Fall 9-11-2020

The Formation of Information Security Practitioner Ethics

Jonathan Jenkins
Middle Georgia State University, jonathan.jenkins2@mga.edu

Shannon Beasley
Middle Georgia State University, shannon.beasley@mga.edu

THE FORMATION OF INFORMATION SECURITY PRACTITIONER ETHICS

Jonathan Jenkins
Middle Georgia State University
jonathan.jenkins2@mga.edu

Shannon Beasley
Middle Georgia State University
shannon.beasley@mga.edu

ABSTRACT

With the provision and consumption of services increasingly driven by software, the execution and effects of behavior occur at machine speed, the actions of a small number of people potentially impacting on many in terms of loss of privacy, cost, and in some cases even physical harm. Practitioners of information security are trained to knowledgeably employ information technologies for the manipulation of information and services. However, this same skill set poses a potential threat to many others leaving the ends to categorize the means. With the burgeoning dependence of society on information technologies, the antecedents of ethical behavior in practitioners of information security justify a corresponding increase in relevance to study. The effect of the modern, relatively earlier introduction of information technologies into life experience on the nascent development of the information technology ethical 'compass' of individuals on their path to professional work can only amplify the case for analysis.

KEYWORDS

Ethics, Organizational Culture, Information Security

INTRODUCTION

In a day and age where the average person must constantly be aware of identity theft and loss of personal information, it is not uncommon for many professionals and students to ask the question, "What is considered ethical behavior at work and at home with regards to technology?" It is a given that almost any skill or technique taught and learned to protect a group or individual from a threat can be used or exploited to harm an individual or group as well. In much the same way that anyone selling a firearm acknowledges the potential for good and evil to result from the exchange, there is an acknowledged understanding that teaching information security principles and techniques may constitute the initial training ground for tomorrow's black hat hacker (Harris, 2004).

The desire to teach the professional of tomorrow without creating the threats that they will combat at the same time is a realistic concern for many educators across academic disciplines. While this dilemma seems simple to address, it is a complicated endeavor to train individuals to recognize potential ethical problems and then shape the thought process that will allow the student to navigate away from breaches in ethics when they take action (Martinov-Bennie & Mladenovic, 2015). If an educator accepts the premise that ethical behavior can be influenced or guided by the application of learned principles, the educator must then decide where to procure the code of ethical behavior that will be taught. This process is also confounded by the nature of ethical actions. Some situations requiring ethical decision-making may also contain elements that are more significant in a decision-maker's mind than simply demonstrating ethical action.

While it is generally agreed that ethics are constantly evolving and vary greatly across geographical regions and cultures, there are many examples of ethical guidelines and frameworks that can be used to promote the development of desired behavior (Paik, Lee, & Pak, 2009). The Association of Computer Machinery (ACM) offers a code of ethics for information technology (IT) professionals that can be used to educate students, but then the question of how to indoctrinate students to produce an increase of ethical professionals becomes the question at front and center (ACM, n.d.; Martinov-Bennie & Mladenovic, 2015). The ability to sculpt education and professional programs in a way that promotes ethical decision making will satisfy the educator's desire to increase the ethical behavior within their discipline and promote an increase in ethics in the field the educator serves.

There is an exposure to both security sensitive resources and skills particular to the core work of information security practitioners which justifies adjustments to the model of how we approach understanding ethical behavior in

the workplace. The fact that the routine exercise of these skills is increasingly tied to the delivery of services, further amplifies the need for investigation of the ethical development of current and future practitioners in the field of information security. This assertion is the driving force and goal behind the creation of this research study.

LITERATURE REVIEW

There is a body of empirical research on ethical decision making which addresses the model of the decision and the ethical challenges faced by members or organizations, with the impact of many particular factors considered, and a key set of dependent variables (such as intent or motivation to act) analyzed. Other researchers have extended the body of knowledge by including additional considerations for the ability and sensitivity of practitioners to determine that ethical questions are present in the intent to act (Martinov-Bennie & Mladenovic, 2015). Additionally, ethical decisions and actions can be attributed to one or an amalgamation of actors or constructs such as an individual, a management team, an organization, or a collective concept ("the way we do things").

The ability of an individual to act ethically when faced with a dilemma is typically described as the belief structure held by the person combined with the organizational influence applied by co-workers, managers, and overall philosophy of the business as an entity. The interaction between beliefs of the individual and influence of organizational factors is further moderated by the moral intensity of the ethical dilemma in question (Miska, Stahl, & Fuchs, 2018). While the variety of factors and variables studied in prior work inform an understanding of the ethical actions of members of organizations, prior work does not sufficiently address factors that would distinguish information security practitioners, or information technology practitioners at large.

Nevertheless, findings on ethical decision-making can be applied to the unique context of work in information security with appropriate adaptation. Adapting from the importance of ethical codes to ethical behavior, a combination of the practice of sensitive skills with an absence of clear cultural climate and standards may contribute to the formation of behavioral standards which allow ethical violations. Sensitive skills, in this formulation, may include work with sensitive information or the use of tools which can pose a potential threat to confidentiality, integrity, and availability of services. In particular, to relate the information security practitioner to the general case of business employee for the study of ethical behavior, it must be noted that security practitioners possess tools and a skill set that can expand the scope of access to valuable information and increase the group of victims affected in exponential fashion.

It is generally accepted by educators in various fields that most students who study ethics within the field of study and have opportunities to practice demonstrating ethical behavior while training will become more ethical as practitioners following graduation (Mladenovic, Martinov-Bennie, & Bell, 2019). Following this assertion leads to a belief that interventions can be made by employers and educators to positively increase ethical behavior within a profession or discipline. This also contributes to promoting ethical awareness in the workplace.

A lack of pressing, immediate perceptions of harm may be related with lower moral awareness, a phenomenon which may be recognized in the "remote" nature of misuses of information security relative to the entities damaged (Reynolds, 2006). This is exacerbated by the temptation to hold revealing security breaches to protect the reputation of the organization. The proposition of immediacy can be supported by existing results demonstrating the influence of moral intensity (except possibly proximity) on moral judgment (Craft, 2012). The magnitude of direct consequences for unethical acts committed through the misuse of information security skills is characterized by a limiting factor that exists because the loss is difficult if not impossible to quantify.

The work of Rest (1986) on studying moral development provided a four-component model of ethical decision-making which identified key processes that participate in the formation of an ethical act. With an awareness of a moral issue associated with a decision (the decision may impact others), the actor may engage in a moral judgment about the propriety of a particular subset of possible options to resolve the issue. The actor is then thought to form an intention of how to proceed, and finally act on the decision even if there is no full agreement on the inclusion of intent before acting (Rest, 1986).

Moral intensity is theorized in the work of Jones (1991) to be positively related with ethical behavior and was combined with work on the model of decision-making to form an overall model which builds toward an understanding of the antecedents of ethical decisions. The construct of moral intensity is described to consist of six factors: magnitude of consequences, social consensus, probability of effect, temporal immediacy, proximity and concentration of effect. Although there have been many plausible factors identified to influence ethical decision-making, the components of moral intensity exhibiting promising prospects for the modeling of the ethicality of information security practitioners (Jones, 1991). The practice of information security, and the misuse of the skills

practiced, might be argued to represent a reduced level of moral intensity, which may open the way to a state of higher acceptance of ethical violations.

A social consensus on the morality of an unethical act is a proposed factor in the moral intensity model of decision-making. A perception that an action is ethical is then associated with ethical behavior on the part of the actor. In comparison to a general context of ethical decision-making, users of information security skills operate in a context in which a consensus may be more difficult to form, due to both a limited community of practitioners and a less clear prospect of characterization of the ethicality of action and behavior. There is not a uniform consensus for the ethicality of various key uses of information security skills, for example the practice of penetration testing, red/blue team exercises, and information security vulnerability research.

The contribution of the proximity of unethical acts carried out with the use of information security skills is a poignant question, given the clear separation of the actor from the victim. Finally, as suggested earlier, the concentration of the effect of an information security ethical violation may be diffused across an unbounded number of individuals, as represented by examples of the theft and sale of personal and financial information by criminal groups/entities.

The available work provides a set of instructive models and useful tools for the understanding of ethical behavior in an organizational environment, and further some motivating results for the importance of study of ethics in more focused applications such as accounting. However, the way is open for the exploration of useful models for the characterization of information security-bound ethical behavior and factors which influence ethics within the timeline of the development of the practitioners of this discipline.

FUTURE RESEARCH

While the recognition of the need for attention to the ethical development of information security professionals is a goal of this work, it also suggests the way forward to the exploration of particular factors which are best able to characterize factors unique to the ethical behavior of professionals in the field. The inability of any singular factor to drive the ethical behavior of information technology or information security practitioners is readily acknowledged, however the widespread penetration of information technology into services demonstrates the value of the identification of unique antecedents tied to the population subset.

Left to future work are the identification and analysis of potential models for the ethical behavior of IS practitioners, as well as the eventual evaluation of suitable models and factors via experimental measurement. The expressions of ethical behavior within the practice of information security will vary with tools and communities, however potential variables can be foreseen in reflections of readiness to take actions which harm others in the context of the practice and application of information security skills. With the benefit of experimentation, there is the hope of suggestions for intervention into the development of those training to use this unique skill set.

CONCLUSION

There is a collection of existing work to study the inner workings and antecedents of ethical behavior, with individual characteristics factoring heavily into the body of knowledge. Like many models for decision-making, ethics is best described from the culmination of factors acting on an individual at a point in time. This becomes of particular interest in the business context, when individuals in the general population hear news stories of identity theft, data loss, exposure of personal information, and other technology related criminal activity.

The available research work on ethical decision-making does not sufficiently address the unique and salient nature of information security work. However, increasing costs and risks justify attention to the antecedents of ethical behavior in individuals with skill in the use of information security principles and tools. As the development of an information security professional progresses, so does the exposure to more sophisticated security tools and potentials for misuse of the developing skill set.

An initial assessment of the factors that may productively elucidate the nature of the information security professional from an ethical point of view are their access to sensitive information out of proportion in scale to their roles, out of scale impact of violations, potential remoteness of the effect of unethical action, lack of clear definitions of what is ethical, and the ability to violate with limited accountability. Based on a study of the available findings for ethical reasoning in business and organizational contexts, the way is beckoning for investigation of the ethical behavior of information security practitioners.

A looming research question is suggested by the intensive use of information security tools and techniques which can simultaneously be applied toward concealment and ultimately as part of intentional attacks. There is an inherent capability for misrepresentation and deception in the use of tools that nevertheless serve to protect critical information for businesses and governments. The effects of the longitudinal practice of skills through these tools on decision making in ethically-sensitive situations represents an illuminating direction. Theoretical and experimental backing, as well as a workable model, for such effects will serve the growing community of organizations which seek to train and employ information security specialists while mitigating risk to all who hold a stake in their work, particularly in light of the modern insider threat.

REFERENCES

1. ACM. (n.d.). *ACM Code of Ethics and Professional Conduct*. https://www.acm.org/code-of-ethics.
2. Craft, J., L. (2012). A Review of Ethical Decision-Making Literature: 2004-2011. *Journal of business Ethics, 117,* 221-259. DOI: 10.1007/s10551-012-1518-9.
3. Harris, J. (2004). Maintaining ethical standards for a computer security curriculum. In *Proceedings of the 1st annual conference on information security curriculum development (pp. 46 – 48).* New York, NY, USA: ACM. Retrieved from http://doi.acm.org/10.1145/1059524.1059534 DOI: 10.1145/1059524.1059534.
4. Jones, T. (1991). Ethical decision-making by individuals in organizations: An issue-contingent model. *Academy of Management Review, 16(2),* 366-395. DOI:10.5465/AMR.1991.4278958.
5. Martinov-Bennie, N., & Mladenovic, R. (2015). Investigation of the impact of an ethical framework and an integrated ethics education on accounting students' ethical sensitivity and judgment. *Journal of Business Ethics, 127,* 189-203. DOI: 10.1007/s10551-013-2007-5.
6. Miska, C., Stahl, G., & Fuchs, M. (2018). The moderating role of context in determining unethical managerial behavior: A Case Survey. *Journal of Business Ethics, 153,* 793-812. DOI: 10.1007/s10551-016-3374-5.
7. Mladenovic, R., Martinov-Bennie, N., & Bell, A. (2019). Business Students' Insights into their Development of Ethical Decision-Making. *Journal of Business Ethics, 155,* 275-287. DOI: 10.1007/s10551-017-3523-3.
8. Paik, Y., Lee, M., L., & Pak, Y., S. (2019). Convergence in International business Ethics? A Comparative Study of ethical Philosophies, Thinking Style, and Ethical Decision-Making between US and Korean Managers. *Journal of Business Ethics, 156,* 839-855. DOI: 10.1007/s10551-017-3629-9.
9. Rest, J. (1986). Moral Development: Advances in research and theory. New York: Praeger.
10. Reynolds, J. (2006). Moral awareness and ethical predispositions: Investigating the role of individual differences in the recognition of moral issues. *Journal of Applied Psychology, 91(1),* 233-243. DOI: 10.1037/0021-9010.91.1.233.