does not mention layoffs.

This paper suggests legal and managerial practices which a company may use to protect its IP. The first section deals with legal strategies for protecting IP. The second addresses IS management strategies. The third considers the management of the layoff per se. The final section presents the first installment of a field study based an a large layoff of IS workers.

LEGAL PROTECTION OF INTELLECTUAL PROPERTY

There are several legal protections for IP. Copyright is perhaps the most important legal protection for computer software. The Federal Copyright Act as amended offers copyright protection to software. Copyright grants the owner exclusive use of the material. Certain types of information, such as customer lists, do not qualify for copyright protection, but may be protected as trade secrets. The classic example of a trade secret is the formula for Coca Cola. The Uniform Trade Secrets Act (UTSA) states that in order to qualify as a trade secret there must be economic value in maintaining secrecy, and reasonable efforts must be made to maintain its secrecy.

Congress recently enacted two criminal statutes that punish IP theft. The Economic Espionage Act of 1996 makes not only the thief criminally liable, but also one who knowingly obtains from the thief. Section 1030 of the Federal Criminal Code makes computer fraud a federal felony.

What should a firm do to legally protect its IP from disclosure? This is not intended as a legal treatise, and as with any legal matter, each firm needs to consult legal counsel to address its specific needs. But, there are general recommendations which should be considered. First, the firm should require an employment contract containing non-compete, non-disclosure and IP security provisions.

The non-compete agreement limits the employee's right to seek reemployment by a competitor. Courts will enforce such agreements if they are 'reasonable', although enforcement varies among the states. The test of reasonableness considers how long a period of time the employee is being restrained; how extensive is the geographic area in which the employee is being restrained; and what kinds of work are being restrained. Non-disclosure agreements constrain the employee from disclosing or using IP learned while employed. It should also establish that any IP created by the employee will be the firm's property.

The Employer should establish a clear IP policy. One part of that policy should prohibit unnecessary removal of IP from the workplace. The lack of such a policy led to theft of copyrighted software in the *Computer Associates* case (U.S. Court of Appeals 1992). Violation of the policy could provide legal grounds for termination. The firm should register copyrightable works with the U.S. Copyright Office. Reasonable efforts must be made to maintain the secrecy of trade secrets.

Finally, affected employees (and new employers) should be reminded of their legal obligations during the exit interview which will be discussed more fully in a later section.

IS MANAGEMENT

While legal protection is essential, it is not sufficient. Good management practices should be followed to reduce the chances of IP theft. A recent informal survey of IS managers (Talkback 2001) suggested several practices for those laying off IS personnel. Many of the suggestions are related to protecting IP and despite the survey's informality, the suggestions stand on their own as valid.

The action most recommended in the survey is to immediately cancel the accounts of the affected employees. Most IS systems have good account management subsystems which will keep track of user privileges. Unfortunately, these may be dispersed to several areas such as network management, database administration, and email administration. One consequence is that it may be hard to keep track of what systems an employee has access to. It would be useful to have a complete list of all employee accounts on all systems.

The problem is magnified by the fact that some affected employees may be the custodians of the systems in question. The possibility exists that they may have created additional, unauthorized accounts for themselves. This suggests that there be a means of authorizing accounts and that systems be regularly audited for unauthorized accounts. It also suggests that layoffs of system administrators are especially sensitive.

A second major concern revealed in the survey was for data backups. Access to backup data must be limited and audited to ensure that the backups are not jeopardized. Backup planning should be part of routine continuity planning (Toigo, 1989). The importance of continuity planning has been made clear to IS managers by Y2K, various natural disasters, and the events of September 11. Layoffs may now be added to the list of concerns to be guarded against.

Even if all accounts are deactivated, there is a hazard because IS employees are familiar with the architecture of the system. McClure et.al. (2000) identify "footprinting" as the initial step in hacking a system. If motivated to do so, former IS employees are already in a position to hack a system because they understand its structure. Thus it is important to treat them is such a way as to minimize their antagonism to the company. This makes the exit interview extremely important.

The possibility of misuse also emphasizes the importance of good auditing practices. Audits may help reveal unauthorized activity such as copying files, creating accounts, or sabotaging the system. Care must be taken to safeguard the audit logs and to ensure that they are regularly monitored by system administrators unaffected by the layoff.

IS LAYOFF MANAGEMENT

While detailed discussion of layoff management per se is beyond the scope of this paper, there are several matters relating to IP protec-

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference.

tion which warrant discussion. There are more complete discussions in many Human Resources texts (for example, Gomez-Mejia 1995).

An employer implementing a layoff must balance the twin objectives of considerate treatment of former employees with the need to protect itself. The exit interview is an essential part of the process. Exit interviews should not be harsh or threatening; indeed that would be counter-productive. Departing employees must be reminded of their legal obligations contained in non-compete and non-disclosure agreements. In a considerate manner the employee should be made aware of the importance the company places on its IP and its willingness to defend that IP by means of civil lawsuits if necessary. The matter of criminal prosecution is more delicate. The firm does not want to make the employee feel accused or threatened. On the other hand, making it clear that theft of IP is a criminal offence, as described above, may well have a deterrent effect.

The manner in which employees are notified of their layoff is important. Some of the respondents urged that the layoff be kept secret until affected employees were notified and that security guards be used to remove equipment from affected employees' offices. Certainly, those laid off should be asked to surrender keys and identification which give them access to IS areas. Respondents also urged that support be provided after the layoffs in terms of placement assistance and email. Sensitivity in such matters may be important in influencing affected workers attitudes toward the company.

When the worker finds new employment, the new employer should be notified as to the worker's prior exposure to copyrighted or trade secret protected works and warned that any infringement will be vigorously prosecuted.

Two final ideas: Jossy (2001) suggests looking for alternatives to layoffs such as job sharing or reductions in hours. Among the advantages are maintaining the knowledge pool so important in running IS operations and positioning the firm for later expansion. Further, there is a large body of labor law dealing with terminations. While not directly related to the problem of protecting IP, following this law is important to protect the company from liability for wrongful discharge.

FIELD STUDY OF AN IS LAYOFF

We conclude the paper with the first phase of a field study of a major corporation which recently laid off a significant number of IS employees. We interviewed an employee who was not laid off as well as a manger in another department. Because the conversations were confidential, we are, at present, unable to reveal the identity of the employees or the company.

According to the employee the company announced a reorganization well in advance of the layoffs. The announcement led to rumors of layoffs and a decline in moral. When it announced that layoffs would take place during the next two weeks and the protocol used to identify those affected, many employees overtly estimated their chances of being laid off. He reported that employees were offered a generous separation package or the option of keeping their jobs for six months. In a department of about 30 employees, 6-8 were laid off and two of these accepted the offer of temporary continued employment. The company provided placement support and continued email access. Subsequently we interviewed one of the involved managers, and he had a very different perception of the events.

The handling of this layoff seems mixed. It seems to have been reasonably sensitive, but allowing laid off IS employees to continue in place seems risky. It provided an opportunity to alienated employees to perform acts of revenge against the firm. The prior announcement of criteria and scheduling of layoffs may have had a negative impact on productivity and morale. Most disconcerting was the very different perceptions of the events. This suggests a communications breakdown.

CONCLUSION

Layoffs now constitute a new concern for IS managers. Many of the recommended practices need to be implemented well in advance of layoffs if they are to be useful. Fortunately, most of these are part of good IS management practice and therefor should cause little dislocation or additional cost.

REFERENCES

Brown, Cecil, ed., IS Management Handbook, Auerbach, New York, 2000.

Computer Associates International, Inc. v. Altai, Inc., 982 F.2d 693 (2nd Cir.1992).

Copyright Act, 15 U.S.C. 1051 (1976).

Duffy, Tom, "Downsizing With Dignity," Network WorldVol.18#40, p.53, 1Oct.2001.

Economic Espionage Act of 1996, 18U.S.C.1831-1839 (1996).

Georgia, Bonny, "Noncompete or Not", Network World Vol.18#33, p.44, 13Aug.2001.

Gomez-Mejia, Luis R., David B. Balkin, and Robert L. Cardy, Managing Human Resources, Prentice Hall, Englewood Cliffs, 1995.

Jossi, Frank, "Take The Road Less Traveled", HR Magazine, Vol.46#7, pp. 46-51, July 2001

McClure, Stuart, Joel Scambray, and George Kurtz, Hacking Exposed, Osbourne / McGraw Hill, Berkeley, 1999.

Nicholls, Randall K., Daniel J. Ryan, and Julie J.C.H. Ryan, Defending Your Digital Assets, McGraw Hill, New York, 2000.

Rosencrance, Linda, " Telecommunications, computer firms post biggest layoffs this year ", http://www.computerworld.com/storyba/0,4125,NAV47_STO64434,00.html. 4 Oct.2001.

Section 1030 of the Federal Criminal Code, 18U.S.C.1030 (1999).

"Talkback" , Information Security vol.4#8, August 2001, p16-18.

Toigo , Jon, Disaster Recovery Planning, Yourdon Press, Englewood Cliffs, 1989.