Measuring Severity of Internet Abuse in the Workplace: Creation of a Thurstone Scale

Craig C. Claybaugh  
*University of Wisconsin - Milwaukee*, claybau2@uwm.edu

Derek L. Nazareth  
*University of Wisconsin - Milwaukee*, derek@uwm.edu

Follow this and additional works at: [http://aisel.aisnet.org/amcis2009](http://aisel.aisnet.org/amcis2009)
Measuring Severity of Internet Abuse in the Workplace: Creation of a Thurstone Scale

Craig C. Claybaugh
University of Wisconsin - Milwaukee
claybau2@uwm.edu

Derek L. Nazareth
University of Wisconsin - Milwaukee
derek@uwm.edu

ABSTRACT
Access to the Internet at work allows employees to be more effective in their jobs. However, it also gives employees the opportunity to engage in non-productive behavior. Several studies have examined the problem of Internet abuse in the workplace. However, a measure of severity of Internet abuse is still lacking. This research employs a Thurstone scale to create an appropriate measure of severity of Internet abuse in the workplace.

Keywords
Internet abuse, severity of abuse, Thurstone scale

INTRODUCTION
It is clear that the Internet has brought some measure of increased productivity to the workplace. This increase in productivity has come in the form of a variety of efficiency gains, spanning search for relevant material, access to business data and information on-line, and processing of transactions. Tasks that otherwise would have involved the use of alternative technologies or slower processing in an off-line context, are now routinized in an efficient and effective manner. The simple act of searching on-line and downloading reference material for research is a far cry from the pre-Internet version which entailed a visit to the library, searching through paper-based catalogs, retrieval of the material from a stack of shelves, or through inter-library loan, and subsequent copying thereof. Access to the Internet in the workplace is commonplace and is generally expected to be offered to most white collar employees. Like any other technology involving discretionary use, it can also be abused. Problems range from a decrease in productivity, to network clogging, to an increase in the incidents of security breaches at an organization (Pee et. al. 2008). It has been estimated that more than 30% of Internet web-surfing is non-work related in nature. Given the large amounts spent by the corporate world on Internet access, this translates to non-trivial waste. Internet abuse, sometimes referred to as cyber-loafing or non-work-related computing, is defined as the voluntary use of the Internet by employees for personal purposes during standard working hours (de Lara 2006). Studies show that cyber-loafing is prevalent across different countries, and spans multiple activities (Lim et. al. 2002). The percentage of employees engaging in Internet abuse ranges from 40% to 70% (Shamra et al. 2003) depending on how Internet abuse is classified. In addition to productivity losses, companies also face added security risks and potential legal problems with unauthorized downloads of copyrighted material through non-work related use of the Internet. Some suggestions for addressing these issues are presented in Anandarajan and Simmers (2003).

Internet abuse falls into a category of behavior traditionally considered to be workplace deviance. As such, it is a behavior that most individuals would consider to be a violation of organizational or social norms (Lim 2002). With that premise, it then assumes the mantle of a behavior that is subject to disciplinary action. There is considerable anecdotal evidence that a wide variety of disciplinary actions have been taken against employees engaged in Internet abuse, ranging from simple cautions, to terminations, and prosecution, if the abuse is of a criminal nature. In the context of deterrence theory, it becomes important to determine the severity of the abuse, i.e. when does the use of the Internet cross the line and become deviant, and what deterrence remedy is appropriate? Clearly, there is a range of internet abuse, from the innocuous to the pathological. Something as simple as checking the weather will probably not entail serious action. On the other hand, viewing pornographic material, sending threats to others, and cyber-bullying might well entail discipline and possible legal and/or criminal prosecution. The severity of Internet abuse has not received much attention in IS research. This paper seeks to address that issue, creating a Thurstone scale to measure Internet abuse severity.

The rest of the paper is organized as follows. A review of prior research on Internet abuse in the IS domain is presented. Possible options for creating a measure for Internet abuse severity are then reviewed. The use of the Thurstone equal-appearing interval scaling method is discussed. A research study to create the Thurstone scale is described. Implications for use of the scale, limitations of the scale, and directions for future research round out the paper.
INTERNET ABUSE IN THE IS LITERATURE

Internet abuse has been the subject of several research articles. Some have been conceptual in nature. For example, Sharma and Gupta (2003) examine the relationship between Internet abuse and worker productivity. Others have sought to provide empirical support for theories about Internet abuse, e.g. investigating of causes and moderators of Internet abuse (Lee et al. 2002). The Communications of the ACM devoted an entire issue to the topic of Internet abuse in 2002 (Anandarajan 2002). Topics ranged widely, and included Internet use policies (Siau et al 2002), profiling Internet abusers (Stanton 2002), and potential liabilities a company might face due to sexual harassment concerns related to viewing pornographic material while at work (Panko and Beh 2002).

Lim (2002) was one of the early researchers to examine Internet abuse from a quantitative research perspective. Using theories of social exchange, organizational justice, and neutralization, she sought to explain how employees are motivated to engage in Internet abuse. This research classified Internet abuse as a deviant behavior and sought to find ways in which an employee would justify their engagement in such behavior. The study sought to identify and understand the factors related to this deviant behavior in order to help craft measures to cope with the behavior. The study found that employees are more likely to rationalize their misuse of the Internet at work when they perceive that their employers do not treat them fairly.

A number of studies have examined at the impact of acceptable Internet use policies and electronic monitoring as effective measures used to deter employees from engaging in Internet abuse (Siau 2002; Nayeem 1997). In early research on computer abuse, Harrington (1996) found that generic and IS-specific codes of ethics have little impact on computer abuse, though denial of responsibility appeared to be significant in judging and perpetrating abuse. The use of monitoring software has been advocated, and is commonly used in many corporate environments. However, it is not without consequences, and has been shown to negatively affect privacy concerns of employees and their job satisfaction. This impact on an employee’s attitude has also been found to reduce their productivity and result in increased union activity (Urbaczewski & Jessup 2002). Other possible negative impacts include a loss of morale and the encouragement of micromanagement by supervisors (Ariss 2002).

Other behavioral theories have been applied in an attempt to explain Internet abuse. Pee et. al. (2008) employed the theory of planned behavior and the theory of interpersonal behavior to explain Internet abuse. Using competing models, and data from graduate students, they found that the theory of interpersonal behavior explained more variance than that of planned behavior. Chen et. al. (2008) adopted a different approach examining Internet abuse as a function of addiction that is determined by individual difference and personality traits. They found that addiction leads to Internet abuse, and is influenced by locus of control and self esteem. Lee et. al. (2005) compared multiple theoretical perspectives in an attempt to explain Internet abuse in the workplace. Using a combination of general deterrence theory, theory of reasoned action, ethical decision making, and the technology adoption model, they assembled a model using rational and unconscious factors to explain Internet abuse, finding personal habits and perceived IS accessibility as significant factors affecting non-work-related computing.

One of the more common theories applied to Internet abuse studies is general deterrence theory. This theory is drawn from the field of criminology and has been applied to a variety of research on information systems (Mirchandani and Motwani, 2003). Deterrence theory has been applied to the concepts of systems security (Straub, 1990), computer abuse (Harrington, 1996; Lee et. al. 2004), and systems risk (Straub et al, 1998). The general aim of deterrence theory is to prevent the behavior from occurring. Possible strategies for dealing with the problem include adoption of an acceptable use policy, monitoring of Internet usage, selective blocking of material, and in more egregious cases, disciplinary action against employees. Lee and Lee (2002) employed deterrence theory in conjunction with social bond theory, social justice theory, and theory of planned behavior to develop a holistic model of computer abuse. The model is presented in conceptual form only. Deterrence theory and social control theory were employed by Lee et. al. (2004) to explain computer abuse by insiders and outsiders within the work environment. Though not truly focused on Internet abuse, their study found that organization trust factors and the presence of security systems played a role in the intention to engage in computer abuse. de Lara et. al. (2006) investigated the role leadership proximity, organizational control, and fear of punishment on the intention to cyber-loaf. They found that fear of formal punishment has the opposite effect, with a more controlling climate resulting in greater cyber-loafing, thereby suggesting that deterrence may be a poor strategy to control Internet abuse. An examination of 18 possible deterrent actions on the extent of Internet abuse was conducted by Mirchandani and Motwani (2003). Their study found that monitoring and blocking actions (term this derived prevention and detection) was the only factor to have a significant effect on Internet abuse reduction, with policies, contracts, and remedial action having considerably less impact.

Other research in the area of Internet abuse draws from deviant workplace behavior theory. Workplace deviance and the theory of planned behavior forms the basis for a model examining adverse usage of IS assets (Tanveja 2006). This research found that attitude towards adverse usage, social influence, perceived behavioral control, and moral norms were significantly related to intention towards adverse usage. Deviant workplace behavior typologies formed the basis for the creation of a scale.
for cyber-loafing (Blau et al. 2006). Based on data collected from 415 medical technologists, they determined that cyber-loafing fell into three distinct categories, namely browsing-related, non-work-related e-mail, and interactive cyber-loafing.

Despite all the prior research in Internet abuse, the notion of severity of Internet abuse has not been adequately tackled. The extent and severity of abuse would appear to play a key role in any disciplinary action taken against employees who engage in Internet abuse. This paper seeks to create a measure of Internet abuse severity through the use of multiple statements that describe Internet abuse. This is done through the use of an equal appearing interval Thurstone scale.

CREATING A SCALE TO MEASURE INTERNET ABUSE SEVERITY

Accurately measuring the severity of a phenomenon has proved to be a challenge in many disciplines. Several different approaches have been adopted, using scales that range from ordinal scales to ratio scales. In the medical field, physicians routinely query patients about the severity of pain they are experiencing on a scale of 1-10. Without adequate anchors for these end-points, responses are usually very subjective, situation specific, and lack consistency across episodes. The physical sciences, particularly atmospheric sciences, also employ a host of scales to measure severity of atmospheric phenomena, most of which are ordinal in nature, e.g. Beaufort scale for wind force, Saffir-Simpson scales for hurricane intensity, among others. In the field of software quality assurance, the severity of error and defects has been categorized using an ordinal scale ranging from “mild” to “catastrophic” (Beizer 1990), based on the consequences of the bugs reported. Despite their evident shortcomings, severity scales continue to be employed, since they provide a meaningful basis for comparison. Creating a scale for severity of Internet abuse involves one critical distinction, though. Most severity scales are aimed at assessing the severity of a specific incident. In the case of Internet abuse, a single incident will not adequately specify the severity of abuse on the part of an individual. Rather, a pattern of use, or in this case abuse, will determine the severity of the phenomenon. Therefore, the scale for Internet abuse needs to consider the range of uses of the Internet, and some measure of their relative impropriety. The Thurstone scale of equal-appearing intervals was deemed to be an appropriate choice in this case.

The Thurstone scaling method has several applications in social science research. The method has been used to measure perceptions of crime severity (Kwan 2002) and been applied to the concept of market orientation (Wrenn 1997). The scaling method has also been applied to measure a range of perceptions related to technology. Duggan et al. (2001) examined student attitudes towards the use of the Internet for educational purposes. Seuntiens et al. (2006) looked at perceptions of image quality based on different image coding and camera angles. However, the methods has seen little application in the IS research area.

The creation of a Thurstone scale using the method of equal-appearing intervals begins with the development of the focus for the scaling research. In the case of this research that statement revolves around the concept of Internet abuse severity. The focus for this list is on the tasks that constitute Internet abuse. It does not try to address other dimensions that might measure severity such as duration of the action or frequency of its occurrence. The first step in the Thurstone scale creation process is to create a large set of potential statements, preferably 80 to 100, that describe Internet abuse. All statements need to be worded similarly and should not differ in grammar or structure. The statements also need to span the range of what is acceptable to unacceptable (Thurstone 1959). A panel of eight individual experts familiar with Internet abuse was used to generate statements to include in the potential list of scale statements. These experts were chosen such that they equally represented gender (four males and four females) and were representative of different ages (raged from 25 to 49). They were given a definition of Internet abuse and the following statement:

“Generate statements that describe specific examples of how an individual might engage in Internet abuse in the workplace.”

Statements generated by the panel of eight were pooled into a single list of statements. After elimination of duplicates, and removal of subsumed items, a pool of 94 items remained.

The next step in the creation of a Thurstone scale on Internet abuse is to submit the list of statements to a group of respondents who act as judges. The judges are asked to rate the statements from 1 to 11 to indicate whether the action is acceptable to be performed at work, with 1 representing acceptable use and 11 unacceptable use of the Internet at work. Judges were instructed to use the whole range of possible ratings and not cluster responses at either extreme. A pretest of the instrument was conducted using eight IS faculty members and doctoral students. Based on the pretest, some additional clarifications were added to the instrument. These included:

- All the activities would take place during standard working hours.
- None of the activities are work-related activities, and all involve use of the Internet.
- Internet sites were not blocked, i.e. it would be possible to use the Internet at work as specified by the item.
The activities would not be performed during a break or during a lunch hour.

A pilot test was conducted to test the feasibility of the method. The test represented a convenience sample of 30 professionals at four corporate institutions, and was administered using Survey Monkey. The items were spread across three data collection screens, and the survey also collected some demographic information. Results from the pilot indicated that the length of the survey proved challenging, with 20 respondents finishing the entire survey, 24 completing the first two screens, and all 30 completing the initial screen. This prompted the researchers to reduce the number of items being rated to about 60. Redundancy, overlap, and similarity formed the basis for exclusion of about 30 items. After reviewing the final list for the range of Internet activity, a few items were added back, bringing the final total to 63, as depicted in the Appendix. The final set of items was randomly ordered. For the main data collection exercise, a paper survey was employed. The respondents were graduate students enrolled in master’s level classes at a Midwestern university. All respondents were employed full-time, and had access to the Internet at their place of work. Eighty-five individuals participated in the data collection process. Eighty-two individuals rated all statements. Fifty of the respondents were male and twenty five were female – not all respondents answered this question.

The next step was to analyze the ratings of the statements using the median and interquartile range (between the first and third quartile) for each item. The interquartile range is a measure of the ambiguity of each statement, since high agreement of a statement’s rating will correspond to a low interquartile range value (McIver and Carmines 1981). The median places the item along the rating scale, while the interquartile range indicates a sense of variability among judges. Using this information, the final statements for the scale can be selected for the instrument. Thurstone provides three criteria for selecting the final scale items. First, items are chosen with the median values distributed along the full range of the scale. Thus, items should be selected such that they span the entire range of the rating of 1 through 11. Second, given that a set of statements have the same or similar median, those with the smallest interquartile range should be selected, using the premise that lower interquartile range reflects less disagreement among the judges concerning the statement. Finally, the items should be chosen to fall at as many equal-appearing intervals along the scale as possible. (Thurstone 1959)

The final items for the scale appear in Table 1. The items reflect the entire range of median values and have a minimum interquartile range. The statements selected also reflect a wide range of activities involving the use of the Internet at work. Two observations are of note in this case. First, several items qualified for inclusion as the last item on the scale, with a median of 11 and an interquartile range of 0. These included “Sending anonymous threats to employees”, “Sending spam”, “Viewing pictures that are considered to be pornographic”, and “Watching videos that are considered to be pornographic”. While all items meet the criteria for inclusion in the final scale, the choice was based on propensity to respond in the affirmative to the item. Second, the interquartile ranges were higher for the main sample when compared to the pilot test. This reflects the larger sample size, as well as the diversity of opinion of the participants.

**Table 1 – Rating of Statements on Internet Abuse**

<table>
<thead>
<tr>
<th>Statement</th>
<th>Q1</th>
<th>Median</th>
<th>Q3</th>
<th>IQR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking today’s weather</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Looking up a local business phone number</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Checking traffic information online to estimate how long your commute will be</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Responding to personal email received at a company account</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>Finding a volunteer opportunity with a local nonprofit organization</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Accessing and responding to email at a private account from another ISP</td>
<td>4</td>
<td>6</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>Looking up stock information for personal purchase</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>Checking to see how much your house is worth</td>
<td>6</td>
<td>8</td>
<td>9.75</td>
<td>3.75</td>
</tr>
<tr>
<td>Uploading personal pictures to a picture sharing website</td>
<td>8</td>
<td>9</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Viewing movie trailers</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>Viewing pictures that are considered to be pornographic</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>0</td>
</tr>
</tbody>
</table>

**DISCUSSION**

Using the Thurstone scale provides an easy approach to measuring severity of Internet abuse. The items are randomized and presented as binary choices of ‘agree/disagree’, or in this case, ‘yes/no’. The predetermined scale scores are then averaged for the ‘yes’ responses representing the severity of a respondent’s Internet abuse. This approach implies implicit equal weights.
among the items. If appropriate, frequency scores can also be collected so as to produce a more accurate measure. The construct then can be used in further research on Internet abuse. Several different areas for use of the scale are available. As a first cut, it can be used to determine if demographic, personality, and individual difference items play a role in explaining the severity and extent of Internet abuse. It would also be invaluable in studies assessing the perceived appropriateness of any disciplinary actions associated with Internet abuse, especially in light of prior research where formal proscription appears to have the opposite effect. It should be noted that the severity of Internet abuse in not a perfect surrogate for the amount of Internet abuse that an individual employee may engage in. For studies involving application of deterrent sanctions, the amount of abuse represents a combination of severity, extent, and frequency of abuse. Clearly, abuse that involves greater severity, longer duration, and greater frequency will be perceived as more abuse, though the measure may not be easy to formulate, and may vary from one context to another. Thus for example, extended periods and high frequencies of low severity abuse, e.g. checking the weather, may not be perceived to be as problematic as short periods of one-time abuse of high severity, e.g. viewing pornographic material. While productivity and expense issues have often been cited as a concern for curbing Internet abuse in the workplace, organizations are more likely to view liability and legal ramifications of Internet abuse as the basis for formulating acceptable Internet use policies in the workplace. In all likelihood, different organizations will apply different criteria for determining the tolerable amount of Internet abuse in the workplace.

There are a number of limitations to this research study. First, the use of a convenience sample to collect the data poses some concern. While the respondents were all employed and had access to the Internet at work, it is arguable that they are truly representative of the workplace population, particularly on dimensions of age and gender. The responses indicated that gender and age played a role in the ratings of the statements. Interests are clearly different between the genders with males more representative of the workplace population, particularly on dimensions of age and gender. The responses indicated that gender and age played a role in the ratings of the statements. Interests are clearly different between the genders with males more interested in sports and women more interested in entertainment and family content (Statton 2002). A random sample would provide greater confidence in the scale creation process. Though the respondents were asked to set aside any policies on acceptable Internet use that are present at their place of work, it is unclear if they were able to effectively do so.

Another concern is the long-term stability of the scale. While the scale is indicative of activities that constitute Internet abuse today, its value could erode over time. Two distinct possibilities emerge here. First, the range of activities covered by Internet abuse will undoubtedly grow larger. If these other activities assume a more mainstream nature and crowd out the current set, then the robustness of the scale becomes questionable. The second concern reflects changing social mores. If accessing adult content is no longer viewed as unacceptable behavior in the future, then the effectiveness of the scale is compromised.

CONCLUSION

Internet abuse continues to remain an ongoing concern for organizations. There is plenty of anecdotal evidence that this problem has not diminished. As organizations seek to reduce productivity losses, as well as limit exposure to risk, liability, and criminal prosecution due to Internet abuse, some measure for the extent and severity of the abuse is necessary. To date, the research on Internet abuse has not addressed the issue of severity. This paper created a Thurstone scale to measure severity of Internet abuse to address this gap. The scale can be can be used to study differences between groups, and their attitudes and propensity to engage in Internet abuse, as well as determine appropriate antecedents and consequence for Internet abuse based on the severity and extent of the abuse.

REFERENCES


Appendix

Original set of items

1. Looking up yesterday’s sports scores
2. Planning a personal trip
3. Placing a bid for a collectible at an auction site
4. Reading articles about politics
5. Forwarding a chain email
6. Emailing risqué material to a coworker
7. Sending anonymous threats to employees
8. Engaging in a chat session on sports
9. Playing fantasy football
10. Paying bills via internet banking
11. Accessing and responding to email at a private account from another ISP
12. Viewing and responding to local personal ads
13. Looking up movie show times
14. Selling personal items on eBay
15. Looking up the latest reviews for a future game you are thinking of purchasing
16. Checking today’s weather
17. Conducting on-line research about a medical condition
18. Using instant messaging to keep in touch with friends
19. Using social networking sites
20. Using the Internet to make personal long-distance phone calls
21. Reading and responding to newsgroups
22. Responding to personal email received at a company account
23. Sending spam
24. Checking to see how much your house is worth
25. Updating Wikipedia entries online
26. Looking for another job on a site like monster or hotjobs
27. Viewing movie trailers
28. Filing one’s taxes electronically
29. Updating a personal blog
30. Viewing pictures that are considered to be pornographic
31. Checking personal 401K status
32. Viewing online videos on YouTube
33. Looking up information on an actress or actor that is considered gossip
34. Checking local newspaper site for local news
35. Updating your Facebook or Myspace page
36. Using music sharing web sites
37. Finding driving directions to a restaurant
38. Finding a dentist
39. Searching for food nutritional information
40. Buying music on iTunes
41. Playing a game online
42. Checking car information online for a future purchase of an automobile
43. Looking up stock information for personal purchase
44. Reading blogs for personal interest
45. Researching consumer reports of items for future purchase
46. Reading and writing on online entertainment forums
47. Reading online national and international news
48. Uploading personal pictures to a picture sharing website
49. Looking up restaurant locations and menu items online
50. Booking personal travel online
51. Checking traffic information online to estimate how long your commute will be
52. Watching videos that are considered to be pornographic
53. Placing bets on a forthcoming sporting event
54. Finding a doctor
55. Downloading a game demo
56. Posting your resume on a job website
57. Finding information about a potential future travel destination
58. Finding a volunteer opportunity with a local nonprofit organization
59. Looking up a local business phone number
60. Managing a personal business online
61. Finding a walkthrough for a game you just purchased
62. Changing your 401K investments
63. Donating money to a local charity