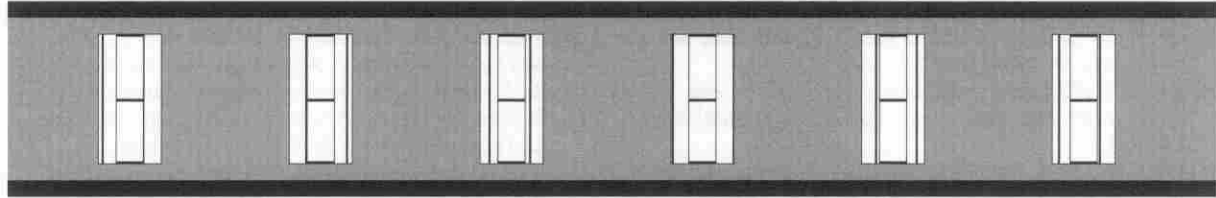


Reducing Internet Abuse in the Workplace

Dinesh Mirchandani, *Grand Valley State University*

Jaideep Motwani, *Grand Valley State University*



Introduction

Several recent articles have discussed the dangers of Internet abuse in the workplace (Verespej, 2000; Marsan, 2000). These commentaries have highlighted among other issues the losses in corporate productivity and the risks of damaging lawsuits in the wake of such abuse. Many companies, however, lack a clear vision of how to cope with Internet abuse, though some, like Xerox Corporation, are beginning to strictly implement their Internet access policies by taking measures such as firing employees who violate them (Merlino, 2000).

Internet abuse may be viewed as a kind of systems risk, i.e., the likelihood that a firm's information systems are insufficiently protected against certain kinds of damage or loss. As with systems risk, managers are generally unaware of the full range of actions they can take to reduce the problem (Straub and Welke, 1998). Therefore, an examination of research theories that have been applied to systems risk may prove relevant to Internet abuse. The general deterrence theory, drawn from the field of criminology, suggests that sanctions and disincentive measures can reduce systems abuse by making potential abusers aware that their unethical behavior will be detrimental to their own good (Pearson and Weiner, 1985).

According to this theory, strategies that can be adopted to reduce systems risk fall into four sequential activities: (1) deterrence, (2) prevention, (3) detection, and (4) remedies (Forcht, 1994). *Deterrent* measures include policies and guidelines for proper system use. These measures tend to be passive in that they have no inherent provision for enforcement and depend wholly on the willingness of system users to comply. *Preventive* measures include locks on computer room doors and password access controls, for example. These are active measures with enforcement that may ward off illegitimate

use. If deterrent and preventive measures are unsuccessful in containing abuse, then *detection* measures can be deployed. These include proactive security responses such as suspicious activity reports, system audits and virus scanning reports, or reactive responses such as detective work after a documented breach in security. These measures gather evidence of abuse and identify perpetrators. Finally, *remedies* are measures that can correct the harmful effect of an abusive act and punish the perpetrators. Internal actions include warnings, reprimands, and termination of employment. Legal actions include criminal and civil suits (Straub and Welke, 1998). Theoretically, these four kinds of defense can help reduce Internet abuse.

A company can start by deploying deterrent measures. If these are not successful, it can then use preventive, detective, and finally remedial measures. There is, however, limited evidence available in practice to prove the effectiveness of these four techniques despite their strong theoretical basis. This research, therefore, seeks to empirically support the general deterrence theory in the context of Internet abuse, to provide help for practicing managers.

Methodology

A two-stage methodology was adopted that consisted of interviews with managers to gather qualitative data, and a field survey of end users to gather quantitative data. Structured interviews were conducted with managers of 66 companies that allowed their employees Internet access. One manager from each of the companies was interviewed for a total of 66 responses. Forty-six of the companies were in the service sector, with the remaining companies in the manufacturing sector. The companies ranged in size from small (<500 employees, $n = 38$, $\mu = 113$ employees), to medium (between 500 and 1000 employees, $n = 16$, $\mu = 871$ employees), to large (>1000

employees, $n = 12$, $\mu = 12,517$ employees). Of the managers interviewed, eight were in Information Systems (IS) and the remaining were non-IS. These managers were asked to describe their companies' measures to reduce Internet

abuse by the employees. They identified 18 measures, which are shown in Table 1 and were used to develop the survey instrument for the second stage of the study.

Table 1

Measures to Reduce Internet Abuse (Percentage of companies using this measure)	Mean	Std. Dev.
To block access to nonwork related and offensive web sites by using Internet Filters (23.4%)	5.24	1.72
To terminate employees who abuse the Internet at work (22.4%)	5.11	1.94
To take away Internet privileges of employees who abuse the Internet at work (24%)	4.87	1.64
To monitor with special software all the Web sites visited by employees (26.6%)	4.85	1.53
To monitor with special software what every computer in the company is being used for at a particular time (15.1%)	4.61	1.82
To monitor electronic files downloaded on the computers of employees to identify if they are nonwork-related (16.7%)	4.60	1.71
To have managers reprimand employees who abuse the Internet at work (29.2%)	4.57	1.58
To monitor with special software all the e-mails of employees (20.8%)	4.51	1.74
To limit Internet access to only certain employees upon their supervisors' consent (25.0%)	4.30	1.86
To allow but limit personal Internet usage to employees in their free time, or after work hours, or in emergencies (17.2%)	4.14	1.82
To have employees who access Internet-enabled computers at work to log their name, time in, time out, and the reason for using the Internet (6.8%)	3.92	1.70
To watch on cameras all employees using computers (0.5%)	3.89	2.16
To use an 'Internet cop' to police the workplace for Internet Abuse (5.7%)	3.83	1.89
To have a written company manual/policy sheet/employee handbook/memorandum stating that the Internet at work is to be used for work related purposes only (42.2%)	3.70	1.73
To have employees sign forms stating that they will abstain from visiting offensive Web sites while at work (21.4%)	3.60	1.69
To have employees agree to accept the company's 'Internet Use Policy' when logging into their computers (18.7%)	3.55	1.65
To arrange seminars, staff meetings, and show videotapes to educate new and old employees about Internet Abuse (4.7%)	3.09	1.55
To have employees with Internet access at work fill out weekly log sheets describing their Internet usage (1.6%)	2.91	1.58

• Instrument Development

The survey instrument was divided into the following major sections:

(1) A definition of Internet abuse in the workplace which evolved from interviews with man-

agers in the first stage. This definition read "Internet abuse in the workplace is defined as sending or receiving nonwork-related e-mails, accessing nonwork-related Web sites, and subscribing or contributing to nonwork-related

Internet discussion groups during work hours while using the company's electronic resources.”

(2) The list of 18 measures from Table 1. Respondents chose from a 1 to 7 (1 being Not Effective and 7 being Very Effective) Likert-type scale to indicate in their opinion how effective each of the 18 measures would be in reducing Internet abuse in their companies. A nineteenth question allowed them to enter a measure and rating in addition to the measures from Table 1.

(3) Two questions that asked the extent to which the employees would abuse the Internet at work if (a) none of the 18 measures were in place, (b) one or more of the 18 measures was in place. A 1 to 7 rating scale allowed the respondent to indicate that extent.

(4) Questions for demographic purposes about the organizations' and subjects' characteristics. Seven end users affiliated with an organization that provided Internet access at work volunteered to participate in a pilot of the survey instrument. The pilots resulted in minor changes to the contents and introduction to the survey.

• *Subjects*

Three instruments were personally administered by each student (total number of students = 72) enrolled in an undergraduate management information systems class of a Mid-western university to three office workers the student was acquainted with. To ensure reliability and unique responses, respondents were required to list their names and telephone numbers at the end of the survey. Completed surveys came from 192 subjects for a response rate of 89%.

Data Analysis

Table 1 reports the perceived effectiveness of the 18 measures in reducing Internet abuse and the percentage of respondent companies actually using each measure. Factor analysis reduces a large number of items to a more manageable number, making key themes visible (Nunnally, 1978). It reveals, in effect, the items that belong together by showing which ones measure the same theme and how much they do so. A factor is thus a construct assumed to underlie a group of items or an individual one. A factor loading can be seen as the correlation between the item and a factor. Eigenvalues represent the amount of variance accounted for by given factors. Cronbach's alpha reliability coefficient measures the extent to which the items that load on a

factor correlate with one another.

The factor analysis revealed four factors and explained 64.36% of the variance in the data. Table 2 shows the factor loadings. Items with loadings greater than .5 were retained, so of the 18 measures, two were dropped because of inconclusive loadings. These were “terminate employees who abuse the Internet at work” and “limit Internet access to only certain employees upon their supervisors' consent.” In performing the factor analysis, we followed an iterative approach of dropping inconclusive loadings as described by Sethi and King (1994). To remove any kind of subjectivity from the analysis, we did not retain any measure that failed to load significantly on a factor. Cronbach's alpha reliability coefficients are shown in the table. The alpha values are greater than 0.6 indicating that the items in each factor do belong together. Table 2 also contains labels that the researcher applied to the factors. In general, most of the factors are meaningful sets of items, and the labels synthesizing the measures were easily identifiable because they tied in well with general deterrence theory. One factor, “explicit prevention and detection,” focused on the prevention and detection of Internet abuse by monitoring the activities of employees. Another factor, “coerced prevention and detection,” included measures that appeared intimidating with an intent to force employees not to abuse the Internet. A third factor, “deterrence,” included four measures that appear passive and require the employee's cooperation. The last factor, “remedies,” included two measures to punish offenders as well as one of cooperation with employees to allay the problem.

Multiple regression analysis shows the relationship among variables in the form of an equation. If an exact relationship does not exist, regression analysis chooses the “best” equation to describe the relationship. Regression coefficients are the coefficients of the explanatory variables in this equation. A measure of how well a multiple regression equation fits the data is provided by the coefficient of determination, R^2 , which represents the proportion of variation in the dependent variable explained by the regression. The F statistic provides an additional measure of how well the multiple regression equation fits the data. Nonsignificance of the F-statistic implies that the explanatory variables in the regression equation are of little or no use in explaining the variation of the

Table 2

Factor 1: Explicit prevention and detection($\alpha = .87$)	1	2	3	4
To monitor with special software all the Web sites visited by employees	.831	.151	-.04	.143
To monitor with special software what every computer in the company is being used for at a particular time	.814	.111	.137	.04
To monitor electronic files downloaded on the computers of employees to identify if they are nonwork-related	.784	.122	.229	.130
To monitor with special software all the e-mails of employees	.778	.164	.206	.113
To block access to nonwork-related and offensive Web sites by using Internet Filters	.692	.130	.09	.194
Factor 2: Coerced prevention and detection ($\alpha = .80$)				
To watch on cameras all employees using computers	.034	.808	.036	.195
To have employees with Internet access at work fill out weekly log sheets describing their Internet usage	.099	.792	.171	.092
To use an 'Internet cop' to police the workplace for Internet abuse	.157	.759	.147	.010
To have employees who access Internet enabled computers at work to log their name, time in, time out, and the reason for using the Internet	.027	.749	.043	.325
Factor 3: Deterrence ($\alpha = .75$)				
To have employees agree to accept the company's 'Internet Use Policy' when logging into their computers	.105	.08	.781	.253
To have a written company manual/policy sheet/employee handbook/memorandum stating that the Internet at work is to be used for work related purposes only	.140	.03	.767	.118
To arrange seminars, staff meetings, and show videotapes to educate new and old employees about Internet abuse	.133	.126	.636	.252
To have employees sign forms stating that they will abstain from visiting offensive Web sites while at work	.140	.367	.613	-.07
Factor 4: Remedies ($\alpha = .67$)				
To take away Internet privileges of employees who abuse the Internet at work	.260	.09	.123	.792
To have managers reprimand employees who abuse the Internet at work	.155	.487	.117	.646
To allow but limit personal Internet usage to employees in their free time, or after work hours, or in emergencies	.109	.06	.321	.617
Eigenvalue	12.21	2.63	1.36	1.31
% of Total Variance Explained	35.48	12.16	9.83	6.89
Cumulative Variance Explained	35.48	47.64	57.47	64.36

dependent variable.

Multiple regressions tested the relationship between the four measure factors described above and the (perceived) extent to which Internet abuse had been reduced due to the

measures. Table 3 shows the results of the regression including the individual regression coefficients for each of the four factors. It also shows each factor's mean perceived effectiveness.

Table 3

Factor (Mean Importance)	Regression Coefficients
1: Explicit prevention and detection (4.78)	.180*
2: Remedies (4.53)	.057
3: Coerced prevention and detection (3.63)	.057
4: Deterrence (3.49)	.014
R ²	.06
F	2.52*
*p ≤ .05	

Discussion and Implications

This research examined the general deterrence theory to determine if it was relevant to Internet abuse. It confirms that companies do indeed use deterrent and remedial techniques to counter Internet abuse as the theory predicts. However, the other two techniques, detection and prevention, do not show up as clearly in the factor analysis. The results show that Factor 1, a combination of detection and prevention measures, which we have called "explicit prevention and detection techniques" (e.g., monitoring with special software all the Web sites visited by employees, monitoring what every computer in the company is being used for at a particular time, monitoring electronic files downloaded on employee computers to identify if they are nonwork related, monitoring all the e-mails of employees, and blocking access to nonwork-related and offensive Web sites by using Internet Filters) is the only significant ($p < .05$) predictor of reduction in Internet abuse. Surprisingly, the other combined technique, "coerced prevention and detection," (Factor 2) and "remedial techniques" (Factor 4) do not appear effective in reducing Internet abuse. However, as predicted by the general deterrence theory, deterrent techniques (Factor 3) that lack inherent provisions for enforcement are not perceived to be effective in reducing Internet abuse.

This research demonstrates that the general deterrence theory can be applied to Internet abuse though its predictions are not entirely supported. Future research, however, could

refine and validate the measures developed here and retest the theory. Perhaps a causal model might shed light on understanding why the theory was only partially supported. An interesting point is that end users do not view coercive techniques as effective in reducing Internet abuse. Perhaps IS managers would have a different viewpoint? Replicating the study using IS managers as subjects might provide interesting results and useful comparisons.

Conclusions

This research helps identify for a practicing manager the measures that may be the most effective in reducing Internet abuse. It also provides a perspective of how other companies and managers are coping with this problem. An interesting revelation of the research is the wide breadth of measures that companies are using to reduce Internet abuse. Some of these may even seem to infringe upon the rights of employees (such as monitoring their screens and keystrokes), which raises ethical concerns. Should companies act as Big Brothers or could other means be used? For instance, several companies allow limited personal Internet usage to employees during their free time, after work hours, or in emergencies. A 'kinder, gentler' corporate image might in fact make employees loyal and more productive.

An interesting point is that the most widely used measure—having a written company policy barring Internet abuse (used by nearly 42% of the respondent companies)—is also considered

(continued on page 55)

Human Resources Report, 19 (46), 1285.
 Bureau of National Affairs, Inc., (2001b, October 15).
Human Resources Report, 19 (40), 1101-1102.
 Bureau of National Affairs, Inc., (2001c, November 12).
Human Resources Report, 19 (44), 1213.
 Bureau of National Affairs, Inc., (2002, July 29). *Human Resources Report*, 20 (30), 826.
 Davy, J., Kinicki, A., and Scheck, C. (1991). Developing and testing a model of survivor responses to layoffs. *Journal of Vocational Behavior*, 38 (3), 302-317.
 Dunham, K.J. (2001, November 6). Fair layoffs? *The Wall Street Journal*, CCXXXVIII (90), B10.
 Galinsky, E., Bond, J., and Friedman, D. (1993). *The national study of the changing workforce*. New York: Families and Work Institute.
 Gay, L. R., and Diehl, P. L. (1992). *Research methods for business and management*. New York: Macmillan Publishing Company.
 Gilbert, J.T. (2000, Spring). Sorrow and guilt: An ethical analysis of layoffs. *SAM Advanced Management Journal*, 65 (2), 4-13.
 Kilbourne, L.M., O'Leary-Kelly, A.M., and Williams, S.D. (1996). Employee perceptions of fairness when human resource systems change: The case of employee layoffs. In Woodman, R.W. and Pasmore, W.A. (Eds.), *Research in Organizational Change and Development*. Greenwich, CT: JAI Press Inc., 25-48.
 Kleiman, L.S. and Denton, D. (2000) Downsizing: Nine steps to ADEA compliance. *Employment Relations Today*, 27 (3), 37-45.
 Ohio Bureau of Employment Services (1998, November). *Ohio job outlook to 2006*. Columbus, Ohio: Labor

Market Information Division, Table 2.
 Ohio Civil Rights Commission. *Historical Data 1992-99*. Columbus, Ohio.
 Ohio Dept. of Job and Family Services, Bureau of Labor Market Information (2001, March). RS 203.1-B — Preliminary employment by major industrial division for Ohio and counties.
 Peters, P. (2000, May). 7 tips for delivering performance feedback. *Supervision*, 61 (5), 12-14.
 Samborn R. (1990, July). Many Americans find bias at work. *The National Law Journal*, 16.
 Stoner, C.R. and Hartman, R. I. (1997, Summer). Organizational therapy: Building survivor health and competitiveness. *SAM Advanced Management Journal*, 62 (3), 25-31, 41.
 Tang, T.L. and Fuller, R.M. (1995, Autumn). Corporate downsizing: What managers can do to lessen the negative effects of layoffs. *SAM Advanced Management Journal*, 60 (4), 12-15, 31.
 Tejada, C. (2001, December 4). Workweek. *The Wall Street Journal*, CCXXXVIII (109), A1.
 Title VII of the Civil Rights Act of 1964, 42 U.S.C.A. 2000e.
 U.S. Department of Labor (2000, December 8). *News*. Washington, DC: Bureau of Labor Statistics, Table A-1, Table B-1.
 Verespej, M.A., (1997, March 3). Time for ageless judgments. *Industry Week*, 246(5), 16.
 Walker Information (2001, September). *Loyalty in the Workplace: 2001 National Employee Benchmark Study*. Indianapolis, Indiana: Walker Information Global Network.

(continued from page 26)

one of the least effective. This clearly suggests that companies need to give teeth to their policy statements rather than mere lip service.

In conclusion, it also helps to visit a practical consideration. Most companies already have the means to track the Internet usage of their employees but choose not to do so because of the effort involved. Some practitioners we interviewed estimated the average cost of Internet abuse to their company (in terms of lost productivity) did not exceed the annual salary of one employee. Therefore, it may not be cost justifiable to add a new staff member to the IS department simply to monitor and eliminate the abuse. Eventually, however, every company must decide for itself if the risks from Internet abuse exceed the costs of lost productivity and alienated employees.

Dr. Mirchandani teaches information systems management and focuses his research on information systems planning and electronic commerce. He has also published widely in journals and conference proceedings. Dr. Motwani has published more than 100 articles in the areas of competitive strategies, inventory management, technology management, quality management,

and health care management. He also serves as consultant, trainer, and facilitator in the fields of total quality management, project management, and customer services.

REFERENCES

- Blumstein, A. (1978). Introduction. In A Blumstein, J. Cohen, & D. Nagin (Eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington D.C.: National Academy of Sciences.
 Forcht, K. A. (1994). *Computer security management*. Danvers, MA: Boyd and Fraser.
 Marsani, C. D. (2000, April 24). Employee study cites rampant Internet abuse. *Network World*, 17, 38.
 Merlino, L. (2000). Employers laid back over Internet abuse. *Upside*, 12 (5), 46.
 Nunnally, J. C. (1978). *Psychometric research*. New York: McGraw-Hill.
 Pearson, F. S., & Weiner, N. A. (1985, Winter). Toward an integration of criminological theories. *Journal of Crime and Criminology*, 116-150.
 Sethi, V., & King, W. (1994). Development of measures to assess the extent to which an information technology application provides competitive advantage. *Management Science*, 40 (12), 1601-1627.
 Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1 (3), 255-276.
 Straub, D. W., & Welke, R. J. (1998, December). Coping with systems risk: Planning models for management decision making. *MIS Quarterly*, 441-469.
 Verespej, M. A. (2000, February 7). Internet surfing. *Industry Week*, 249 (3), 58-64

