IT Ethics and the Role of Perceived Possibility of Disclosure: An Interventional Research

Dr. Alireza Bolhari, Islamic Azad University, Tehran

Dr. Alireza Bolhari holds a PhD in Information Technology Management (Business Intelligence) from Science and Research Center of Islamic Azad University; where he currently serves as a lecturer. Dr. Bolhari received his MSc in Information Technology Management from Shahid Beheshti University and has completed BSc in Industrial Engineering at Iran University of Science and Technology. His research interests are mainly focused on behavioral and organizational aspects of information technology, as well as ethical decision making.

Dr. Azadeh Bolhari, Angelo State University

Dr. Bolhari is currently an Assistant Professor of Environmental Engineering at Angelo State University. She has previously served as a lecturer at University of Colorado Denver. Dr. Bolhari hold her PhD from Colorado State University in Environmental Engineering. Her research interest include Fate and Transport of Contaminants, Environmental Justice, Water-Energy-Food Nexus and Retention of Minorities in Engineering.

IT Ethics and the Role of Perceived Possibility of Disclosure: An Interventional Research

Abstract

Since the evolution of information technology, concerns have been raised to unethical IT conducts and their significant monetary and non-monetary losses for corporations. To date, a number of endeavors have been undertaken to model individuals' IT ethical behaviors. Perceived importance of the ethical issue, ethical judgment, ethical obligation, ego strength, codes of ethics, and law are some of the influencing factors. A relatively new factor, which needs further empirical examinations, is perceived possibility of disclosure, i.e. the possibility one perceives about disclosing either the unethical behavior or its consequences to others. The objective of this research is to practically examine the influence of perceived possibility of disclosure on ethical conducts in an IT context. Accordingly, an interventional research (pre-post study) is designed and data were gathered from 347 computer stations in an IT-centric company in Iran. Due to the company's codes of ethics, six categories of unethical IT-related behaviors were defined as a) surfing social media, b) checking personal emails, c) sending organizational documents without authorized tools, d) sharing video or music files in local network, e) stockbroking, and f) installing non-job-related software on computers. Two non-simultaneous phases with duration of three months were examined. In the first phase, a total number of 906 unethical behaviors were observed by means of company-wide log-systems. Subsequently, for the second phase, every personnel were *formally* informed that their working behavior with computer stations is systematically monitored. Then, all computer stations were monitored for another three months and 155 unethical behaviors were observed. Results revealed that in comparison with the first phase, by average more than 82% of unethical behaviors were reduced. In addition, the most three reductions in unethical behaviors were stockbroking (95.91%), transmission of organizational data (91.95%), and software installation (89.51%), respectively. Finally, practical solutions to decrease the risk of unethical conducts in the domain of perceived possibility of disclosure in an IT context are discussed.

Keywords: Ethical Decision Making, Perceived Possibility of Disclosure, Computer Ethics, Big Data.

Introduction

Ethics in management and engineering has attracted a considerable number of research studies so far. The entrance of information technology (IT) into organizations and its wide range of applications have brought various challenging ethical dilemmas. This is mainly due to the four characteristics of IT as: a) immediate transactions, b) storage capabilities, c)

accessibility to data in a wide geographical scale and, d) rapid copying capability (Schultz, 2006, p. 5). This has transformed the classical privacy, piracy, and ownership notions and has attracted a wide range of research studies. A misutilization of social networks for marketing purposes, software piracy, and entering websites without permission (hacking) are all examples of today's ethical challenges (Phukan, 2005). It is shown that software piracies, computer viruses and illegal accesses to web-based services bring billions of dollars in losses (Peterson, 2002). It is estimated that in 2003 and 2004 software piracy has had more than 28 and 32 billion dollar losses, respectively, and about every ten years it doubles (Moores & Chang, 2006, p. 167).

To date, many endeavors have been put to model ethical decision making in an information technology context. To name a few, Leonard et al. (2004) empirically modeled a two-step approach to measure ethical attitude and intention. Barger (2008) believed in a case-based approach. He suggested 8 questions to help overcome any ethical dilemma. Yoon (2011) proposed a model based on five moral theories (justice, relativism, egoism, deontology, and utilitarianism). He then developed four IT ethical scenarios and empirically tested the model. Riemenschneider et al. (2011) considered attitude, subjective norm, moral judgment and perceived importance as the influencing factors of ethical behavioral intention based on the Theory of Planned Action. Renwick and Riemenschneider (2013) proposed a model of ethical decision-making among IT students and showed that moral judgment is the most important indicator of ethical intention.

The theoretical foundations of this research are based on the Theory of Perceived Possibility of Disclosure[1] presented by Bolhari et al. (2017). They argue that the possibility of conducting an unethical behavior is higher when one (an agent) perceives that other people would recognize his or her behavior with lower possibility. The following formula demonstrates the equation:

$$\mathrm{CUB} \approx f([P(PD_x)])$$

where:

CUB: Conducting Unethical Behavior

P: Possibility

PD: Perceived Disclosure of behavior x

Formula 1

To further clarify the mentioned theory, imagine Dr. Jefferson[2], a general practitioner, who works in the Ministry of Health Affairs. Since the beginning of the project he has been engaged with the business analysts team in development of a Fraud Detection System (FDS) as a "business person" to clarify system requirements. Every hospital and healthcare institutes across the country has authorized access to FDS and their daily transactions are processed online. Dr. Jefferson accidently finds out that he has an administrative access to all features

[1] or shortly "Theory of Perceived Disclosure"

[2] Name of the people or institutions in this manuscript are imaginary.

of FDS. He frequently uses admin features of the system (behavior x) to facilitate working processes and to avoid bureaucracy (Bolhari, Radfar, Alborzi, & Poorebrahimi, 2016).
Now consider the following two scenarios:

- Dr. Jefferson is highly confident ($P(PD_x) \cong 1$) that if he continues to operate with admin features of the fraud detection system, no one would find out.
- Dr. Jefferson is doubtful ($P(PD_x) \cong 0$) if others would notice him when operating with admin features of the system.

In the Theory of Perceived Disclosure, it is theorized that Dr. Jefferson's ethical behaviors would be different in either of the above cases. This statement is empirically tested in this research.

Methods

An interventional research is conducted among 347 computer stations in an IT oriented company. The main products and services of the company are software packages, information systems, data center services, security solutions, etc. in banking industry. According to the codes of ethics' documents of the company, unethical IT-related behaviors were listed through formal sessions with the managers and the supervisors. The list finally narrowed to six unethical behaviors, as follows: surfing social media, checking personal email, sending organizational documents without authorized tools, sharing files in local network, stockbroking, and installing software on computer stations.

Moreover, to undertake interventional research, two phases were defined as follows:

- Phase 1: For a three-month time period, all unethical occurrences were extracted from the company's logging system.
- Phase 2: Employees were officially re-informed about company's codes of ethics and the fact that all computer stations are remotely monitored. During this phase, a three-month data of all unethical occurrences were collected from the company's network.

To reduce the error of counting random or inevitable unethical IT-related behaviors, during each three-month period, the following cut-off points were defined in this period:

1. Surfing social media: entering social media websites for at least five times;
2. Checking personal emails: entering personal email services for at least five times;
3. Sharing files in local network: sharing video or music files for at least one time;
4. Installing software on computers: installation of any non-job-related software on computers.
5. Sending organizational documents without authorized tools: transmitting at least one document;
6. Stockbroking: entering stockbroking websites for at least 5 times;

It is worth mentioning that although a single instance of the above unethical behaviors is despicably regretful, but the notion of '*at least*' – to some extent – limits counting random or inevitable behaviors. For instance, if during a period of three months, an individual has only

checked his personal email once, this is counted as a *'sorry I did not mean that'* or *'sorry I had to find my tax payment receipt'* behavior.

Findings

Remarkable reduction in number of unethical occurrences was observed in all six categories of unethical behaviors (Table 1). Surfing social network websites, accessing personal emails and file sharing were the top three highest occurrences. Although transmission of organizational data and activity on stock exchange were in the 5th and 6th ranks, their reductions in percentage were noticeable (91.95% and 95.91%, respectively). In total, the initial 906 unethical occurrences were reduced to 155 (over 82%) over a three-month time period.

Table 1. Unethical occurrence data of pre/post monitoring intervention

No.	Unethical behavior	Number of occurrences		Reduction in occurrences	
		Before intervention	After intervention	N	%
1.	Surfing social media	263	53	210	79.84
2.	Checking personal emails	218	43	175	80.27
3.	File sharing	146	35	111	76.02
4.	Software installation	143	15	128	89.51
5.	Transmission of organizational data	87	7	80	91.95
6.	Stockbroking	49	2	47	95.91
Average		151	25.83	~125	82.91
Total		906	155	751	82.89

Discussions

In this research, a recent finding by Bolhari et al. (2017) in the context of IT ethical decision-making is further investigated through an interventional study. Their findings disclose that the intention to commit an unethical behavior is directly influenced by perceived possibility of disclosure. Accordingly, the authors conducted an interventional study to examine this influence. The results reveal that in the first phase (pre intervention), numbers of unethical behaviors were dramatically higher compared to the second phase (post intervention). In explicit words, in occasions where individuals are aware that their IT ethical behavior is monitored, they tend to behave more ethically. On the contrary, in occasions where people believe that their behaviors are not monitored, they tend to violate the ethical codes easier. The roots of this phenomenon may be underlined as follows:

- Ego strength: Ego strength is defined as "the extent that someone is capable of controlling his or her thoughts, feelings, and behaviors, and to the extent that someone is capable of dealing with anxiety" (Lake, 1985). Haines and Leonard (2007) argue the influence of ego strength on IT ethical decision making and found that people with higher ego strength are likely to behave more ethically. Since ego strength concerns

about controlling behaviors, this might be interpreted as a direct or indirect moderator of perceived disclosure.

- Self-esteem: Brockner (1988) defines self-esteem as one's beliefs about his or her mental values. Avey et. al (2010) found that leaders with lower self-esteem tend to have less ethical decisions. Similarly, it can be inferred that in those individuals with lower self-esteem, the possibility of committing unethical behaviors is higher (the first phase of the study).

Practical solutions to reduce effects of perceived possibility of disclosure might be counted as empowering by ethical trainings, redesigning the layout of the workplace as in office partitions to expand shared areas, and applying network monitoring tools. These solutions require further empirical investigations.

References

Avey, J. B., Palanski, M. E., & Walumbwa, F. O. (2010). When leadership goes unnoticed: The Moderating role of follower self-esteem on the relationship between ethical leadership and follower behavior. *Journal of Business Ethics , 98* (4), 573–582.

Barger, R. N. (2008). *Computer ethics: A case-based approach.* New York: Cambridge University Press.

Bolhari, A., Radfar, R., Alborzi, M., & Poorebrahimi, A. (2016). Ethical Decision Making in Business Intelligence: Scenario Development. *The First International Conference on New Research Achievements in Management, Accounting & Economics.* Tehran: IFIA Agent Office in IRAN.

Bolhari, A., Radfar, R., Alborzi, M., Poorebrahimi, A., & Dehghani, M. (2017). Perceived Possibility of Disclosure and Ethical Decision Making in an Information Technology Context. *Engineering, Technology & Applied Science Research , 7* (2), 1567-1574.

Brockner, J. (1988). *Self-Esteem at Work: Research, Theory and Practice.* MA: Lexington Books .

Haines, R., & Leonard, L. N. (2007). Situational influences on ethical decision-making in an IT context. *Information & Management , 44* (3), 313–320.

Lake, B. (1985). Concept of ego strength in psychotherapy. *British Journal of Psychiatry , 147* (5), 471-478.

Leonard, L. N., Cronan, T. P., & Kreie, J. (2004). What Influences IT Ethical Behavior Intentions – Planned Behavior, Reasoned Action, Perceived Importance, or Individual Characteristics? *Information & Management , 42* (1), 143-158.

Moores, T. T., & Chang, J. C.-J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *Mis Quarterly , 30* (1), 167-180.

Peterson, D. K. (2002). Computer ethics: the influence of guidelines and universal moral beliefs. *Information Technology & People , 15* (4), 346-361.

Phukan, S. (2005). Using Information Technology Ethically: New Dimensions in the Age of the Internet. *The Business Review, Cambridge , 4* (1), 234-239.

Renwick, J. S., & Riemenschneider, C. K. (2013). A model of ethical decision making by information technology students. *Journal of Computing Sciences in Colleges , 28* (5), 62-69.

Riemenschneider, C. K., Leonard, L. N., & Manly, T. S. (2011). Students' Ethical Decision-Making in an Information Technology Context: A Theory of Planned Behavior Approach. *Journal of Information Systems Education , 22* (3), 203-214.

Schultz, R. A. (2006). *Contemporary issues in ethics and information technology.* Hershey PA: IRM Press, Yurchak Printing Inc.

Yoon, C. (2011). Ethical decision-making in the Internet context: Development and test of an initial model based on moral philosophy. *Computers in Human Behavior , 27* (6), 2401-2409.