Investigating the Knowledge, Attitudes and Habits of Academic Users Regarding Computer Usage Policy

By:

Brian Johnston

ID: 108956

In accordance with the requirements of the
Masters of Information Systems Security Management program of

Concordia University College of Alberta

August 2010

Abstract

Academic organizations typically require individuals using their information technology resources to agree to follow a set of rules regarding usage of those facilities and resources that the organization sets out as its computer usage policy document. Users may have to read a document, agree online via web script or be held to the policy by a statement in the institution's calendar. But, regardless of this, what do they actually know about the document's specific contents, what attitudes do they form toward the policies set out there, and how are both reflected in their actual usage of the facilities and IT resources? In this study I attempt to address questions of this kind based on responses from an online survey of users at the Concordia University College of Alberta.

Acknowledgements

I wish to thank my supervisors on this project, Ron Ruhl, MBA and Pavol Zavarsky, PhD, who provided academic and morale support through this study, and to my father, J. Paul Johnston, MA, for editing assistance and a dearly-needed refresher course on social statistics.

Universities, research institutes, schools of all kinds, governments, corporations and unions – indeed, organizations of any kind and scale which employ computers and modern information technology to conduct their affairs – regularly require individuals using those facilities and resources first acknowledge and agree to follow a set of rules the organization puts forward as a computer usage policy document. How well do users actually follow through on that requirement? Do they read the policy document carefully and completely before they click on the "I accept" button, or do they just click the button? What do they actually know about the regulations set out in it and the responsibilities they take on in agreeing to its requirements? What attitudes do they form about having to agree to those policies, both in general and with respect to specific policies? And, how is their actual behavior in making use of an organization's computer facilities and its IT resources influenced by the user's knowledge of the contents of computer usage policy document put forward?

These are questions relevant to the security of an organization's computer facilities and IT resources. Yet, apparently little research has been done that is directed specifically toward answering them in any empirically-based fashion. The research presented in this paper offers a beginning effort in that direction. It describes the results of a voluntary online survey of computer users at the Concordia University College that attempts to assess the extent and accuracy of their knowledge of the contents of the usage policy document established there, their attitudes toward certain aspects of it, and their habitual usage of the facilities and resources in question.

The discipline of Information Security Management holds that information security is materialized through managers' actions. Managers establish security by externally imposing it through the creation and publication of policies and guidelines governing usage of IT assets, and internally through the use of access control lists and system permissions, while ensuring the spirit of security via adherence to society's laws and strong professional ethics. Hence, this view specifically places the responsibility for establishing security squarely on an organization's managers.

However, while managers may decide what policies and procedures are mandated, they are not the people who generally perform the actions leading to a secure environment. Rather it is the ordinary end user who determines whether the usage restrictions are actually observed in practice, through the day-to-day understanding of and adherence to said policies, permissions and principles. Consequently, there is a empowerment of the ordinary users, who become the ultimate "keepers" of the security of information contained in and transmitted through the Internet, and not those who frame and impose the regulatory policies that apply to such use. Because of this important consequence, it is worthwhile to the Information Security noosphere to investigate the impact the average user has on security. To do this, we should define the world in which the average user exists, security-wise.

It can be reliably assumed in our present electronic age that the average user uses IT assets for a variety of purposes spread across a range of differing contexts. For example, the user may employ such assets to conduct the day-to-day responsibilities of their

employment. Use of these assets for employment-related duties and “personal business” may be subject to a range of permissions and restrictions on time, content, and intensity, this range delineated by company mandate, societal influence or personal motivation. Usage may occur at a place of employment, in a personal or public space, or in transit between locations. These different locations may subject the user to differing sets of, formal or informal, guidelines regarding the use of those assets (possibly altering the set of IT assets in the process, further complicating the issue).

Are users conscious of this dynamic regulatory environment? Perhaps, they are aware of the various rules in place and agree with the intent of the policies they reflect. If so, which subsets of guidelines are dominant during which periods of usage and in what locales? Or, maybe they are not so informed. Can they be charged with avoiding the observance of them? Indeed, if users are not aware of the policies in force but nonetheless adopt practices that conform to them, can they be said to be adhering to those policies? Then, there is the condition where knowledge of the guidelines is present, but policy intent is at odds with users' desires, leading to a question of enforcement. If the rules are seen to be unenforceable, would recognition of such a situation lead to widespread non-observance of the policies in question or will users see the benefit intended by the policy for adopting the desired practice? Or, if the laws are enforceable, will users refuse to adopt the practices called for under the policy even if doing so is punishable? These are all key questions one must answer in addressing the user's role in defining the security of the Internet that is achieved in practice. Answers that may give future policy writers a better grasp on what limitations can be reasonably imposed upon a general population of users.

No scholarly publications (regarding information security) that investigate the relationship between policy and action on these matters could be found, although it is likely that related studies may have been done in other areas of the social sciences (e.g., works on management theory, human behaviour, etc). Therefore, in this study I investigate what relationships exist (if any) between a user's knowledge of security policy as reflected in the questions asked about it in my survey, their adherence to it, and their intent either to fulfill or to deny it as reflected in their reported usage practices. Owing to time and financial resources, it does so only for a limited range of issues, in no way as broad as the number set out above. However, the research is a limited beginning toward addressing that larger research agenda.

Methodology

To address these questions, a study was conducted using a survey based on anonymous, voluntary participation. Therefore it was not a concern of the study to create a balanced population to drawn a random sample from. Despite this choice restraining any findings to be applicable to only the sample itself, it was felt that any notable relationships so found might spur more rigorous investigations in the future.

This survey was constructed with the designed goals of participants being motivated to answer truthfully and completely, despite several aspects of the questions dealing with

potentially illegal or unethical behaviour. Thus the survey was written with a concern for the participant's potential concern to remain anonymously and their time spent in answering. This limited the size of the survey and the construction of the questions to a short list of multiple-choice, single-answer items.

This resulted in a survey having four sections: basic demographics, followed by sections that respectively tested knowledge of computer usage policy, attitudes towards potential usage and habits surrounding said usage. Demographics were limited to asking about the participant's age range and their generalized role within the participating institution. Two sets of indicators, each comprised of eight items, were used to assess the extent and accuracy of the respondents' knowledge of the contents of the computer policy document governing use of the computing facilities and resources at Concordia University College. The items in the first of these two sets dealt with such matters as who can use the university's computer facilities and IT resources, what constitutes appropriate use of them, the university's right to inspect and oversee such usage and the provision of security guarantees regarding both the facilities and data stored on the university network. The second set of items focuses on the user's responsibilities towards the institution's IT assets, as outlined in the usage document. For each of these two sets, four of these items ask about provisions or expectations that actually appear in the computer policy document whereas the remaining four deal with issues not formally included there, with respondents being asked to check off the items whose contents do appear in the policy document. Thus, for our purposes here knowledge of what is in the document includes knowing what is not in it, as well. Attitudes towards IT asset usage were evaluated by asking respondents to rate several categories of websites on an ascending scale of five descriptive permission terms. These choices were selected for the study on several factors, the two dominant ones being presence on the Internet and potential social impact. Habits of use were also checked in this fashion, with the descriptive scale being of four items.

Evaluation of the data was done using basic statistical techniques for frequencies, and for the purposes of nominal variable association, we used Cramer's V measurement, as it is the most appropriate measure to use on large or rectangular matrices. For ordinal variables in rank-ordered correlations, we used Kendall's Tau-b correlation measurement, as the data has a large number of ties in the rankings, however Gamma is mentioned as a comparative value in certain tables.

Participants were recruited to the study's population via an email-based appeal to the student, faculty and staff of the institution. The survey was administered using two separate implementations of the same question set, it being made available in an in-person paper-based proctor-administered version and a self-administered internet-accessible version. The internet-accessible version was facilitated through the contracting of the online survey distribution company, SurveyMonkey.com, to provide distribution and content hosting services. This resulted in 169 respondents, of which 34 withdrew from the study before completion, leaving a total of 129 completed surveys for analysis.

Analysis

The purpose of the research reported here was to discover what individual computer users at the Concordia University College of Alberta know about the content of the computer usage policies set out by the University in their policy document, to assess how accurate their knowledge of such matters is, and to investigate what impact that has on attitudes they hold toward one area of usage – restrictions on users' access to different kinds of sites through use of University facilities – and on their actual usage of those facilities for a range of activities.

I will begin by describing the age and role composition of my sample, since individual differences with respect to knowledge, attitudes, and usage behavior may be effected by the age of a user and their role within the University College community. Next, I will present my findings concerning the respondents' knowledge of the content of the institution's policy document, move on to report on the data collected on their attitudes, and then discuss their reported patterns of actual usage. In each of these three sections I begin by presenting information about the general patterning indicated in the frequency distributions of the responses. Following this I will indicate any noteworthy associations that can be attributed to the influence of users' age and their role at the University College and comment on the nature of such relationships. A fourth and closing section will draw together the information presented in the three previous areas of investigations, assessing not only the extent and accuracy of their knowledge of the institution's usage policy document, but also its influence on their attitudes and reported actual activities. Whatever broad conclusions I arrive at as a result of that discussion, as well as suggestions about the need for future research arising from my research, will bring the report to an end.

Composition of the Sample by Age and Institutional Role

Of the 121 persons who comprise the final sample of respondents in my survey, seventy-five (62.0%) placed themselves in the youngest age category on the age variable question. Thirty-two (26.4%) persons reported their age as between thirty and forty-nine years made up the second largest group. Only fourteen respondents (11.5%) recorded their age as fifty years or older. Seventy-one of the persons in the youngest age category identified their role as undergraduate (61) or graduate (10) students at the University College. As one might expect, teaching faculty and administrative staff were primarily drawn from the two older age categories, as one-fourth of the persons falling in the "30 to 49" age group identified themselves as being teaching faculty and another fifteen (46.9%) of the thirty-two persons in that category described themselves as administrative staff. This pattern becomes even stronger for persons fifty years old or older. Of the fourteen persons comprising that group, six (42.9%) designated themselves teaching faculty and another seven (50.0%) reported being administrative staff. In passing, it should be noted that no persons listed their role as being research faculty or as contract researchers, and that another eight persons classified their role as "other unspecified." These two categories were excluded from the study, so as to reduce ambiguity in the implicit ordering of the list of roles, leaving 121 cases as our final database.

The joint distribution of respondents with respect to the age and role variables is presented in Table 1. It is clear from the patterning of that distribution that a moderately strong, positive association exists between these two variables. The Cramer's V coefficient reported for that table (0.575) confirms this interpretation. Curiously, a respondent's role seems to correctly predict their age grouping then their age grouping predicts their institutional role. This is indicated by a higher lambda coefficient (λ: 0.413) in the first case than in the second case (λ: 0.321). The reader should note that the frequency distribution for the Age variable appears as the right-hand marginal total in Table 1.

What do these 121 persons know of the content of their institution's computer usage policy document? And how is that knowledge shaped, if at all, by their age and role in the institution? Answering these two questions will be our next task.

Knowledge of Policy

Our respondents' knowledge of the contents of the institutional usage policy document was assessed using the two sets of questions already described earlier in the methodology section. The first set of eight questions [KA] focus on whether users are allowed to engage in specific activities or not, with the frequency distributions of responses given for the items in this set presented in Table 2a. The second set of eight questions [KB] judged the respondents' grasp of user responsibilities as stipulated by the usage policy. These responses are given as a set of frequency distributions in Table 2b. Due to space constraints, item labels may be used with their descriptors listed in a legend below the respective table. These labels may be used in the body of this work, but only to speed the reader's table referencing.

The most noteworthy feature of the frequency distribution of the first set of items is the rather low rate of accuracy that the respondents achieved. For six of the eight items in the set, the percentage of persons who answered correctly ranged between 34.7% and 15.7%. A seventh item, that deals with the presence of guidelines for altering or renewing passwords, was correctly identified as being absent from the policy by 43.0% of those persons answering. Only the item dealing with an expectation that institutional computer resources would be used in an ethical and effective manner – itself almost a "gift" question – was correctly identified by a large majority (90.9%) of participants in the study. Judging from these results, the respondents are not very knowledge about the kinds of activities that are permitted or proscribed by the usage policy.

Turning to the frequency distribution of responses to the second set of items, we see a markedly improved rate of accuracy from the respondents, as the percentage of respondents answering correctly ranged between 54.4% to 89.6% for five of the eight items. Of note is the third item in this second set, where respondents answered incorrectly 94.4% of the time, deals with the usage policy's requirement for users to be responsible for the general maintenance of security (antivirus tools, physical security, etc) of any IT assets they regularly use or are entrusted with.

The data presented in Tables 2a and 2b describe the level of accuracy, item by item, for the respondents taken as a group. But what level of accuracy do the individuals achieve over each set of questions? To assess this, I created two indices, [KARight] and [KBRight] by summing the number of correct answers a person gave across each set of items, with each index having a potential score range of zero to eight. The frequency distributions of scores in these two indices are given in Table 2c. Note that the distribution of KARight scores is flatter and more skewed (positively) then the KBRight scores, which display a more symmetrical shape. Additionally, the mean number of correct answers for KBRight (4.3) is greater than that for KARight (3.1), and KBRight's standard deviation is smaller that KARight's standard deviation, as well (1.3 v 1.6). All these markers indicate that our respondents have a greater overall knowledge of personal responsibilities than of the permitted/proscribed activities, as these matter are set out in the usage policy document.

Looking at the associations between the demographic data and the two indices, we found that older respondents show slightly higher scores on the KARight index than younger ones (Kendall's Tau-b: 0.212, Gamma: 0.312), whereas no systematic age difference on scores for the KBRight index were found. In contrast, a person's role at the university does seem to affect their accuracy score on both of the indices. Persons placed higher in the hierarchy of roles at the institution had slightly higher scores one the KARight index (Kendall's tau-b: 0.189, Gamma: 0.264) whereas the reverse is true for scores in the KBRight index (Kendall's tau-b: -0.154, Gamma: -0.221)

To what extent does a person's age or role then have on their knowledge of the policy document's contents? Examining the rank order correlations between the scores within these two indices and the demographic data, I found only a positive association between age and overall score for the first set of items KA] at a Cramer's V value of .305. Institutional role appeared, at least at first glance, to have no effect on either knowledge of permitted activities or on knowledge of user responsibilities specified within the usage policy document. Extending the analysis of role to a finer granularity on the two sets of questions gave us the results as shown in Table 2d, which indicate that in fact that the responses given on several of the separate items are significantly correlated with the participants' institutional role.

In summary, we have found that, in general, our respondents have a notably greater knowledge of their responsibilities as stated in the usage policy document than of the activities that are permitted or proscribed under the same document, and that age and role play little part in the participants overall knowledge beyond that age has a mild positive effect on knowledge of permitted/proscribed activities.

Attitudes Towards Site Access

Whether students or employees who have institutional accounts can use them to visit certain kinds of sites or engage in certain kinds of activities is a very controversial issue at present and promises to grow more so in the immediate future if current trends hold true. One might well expect that this issue is easily resolved for certain kinds of sites and

activities that breach laws and social mores, for example, hate speech and other kinds of illegal sites and hardcore porn sites. Here, the norm would be to adopt policies that proscribe using institutional computer facilities to visit sites that prompt behaviour unwanted in the institution. However, adult sites remain probably the most commonly visited sites on the Internet and gambling sites are also quite popular. Although gaming and social networking sites escape much of the moral disapproval that links to the kinds of sites noted above, employers and others administering computer facilities at institutions are increasingly concerned about persons using their facilities access such sites, seeing it as an inappropriate use of those facilities. In contrast, many might regard banning the use of institutional facilities to access social, religious and political sites as almost constituting a restriction of one's freedom of speech and assembly, if not violating the traditional academic spirit of research freedom.

Participants in the study were asked whether users should be always able to use institutional computing resources to visit a particular kind of site, usually yes, doing so should depend on the circumstances, usually not, or never able to do so. The sites considered were: adult sites, political or social movement sites, counterculture or subversive movement sites, criminal or illegal sites, anonymizer or proxy sites, torrent aggregator sites, religious sites, and social or social communication sites.

The frequency distributions of respondents' attitudinal judgments regarding what access users should have to such sites from University computer facilities are presented in Table 3a. In this table, sites do not follow the numerical order assigned to them in the questionnaire; rather, they have been re-ordered to contrast the extent to which respondents are predominately prescriptive (choose "always") versus being overly proscriptive (choose "never") in rendering their judgments. It is obvious that the re-ordering of columns reflects a clear pattern in the responses. A strong majority of persons adopt a sharply proscriptive attitude toward allowing users to use institutional computing resources to access illegal (73.2%) and adult (66.1%) sites. A simple majority (53.6%) takes the same position about accessing torrent sites and a clear plurality (41.6%) do so regarding proxy sites. And, in all four cases a two-thirds majority of them choose either "never" or "usually no" as their response. On the prescriptive or permissive side of the question, a simple majority of persons think that users should always be able to access religious sites (51.2% using the University College facilities and clear pluralities take that position for social (41.6%) and political (35.2%) sites. By combining those who choose either "always" or "usually yes" as their response, we find strong majorities for all three sites. In essence, the respondents generally took either a proscriptive or prescriptive perspective on this matter, with markedly less ambiguity in comparison. Only in the case of counter-cultural sites is there any notable difference of opinion indicated. The modal choice in responding there is "depends".

This pattern of responses is also reflected in the matrix of Kendall's tau-b rank-order correlations reported in Table 3b. Here, judgments given about one kind of site are correlated with those for each of the other kinds of sites. A distinct clustering of the judgments about political, religious, social and countercultural sites is indicated. The average correlation among sites here is 0.543, indicating a relatively tight cluster. A

second, looser (the average correlation being only 0.323), cluster links together the remaining four kinds of sites. Closer examination of the correlations involving proxy sites, however, reveals that it links to both clusters almost equally well. Overall, we see that the prescriptive versus proscriptive contrast organizes the judgments regarding whether use of institutional facilities for accessing these kinds of sites should be permitted.

Curious as to whether or not knowledge had any apparent impact on attitude, we looked at a Cramer's V association of each of the two indices, KARight and KBRight, and compared them against the attitude values. We were surprised to find that no significant associations existed, implying that knowledge of the content of the institutional usage policy has practically no effect on participants' judgments on what websites may be accessed from university IT assets.

In closing this section, we note for the reader our findings on our respondent's attitudes. We found that, on average, participants tended to rate sites they felt negatively about accessing from an institutional computer at a higher degree of proscription then they did sites they felt positively about in terms of permission. This extremity of evaluation results in clear groupings forming within the association data between the various attitude items, however while it may be expected that like attitudes about possibly similar sites may be themselves closely related, we found that knowledge of the institutional usage policy document had no association with any of the attitude items, showing a clear gap between knowledge and intent.

Habits of Site Access

It is a common thought that thought precedes action, thus attitude should precede habit. We can question, in relation to online activity, where gratification is but a click of a mouse button away, if attitude does actually precede regular action. If a user is accustomed to checking their Facebook status, will a prohibitive policy actually prevent the user from accessing Facebook.com? Considering the modern business life, do users occasionally play a game of Solitaire to release some tension from their stressful day? Policies can certainly be constructed in a fashion intended to restrict action rather than motivation, but as we have seen from the previous areas of analysis, our participants' grasp of university usage policy is rather lacking, and what knowledge they do have doesn't appear to have much of an impact on their opinion on what sites should be accessed or not via university computer assets. Indeed, if policies do not have much effect on guiding thought, can they have much of an effect on action? Perhaps usage policies are not as effective in guiding behaviour as we might wish to believe. So, to address this basic question of capability, we turn now to the final portion of data gathered in our study, and assess our participants' reported habitual usage regarding a variety of activities that could be performed using university IT assets.

Our respondents were asked to record their frequency at which they would perform ten different types of tasks involving university computer assets. The participants rated these tasks using a four-point interval scale ranging from regular access to never performing

the task. These ten activities were: social networking, computer gaming, e-commerce, the sharing of copywrited files, letting other university people use their accounts, using university computer to conduct research, accessing university services, accessing email, conducting university-related business and letting trusted, non-university people use their accounts. These ten items were chosen to reflect a range of activities that are either implicitly or explicitly allowed or banned within the university's computer usage policy document.

The frequency distributions of respondents' habitual activities are presented in Table 4a. In this table, as we so did in Table 3a, activities do not follow the numerical order assigned to them in the questionnaire; rather, they have been re-ordered to contrast the extent to which respondents are regularly performing the activity (choose "always") versus refraining from doing so (choose "never"). Again, it is obvious that the re-ordering of columns reflects a clear pattern in the responses. A supermajority of persons frequently perform several activities, ranging from 87.0% to 94.3% of the polled participants regularly checking email, conducting university business, researching facts and data and accessing university-based services. Similar sets of plurality rarely commit many of the remaining possible actions, as a range of 72.5% to 93.4% of the respondents stated they refrain from actions like letting anyone else (university member or not) use their account, playing computer games, sharing copywrited files, or even online shopping. I find this interesting because, as compared to the attitude frequencies where it was very obvious that the way our respondents rated site access permission more extremely in negative cases then in positive ones, we have the situation with the habitual actions where the two ranges are very similar, with popular actions having a slight edge in extremity as compared to unpopular ones. Granted, the popular actions are ones implicitly or explicitly allowed under the university's usage policy document, however the not all of the unpopular ones are banned within the guidelines. While sharing of copywrited files is a legal infringement of rights (and thus unethical and against the rules), and the sharing of your account at all is explicitly banned, Concordia's usage policy does permit reasonable use of the computer assets for personal activities like gaming, e-commerce and social networking, provided they do not unduly impact upon the network or other users' usage of the collective IT assets. The results for social networking participation is of definite interest to us, since interaction and communication are seemingly almost instinctual activities in human beings, and are arguably fundamental cornerstones in university life when one considers the teacher-student or student-student relationships, yet our participants recorded participating in networking via university computers at almost an equal rate in all four categories of frequency.

This pattern of participation frequencies is reflected in the matrix of Kendall's tau-b rank-order correlations reported in Table 4b, again in very similar fashion to the attitudinal data. Here, the frequency of participation in a given activity is correlated with the frequencies of participation in all the other activities. A distinct clustering of the popular activities are clearly indicated, although the apparent inclusion of social networking into this group strikes us as unusual, considering the rather flat distribution of frequency scores it attained as compared to the more popular activities. The average correlation among these actions is 0.367, indicating a somewhat dense cluster. A second, much

looser (the average correlation being only 0.242) cluster links together three of the remaining five actions, these being activities that would be generally perceived as permitted under reservation of use of the IT assets in the event of more appropriate demands of use being made. A third tight pairing (of correlation .486) exists almost completely disconnected from the other two groups, being linked fairly strongly to one item within the second group and not at all to the first set, this third set only involving actions in which a participant allows someone else to use their university account. What is apparent here is that the participants' habitual use of the institution's computer assets do appear to fall in line with requirements as laid out in the university's computer usage policy document.

Considering that our participants did not appear to have any real grasp of the contents of the usage policy document, we became curious as to whether or not knowledge had any effect on frequency of specific uses of the IT assets. Keeping in mind our results from the attitude data, we looked at a Cramer's V associations of each of the two indices, KARight and KBRight, as compared to each of the habitual values, and we were at this point not too surprised to find that no significant associations existed, implying that knowledge of the content of the institutional usage policy has practically no effect on participants' frequency of usage as performed on university IT assets.

Given that there is likely a link between attitude towards usage and the actual usage of the IT assets itself, I performed a rank-order correlation of the attitudinal and habitual data, choosing the attitude data to be the independent variable, since it is reasonable to expect motivation to precede action. We found that there were nineteen separate correlations of significant value within the eighty possible comparisons, and ranked them according to their Cramer's V value grouped by attitude variable. These correlations, as seen in Table 4c, show that there are several attitudes that have weak to strong correlations with frequencies of use for specific activities.

Conclusions

It is at this point that I regret not having assembled a representative sample to survey, as the findings in this study certainly call into question the educational value of the university's computer usage policy document. If the participants can show that their knowledge of what is allowed and what is prohibited, as specified in the usage policy document, is relatively lacking and yet they display attitudes towards what is reasonable to access on university computers and what activities should be the most commonly performed on the institution's IT assets, then it implies that the policy document has little or no direct effect on their day-to-day usage of their university's computer resources. Furthermore, if the policy document does not serve as a controlling variable to the users' computer usage, but rather that both variables are dependant on an outside set of social mores, then the use of the policy document as an motivational tool is rendered somewhat moot, leaving the computer usage policy document as part-enforcement, part-judicial tool fit to be used to clarify disputes and police behaviour by persons who do not hold themselves to this assumed set of collective social guidelines.

Bibliography

- Concordia University College of Alberta Computer Usage Document:

  http://computing.concordia.ab.ca/system/files/ComputingUsePolicy.pdf

- Policy Theory and Construction:

  Information Assurance for the Enterprise: A Roadmap to Information Security, 1st Edition, C. Schou, D. Shoemaker, ISBN: 0072255242

- Theory on Knowledge/Attitude/Habit Relationships:

  Canadian Organizational Behaviour, 6/e, Steven L. McShane, University of Western Australia, ISBN: 0070876940

- Research Design, Methodology Construction, Data Interpretation:

  Foundations of Behavioral Research: Educational and Psychological Inquiry, 1st Edition, Fred N. Kerlinger, ISBN: 0248980114

Table Appendix

Table 1:

Joint Distribution of Age and Role Responses

			Role of Respondent				
			1	**2**	**4**	**5**	**Total**
Age of Respondent	1	Count	61	10	0	4	75
		Expected Count	40.3	9.9	8.7	16.1	75.0
		% within Role	93.8%	62.5%	0%	15.4%	62.0%
	2	Count	3	6	8	15	32
		Expected Count	17.2	4.2	3.7	6.9	32.0
		% within Role	4.6%	37.5%	57.1%	57.7%	26.4%
	3	Count	1	0	6	7	14
		Expected Count	7.5	1.9	1.6	3.0	14.0
		% within Role	1.5%	0%	42.9%	26.9%	11.6%
Total		Count	65	16	14	26	121
		Expected Count	65.0	16.0	14.0	26.0	121.0
		% within Role	100.0%	100.0%	100.0%	100.0%	100.0%

Directional Measures for Joint Distribution of Age and Role

			Value	**Asymp. Std. Error[a]**	**Approx. T[b]**	**Approx. Sig.**
Nominal by Nominal	Lambda	Symmetric	0.363	0.068	4.370	0.000
		Age Dependant	0.413	0.087	3.877	0.000
		Role Dependant	0.321	0.075	3.727	0.000
	Goodman & Krustall tau	Age Dependant	0.429	0.054	-	0.000[c]
		Role Dependant	0.306	0.049	-	0.000[c]

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. *Based on the chi-square approximation.*

Table 2a:

Frequency Distribution of Knowledge of Permissive/Proscribed Activities KA]

	KA1	**KA3**	**KA2**	**KA8**	**KA6**	**KA7**	**KA5**	**KA4**
Correct	90.9	43.0	34.7	33.1	32.2	32.2	29.8	15.7
Incorrect	9.1	57.0	65.3	66.9	67.8	67.8	70.2	84.3

Table 2b:

Frequency Distribution of Knowledge of User-Based Responsibilities KB]

	KB1	KB7	KB5	KB6	KB2	KB8	KB4	KB3
Correct	89.6	80.0	77.6	63.2	54.4	36.0	23.2	5.6
Incorrect	10.4	20.0	22.4	36.8	45.6	64.0	76.8	94.4

Table 2c:

Frequency Table for Indices KARight and KBRight

		KARight	KBRight
N	Valid	121	121
	Missing	8	8
Mean		3.116	4.322
Median		3.000	4.000
Std. Deviation		1.6237	1.2859
Variance		2.637	1.654
Skewness		0.701	0.307
Kurtosis		0.156	-0.236
Minimum		1.0	2.0
Maximum		8.0	8.0

Table 2d:

Knowledge Items that have a Significant Relationship with a Person's Institutional Role

Item	Descriptor Title	Kendall's Tau-b	Gamma	Cramer's V
KA1	Appropriate Usage of Assets	0.136	0.445	NS
KA2	University Right to Inspect	0.187	0.334	NS
KA3	Password Guidelines	0.136	0.445	NS
KA5	Wireless AP Installation	0.162	0.328	NS
KA8	Software License Requirement	0.302	0.496	0.478
KB1	Ethical & Effective Use	0.154	0.491	NS
KB2	User-based Data Backups	-0.295	-0.491	0.405
KB4	Off-Campus Data Security	0.327	0.577	0.459
KB6	Loss due to Unavailability	0.297	0.548	0.353
KB8	Access Request Requirement	-0.160	-0.283	NS

-: Approximate significance level of greater than 0.100, therefore discarded.

Table 3a:

Frequency Distribution of Attitude Items [AT]

	A7	A8	A2	A3	A5	A6	A1	A4
Always	51.2	41.6	35.2	13.7	4.4	2.7	4.0	1.6
Usually Yes	26.4	32.8	23.2	17.7	1.8	2.7	1.6	1.6
Depends	26.5	23.2	23.2	33.9	26.5	17.9	11.3	6.5
Usually No	2.4	4.0	8.8	12.9	25.7	23.2	16.9	17.1
Never	8.0	7.2	9.6	21.8	41.6	53.6	66.1	73.2
Missing Cases[a]	4	4	4	5	16	17	5	6

a. Out of 129 cases.

Table 3b:

Kendall's Tau-b Bivariate Correlation of Attitude Items [AT]

A2	A7	A8	A3	A5	A6	A1	A4	
1.000	0.701	0.487	0.590	0.415	0.195	0.199[a]	0.192	Political Sites (A2)
	1.000	0.603	0.524	0.313	0.256	0.128	0.174	Religious Sites (A7)
		1.000	0.350	0.233	0.253	0.162	0.128	Social Sites (A8)
			1.000	0.490	0.310	0.313	0.339[b]	Counterculture Sites (A3)
				1.000	0.496	0.279	0.285	Proxy Sites (A5)
					1.000	0.186	0.284	Torrent Sites (A6)
						1.000	0.409	Adult Sites (A1)
							1.000	Illegal Sites (A4)

a. Significance level of 0.111.
b. Significance level of 0.116.

Table 4a:

Frequency Distribution of Habit Items [H]

	H8	H9	H6	H7	H1	H3	H4	H2	H10	H5
Always	75.8	50.0	40.2	39.0	23.2	6.5	1.7	4.8	2.4	1.7
Often	18.5	35.5	45.1	48.0	30.4	21.1	9.2	4.0	3.3	5.0
Seldom	4.8	8.1	7.4	8.1	23.2	35.0	28.6	25.8	15.4	8.3
Never	0.8	6.5	7.4	4.9	23.2	37.4	60.5	65.3	78.9	85.1
Missing Cases[a]	5	5	7	6	9	6	5	6	10	8

a. Out of 129 cases.

Table 4b:

Kendall's Tau-b Bivariate Correlation of Habit Items [H]

H9	H6	H7	H8	H4	H3	H1	H2	H10	H5	
1.00	.508	.503	.340	.185	.203	-	-	-	-	H9
	1.00	.485	.388	.225	-	.148	-	-	-	H6
		1.00	.404	.351	-	-	-	-	-	H7
			1.00	.288	.144	-	-	-	-	H8
				1.00	.221	.179	.274	-	-	H4
					1.00	.187	.279	-	-	H3
						1.00	.317	.198	-	H1
							1.00	.368	-	H2
								1.00	.486	H10
									1.00	H5

-: Approximate significance level of greater than 0.100, therefore discarded.

Table 4c:

Attitudes and Habit Items with Significant Correlation Values

Attitude Item	Habit Item	Cramer's V	Gamma	Kendall's Tau-b
Social Sites	Social Networking	0.383	-0.575	-0.430
Social Sites	Email Services	0.313	-0.067	-0.128
Social Sites	University Services	0.295	0.011	0.017
Social Sites	Research Access	0.283	-0.121	-0.179
Illegal Sites	File Sharing	0.327	-0.125	-0.241
Illegal Sites	Univ. Person Use	0.294	0.044	0.136
Illegal Sites	Gaming	0.243	-0.150	-0.292
Illegal Sites	E-Commerce	0.226	-0.099	-0.180
Torrent Sites	E-Commerce	0.316	-0.118	-0.117
Torrent Sites	Gaming	0.289	-0.223	-0.356
Torrent Sites	Univ. Person Use	0.240	0.029	0.069
Torrent Sites	Non Univ. Person Use	0.237	-0.032	-0.066
Political Sites	Research Access	0.266	-0.142	-0.204
Proxy Sites	File Sharing	0.266	-0.098	-0.152
Religious Sites	Research Access	0.248	-0.133	-0.203
Religious Sites	Social Networking	0.230	-0.283	-0.200
Adult Sites	File Sharing	0.245	-0.169	-0.294
Adult Sites	Univ. Person Use	0.230	-0.084	-0.212
Adult Sites	Non Univ. Person Use	0.227	-0.122	-0.260

All Cramer's V values have an approximate significance level of less than 0.11.