3-24-2014

Development of virtue ethics based security constructs for information systems trusted workers

John M. Gray
Nova Southeastern University, jg1553@nova.edu

Gurvirender Tejay
Nova Southeastern University, tejay@nova.edu

Recommended Citation

Gray, J. M., & Tejay. G. (2014). Development of virtue ethics based security constructs for information systems trusted workers. Proceedings of the 9th International Conference on Cyber Warfare and Security (ICCWS-2014), West Lafayette, IN, USA, 256-264. doi: 10.13140/2.1.1946.4328

Development of Virtue Ethics Based Security Constructs for Information Systems Trusted Workers

John Gray and Gurvirender Tejay
Nova Southeastern University, Fort Lauderdale, USA
jg1553@nova.edu
tejay@nova.edu

Abstract: Despite an abundance of research on the problem of insider threats only limited success has been achieved in preventing trusted insiders from committing security violations. Virtue ethics may be a new approach that can be utilized to address this issue. Human factors such as moral considerations and decisions impact information system design, use, and security; consequently they affect the security posture and culture of an organization. Virtue ethics based concepts have the potential to influence and align the moral values and behavior of Information Systems workers with those of an organization in order to provide increased protection of IS assets. This study examines factors that affect and shape the ethical perspectives of individuals trusted with privileged access to personal, sensitive, and classified information. An understanding of these factors can be used by organizations to assess and influence the ethical intentions and commitment of information systems trusted workers. The overall objective of this study's research is to establish and refine validated virtue ethics based constructs which can be incorporated into theory development and testing of the proposed Information Systems security model. The expectation of the researcher is to better understand the personality and motivations of individuals who pose an insider threat by providing a conceptual analysis of character traits which influence the ethical behavior of trusted workers and ultimately Information System security.

Keywords: information system security, insider threat, virtue ethics

1. Introduction

Businesses and organizations are increasingly dependent upon Information Systems to maintain and control intellectual property, business sensitive information, and in the case of government agencies, classified information. While these systems are threatened by a variety of attackers, the greatest threat is that posed by trusted insiders, individuals who have legitimate access to the Information System (Randazzo et al. 2005). System administrators, users with access to sensitive or classified information, and Information Assurance and security personnel all hold positions of trust, have legitimate access to systems, and are tasked with protecting organizational data and Information Technology assets. Most have some degree of physical access or administrative/elevated privileges on the system. As a result these personnel pose the greatest threat to the Information System (IS) and its data (Leach 2003). Trusted workers who attack a IS understand the system security protections and typically do not arouse the suspicions of co-workers. Security violations by trusted workers who have access to organizational IS assets are a significant threat. These threats include the inadvertent loss or exposure of data and deliberate disregard for security or theft of information for personal gain or other motivations (Alfawaz, Nelson, and Mohannak, 2010).

Organizational security efforts historically focus on external threats or in response to legal or regulatory requirements and mandates (Wiant 2005). Insider threats however, those from IS workers in trusted positions, can be the most damaging and costly. Insider threats are identified as employees who have privileged access or legitimate authority to information, and who either accidentally or intentionally compromise the confidentiality, integrity, or availability of that information by abuse, illegal actions, sabotage, or unauthorized release (Colwill 2009).The significance of internal threats is becoming increasingly apparent to Information Technology executives. Managers and security professionals' state that the insider threat is what they are the most concerned with because IS workers are in trusted positions, know what data is important or sensitive, and have access as well as the technical knowledge to exploit system security controls (Greenemeier and Gaudin, 2007). Malicious actions by trusted insiders can result in serious damage to an Information System, loss or compromise of data, denial of services, or damage to the organizations reputation. Trusted IS workers account for well over 50% of computer crimes with most violations being committed by employees who have bypassed or subverted security controls. Because almost all modern organizations rely on Information Systems

to conduct operations this pervasive use means that most organizations are vulnerable to trusted insider threats.

Damage due to insider threats is not limited to employees filling technical or lower management positions. Senior Executives, by virtue of their powerful management position have the ability to effect security policy implementation and oversight. Information Systems Security managers and workers typically have the capability to affect the security posture of an Information System through their decision making authority, technical knowledge and access to make system configuration changes, or by having elevated privileges that makes sensitive data available to them. They are generally all considered to be in trusted positions and their decisions about configuration, operation, or management of the Information System can affect the systems security posture, consequently they have the capability of inflicting significant damage to the organization.

The use of IS policies, technical solutions, and access controls have proven not to be effective against trusted insiders who are motivated to compromise the system or its information (Boss et al. 2009; Dhillon 2001). Performance of malicious acts can be attributed to the ethical commitment of trusted IS workers, and preventative approaches such as technical solutions and policies will not solve these human issues. Investigation into what affects insider motivations and how their motivations can be influenced is called for in order to develop new methods of addressing the associated threats and risks.

2. An ethics based approach to information system security

In order to understand how management can influence and align the moral values and behavior of Information Systems workers with those of the organization in order to provide increased protection of IS data assets, a new approach must be considered. Pollack and Hartzel (2006) note that how individuals use information they are entrusted with is solely determined by their beliefs, ethics, and values. One of the essential factors for Information Systems Security (ISS) management is realizing that one of the dimensions of ISS is ethics (von Solms and von Solms, 2004). Eloff and Eloff (2003) note that ISS should be addressed from more than just a technical aspect; it needs to consider human issues such as culture, ethics, and training. The need for investigating the influences on the ethical decision making processes in regards to compliance with IS security policies was identified by Myyry et al. (2009). It has been shown through past ethical failures that an individual's ethical commitment will likely over-ride any organizational guidance provided through security training, directives, and policies. The implications of prior research are that an understanding of the ethical foundations of socio-organizational ISS can lead to development of ethics based normative controls.

Normative ethics examines the rightness or wrongness of the ethical actions of individuals as they relate to the moral rules of society. The three primary approaches to normative ethics are consequentialism, which focuses on the goodness or consequences of actions; deontological, which focuses on duties and rules; and virtue ethics, which focuses on character traits (Chun 2005; Shanahan and Hyman, 2003). Virtue ethics based normative controls are used to induce increased commitment from individuals by appealing to their beliefs, emotions, thoughts, and values instead of actions and consequences. They are a prescriptive approach which can be used by organizations to institute cultural change with the goal of providing benefit to the organization by shaping the actions of employees (Trevino and Weaver, 1994). Normative controls based on virtue ethics present a unique approach to the challenge of protecting Information Systems and their assets. An individual's decisions are shaped by ethics and norms; and the factors that influence decisions can be identified and therefore affected by other influencers such as leadership, training, and continual practice (Harrington 1991). Previous research concludes that moral considerations and decisions impact IS design, use, and system security; consequently they affect the security posture and culture of the organization.

Virtue ethics focuses on development of desirable character traits rather than the results of actions as a basis for a person's morality (Artz 1994). Virtues are lasting character traits which are manifested in a person's behavior and become associated with their personality (Moore 2005). Virtues help guide, motivate, and correct an individual's moral deliberations and actions and practicing virtuous acts creates a virtuous character which once formed, is no longer the outcome of the virtuous acts, but rather the cause of them. Siponen and Iivari (2006) recommend that virtue theory should influence the application of ISS and that virtue ethics can help guide the application of security policies and guidelines. Grodzinsky (1999) argues that ethical theories that are directed towards character formation and development such as virtue ethics are more applicable to IS ethics than action guided theories such as utilitarianism or deontology, both of which focus on what a moral

agent should do in a situation without requiring them to internalize ethics. Virtue ethics can help to address the changing nature of ISS because it is based on developing enduring character traits in a moral agent, the individual making the ethical choice. And while there are several forms of virtue ethics, computer ethicists generally emphasize the Aristotelian form (Stamatellos 2011).

Dunkerley and Tejay (2011) point out that technical controls have dominated research in the ISS field and that those controls focus on ensuring the confidentiality, integrity, and availability of the information system and associated data, but it is currently contended that over reliance on this perspective limits the ability to understand, manage, and ensure IS security (Dhillon and Torkzadeh, 2006). Organizations devote the largest part of ISS efforts to various security technologies and tools, but researchers argue that security cannot be achieved solely by technical controls (Dhillon, 2001; Wiant, 2005). Despite the research showing that technical controls, formal polices, and procedures alone fail to adequately protect an ISS, the number of research efforts focusing on management, social, and human concerns are few in comparison to those focusing on technical issues (Chang and Ho, 2006). Various ethics studies state that a failure to understand the human context has been the cause of many IS failures. It is recognized that increased attention must be placed on the part played by organizational culture and the human element because the primary factor in ISS is people (Wiant 2005). Non-technical activities are accepted as being a part of Information Security Management and offer an alternative to the approach of relying solely on technical solutions. ISS non-technical activities include development of policies, procedures, training, and awareness programs; and background screening of potential IS employees who will occupy trusted positions. However, Grodzinsky (1999) asserts that formal policies and procedures are meaningless if the persons they are directed at are insensitive to ethical matters and that virtue ethics is an appropriate model for the development of personal ethics and character, which in turn will carry into that individual's professional ethics. Despite the significant role of human behavior on systems and the recognized applicability of ethics to IS security, the importance of ethics has been ignored or minimalized by most practitioners and researchers. Ethics in general and especially ethics based in philosophy has very little research tradition in the field of ISS (Adam and Bull, 2008).

The relevant literature emphasizes the importance of virtue ethics and their effect on the actions of IS trusted workers and details the many factors that influence an individual's decision making, concluding that all decisions made by people are influenced and driven by ethics. Further investigation is needed to determine how the use of virtue ethics could be an effective approach to addressing ethical behaviors of IS trusted workers (Myyry et al. 2009). Individuals interpret situations based on their background and experiences', therefore ascertaining details about their ethical viewpoints is important to predicting how they may react in ethical situations.

3. Theoretical background

According to Moor (1985) a significant portion of computer ethics research is comprised of developing conceptual frameworks for understanding ethical issues involving computer technology. Adam and Bull (2008) note the need to explore alternate ethical frameworks such as virtue ethics in order to address IS issues. Whetstone (2001, 2003) determined that virtues are essential moral attributes required of organizations and people, that virtue based frameworks may be a method for management to develop the ethical culture within an organization. The potential impact of virtue ethics on the ethical behavior of trusted workers and the subsequent effect on ISS indicates a need to integrate the phenomena into a new security model.

The proposed theoretical basis for this study builds upon the previous work and theoretical frameworks of James Weber and Luciano Floridi in order to develop a new theoretical model for Information System Security trusted worker ethical behavior. Weber's research focuses on institutionalizing ethics into business organizations. According to Weber (1981, 1993) institutionalizing ethics consists of the integration of ethics formally and explicitly into the day to day work practices and decisions of organizations employees. He proposes a multi-component model for institutionalizing ethics into a business of which the component of Employee Ethics Training contributes to the desired result, specifically that of Employee Ethical Behavior.

Luciano Floridi researches the nature of Information Ethics, and determined that existing theories of ethics are inadequate to address the ethical issues involving Information Systems. Floridi (1999, 2006) describes his theory of Information Ethics (IE) as the study of moral issues that develop from information that a moral agent receives from an infosphere, defined as the environment in which information plays a significant role, such as

an Information System. The theory of Information Ethics claims that an individual's morals guide their decisions and behavior, and while Information Ethics does not address individual ethical issues themselves, its concepts can be used to develop or shape a conceptual framework which will guide moral agents to solutions for specific problems. Actions taken by a moral agent that contribute positively to the welfare of an infosphere are considered to be virtuous (Floridi 1999, 2006).

The research in this study integrates and expands on elements of Weber's (1993) Multi-component Model to Institutionalize Ethics into Business Organizations which focuses on organizational influences; and the Internal Resource Product Target Information Ethics Model presented by Floridi (1999, 2006) which considers influences and their presence or absence that effect the actions of moral agents and ultimately the security of an IS. The resulting effect of influencers on the ethicality of people, particularly trusted insiders is that despite any ethics codes, policies, procedures, or work practices implemented by an organization, the moral agent's own internal sense of ethics and morality will be the primary factors in any ethical decisions they make and will in turn affect the overall IS security posture. By recognizing these internal motivations virtue ethics can be used to influence the moral agent's evaluations, actions, and behavior.

4. ISS trusted worker ethical behavior model

In this paper, we propose the ISS TWEB Model (figure 1), which demonstrates influences on ISS trusted worker behavior within an organization. This model can be used to explore whether virtues can replace duties and mandates as a prevailing approach for achieving information system security. The TWEB Model is comprised of seven components grouped into the three categories of Virtue Ethics, Influencers, and Effects. The Virtue Ethics category is an ethical concept that emphasizes the role of moral character and virtue in the character development and personal ethics of a moral agent. This category is comprised of four ISS components, the constructs of Astuteness, Conviction, Rectitude, and Self-Discipline. These constructs are derived from the Cardinal Virtues of Prudence, Fortitude, Justice, and Temperance respectively. These virtue ethics based ISS constructs form the basis of the theoretical model that shape the ethical beliefs, character development, and personal ethics of a moral agent and ultimately results in professional ethics.

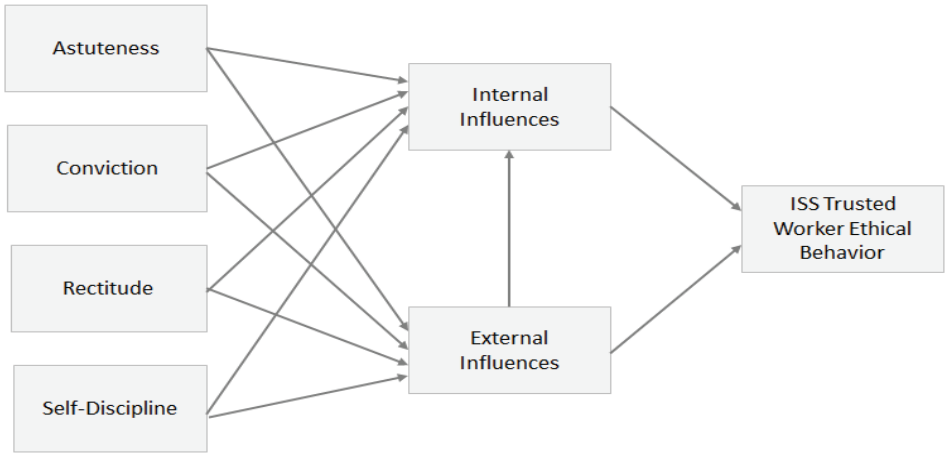

Figure 1: ISS trusted worker ethical behavior model

The Influencers category consists of environmental factors that are internal and external to the organization which exert influence on the ethical makeup, moral choices, and behavioral intentions of a moral agent. The Effects category indicates the effectiveness that the internal and external influences have on the resulting behavior of a moral agent, whom in the context of this study is defined as trusted workers with privileged access to information systems.

Prior IS research has identified the personal and professional qualities of successful IS workers which contributes positively to desired security behaviors and organizational culture. The body of knowledge was reviewed to identify behavioral and ethical characteristics of ISS trusted workers which potentially correlate to the Cardinal Virtues as defined by Aquinas (2005). Based on that review four ISS constructs rooted in virtue

ethics are proposed and it is suggested how they may influence the character development and moral choices of trusted workers. These are further discussed in next sub-sections.

4.1 Virtue ethics

A review of relevant literature identified the measures or indicators of the virtue ethics constructs of temperance, fortitude, prudence, and justice and facilitated item generation of potential measures for each of the proposed formative constructs of Astuteness, Conviction, Rectitude, and Self-Discipline and their definitions as they relate to IS security. The results are summarized in Table 1, ISS Trusted Worker Ethical Constructs.

The proposed construct of Astuteness aligns with the virtue of prudence or practical wisdom, characterized as being able to effectively deliberate and reason between actions with regard to which is appropriate at a given time. Stamatellos (2011) advocates that ethical computer behavior is comprised of morally right actions, intellectual excellence, and responsibility. Myyry et al. (2009) found that compliance with IS policies and moral behavior is determined by an employee's skills, creativity, being able to recognize or interpret situations involving moral issues, and ability to rationalize the importance of IS security policies. An individual's expertise and making impartial decisions are ethical characteristics identified by Adam and Bull (2008). Employee professional skills, knowledge, and awareness of security issues, and values impact ISS (Pahnila, Siponen, and Mahmood 2007; Alfawaz, Nelson, and Mohannak 2010; Artz 1994). Virtuous acts include being able to resolve conflicts between organizational goals and security policies according to Siponen and Iivari (2006). Employee actions should be logical and consistent, recognizing ethical issues as they pertain to ISS (Siponen 2000).

Table 1: Trusted worker ethical behavior constructs

Cardinal Virtue	IS Security Construct	Definition	Source Literature
Prudence (Practical Wisdom)	Astuteness	Skill in making assessments and in the application of professional knowledge, experience, understanding, common sense, or insight in regards to Information System security.	Stamatellos (2011); Myyry et al. (2009); Adam and Bull (2008); Pahnila, Siponen, and Mahmood, (2007); Artz, (1994); Alfawaz, Nelson, and Mohannak (2010); Siponen and Iivari (2006); Siponen (2000)
Fortitude (Courage)	Conviction	Fixed or firmly held beliefs regarding Information System security that affect decisions regarding compliance.	Stamatellos (2011); Myyry et al. (2009); Artz (1994); Alfawaz, et al. (2010)
Justice	Rectitude	Rightness/correctness of conduct and judgments that could affect Information System security.	Stamatellos (2011); Myyry et al. (2009); Adam and Bull (2008); Alfawaz, et al. (2010); Dhillon and Torkzadeh (2006)
Temperance	Self-Discipline	Willpower and control over one's personal, desires and conduct when considering actions that affect Information System security.	Stamatellos (2011); Myyry et al. (2009); Pahnila, Siponen, and Mahmood (2007); Alfawaz et al. (2010); Siponen, (2000); Dhillon and Torkzadeh, (2006)

Conviction is the proposed construct which is equivalent to the virtue of fortitude, also referred to as courage, recognized as the ability to confront fear, uncertainty, or intimidation. Alfawaz et al. (2010) maintain that understanding and willingness to comply with and enforce security policies are behaviors that contribute to ISS. Complying with ISS requirements requires character based development, personal growth and improvement, making morally correct judgments, internalizing policies, and having the courage to follow right moral actions even when placed under pressure (Stamatellos 2011; Myyry et al. 2009). Regarding computer ethics based on the virtues, Artz (1994) points out that the burden of responsible action is on the user. A user

intending to commit a violation may rationalize that committing the violation is the right choice, and sometimes it takes courage to make the ethical choice when it appears not to be beneficial to do so.

Rectitude is synonymous with the virtue of justice, which is concerned with acting fairly, responsibly, and being sensitive to the rights of others. Virtue based ISS work ethics are created by promoting loyalty, respect, and trust, particularly when safeguarding sensitive information (Dhillon and Torkzadeh, 2006). The ethical approach to using an IS includes treating coworkers, customers, and management well, and making morally fair judgments regarding security policies (Myyry et al. 2009; Adam and Bull 2008). Stamatellos (2011) states that cyber ethic morals and behavior includes feelings of caring, considerations of personal policies, social policies, and of decisions that may affect society; with the aim of the moral agent achieving good netizenship through character based morals. All of these concepts seem to appropriately align with the concept of ISS Rectitude.

Temperance, defined as individual humility, self-restraint, and control of emotions and actions is represented in ISS by the construct of Self-Discipline. Employee beliefs, habits, control or emotions, and positive attitudes promotes ethical conduct and contributes to ISS (Alfawaz et al. 2010; Pahnila et al. 2007; Siponen 2000). An individual's work ethics are positively affected by improving their morals and professionalism and contributes to security (Dhillon and Torkzadeh, 2006). Myyry et al. (2009) state that a moral agent's temptations to commit security violations are controlled by their willpower and self-discipline, which the sums up the primary concept of this proposed ISS construct.

It is contended that these four new constructs collectively form the concept of ISS Virtue Ethics and through processes internal and external to the organization exert influence on the moral character of trusted Information Systems workers. These constructs can potentially be operationalized to predict a workers future ethical behavior.

4.2 Influencers and effects

The influencer components are comprised of internal and external influences and include factors such as age, education, intrinsic beliefs, religious institutions, peers, social organizations, training, and values. An internal influence refers to any factor that is exerted from within an organization. Attempts to integrate ethics into an organization can occur through various business processes. Organizational influences are recognized as important factors in moral development and ethical decision making (Trevino 1986). Weber (1981, 1993) identifies several key organizational influences on employee ethical decision making processes including ethics training, ethical codes of conduct, existing organizational culture, and organizational enforcements such as rewards and punishment.

One approach to ethical development and change is through employee orientation and training, and organizational climate is an important factor in the moral development of an employee (Weber 1993). Organizations develop ethical codes of conduct, ethics training, and ethics policies with the expectation of them having a positive impact on the ethical behavior of employees and ethics training has been shown to be an effective method for moral development. Senior executives within an organization are a significant influence on ethical standards, and management decisions and processes ultimately manifest themselves as character traits (Weber 1981). Each of these represents processes internal to an organization that potentially influence the ethical considerations of an individual and are included in the influencer component of the TWEB Model.

Floridi (1999, 2006) concurs that influences on moral decision making can originate from within an organization but they also originate from sources external to the organization and that an all-encompassing approach to Information Ethics must take into consideration all aspects of how information is created and used, and all entities involved that may interact with a moral agent. External influences on a moral agent's personal ethical values and behavior include individual variables such as social, cultural, and ethnic background, personal idols or family members that they emulate or hold in high esteem, religion, social memberships, and personal experiences (Trevino 1986 & Whetstone 2003). These external influences affect a person's values, honesty, reliability, loyalty, and integrity and help form an individual's ethical belief system or moral philosophy which in turn affects their ethical decisions. They also influence how a person interprets and internalizes other external influences. Additionally, external influences may have an effect on how

organizational internal influences such as ethical codes of conduct are perceived, interpreted, and acted upon by a moral agent. Societal influences such as social norms, religious beliefs, laws, and an individual's upbringing are included in the external influencer category. The resulting effect of influencers on the ethicality of people is that despite any ethics codes, policies, procedures, or work practices implemented by an organization, the moral agent's own internal sense of ethics and morality will be the primary factors in any ethical decisions they make and will in turn affect the overall IS security posture. By recognizing these internal motivations virtue ethics can be used to shape the moral agent's evaluations, actions, and behavior.

When implementing an ethics based model, an organization must define what is considered ethical behavior in order to have a frame of reference for desired outcomes. Expected employee behavior should be based on the core principles of the particular ethical philosophy chosen (Weber 1993). The virtue ethics approach focuses on the character of the moral agent involved instead of a specific action. It emphasizes that the virtues which make up an individual's character will guide and determine their ethical behavior. The Effects category of the TWEB Model is the product of the trusted worker ethical evaluations and actions generated from the information influencer sources. It is important to note that the effect of influencers on the behavior of a moral agent can be positive or negative.

5. Discussion and conclusion

Information gathered from the literature review regarding virtue ethics, Information System security, security cultures in organizations, trusted workers, and failures of technical controls, policies, and procedures was considered when developing this research framework. Recognizing and understanding the qualities of virtuous character is important to an organization so that they can be identified in employees (Whetstone 2003). In the context of ISS, virtue ethics has the potential to affect trusted worker ethical behavior and ultimately system security by providing a means of identifying existing character traits as well as a methodology to follow for developing and influencing desired traits which may predict or foresee how employees will respond when presented with an ethical situation. Research to determine whether virtue ethics concepts can be effectively incorporated into those organizational efforts may contribute to development of more effective employee hiring processes, security polices, ethics training, and ethical codes of conduct.

With the understanding that trusted workers have privileged or elevated access to system information and knowledge of how to circumvent system security controls or conceal illegal actions, an ethical methodology that appeals to the internal motivations of an individual has the potential to provide more effective protection of system information. The TWEB Model presents a virtue based methodology in which to identify and determine whether the four constructs are in fact influences, investigate interrelationships between them, their effect on ethical behavior, and if they have potential to be incorporated or operationalized in a way that introduces virtue ethics explicitly and formally into organizational processes. It provides a framework to assess beliefs and to develop procedures or tests for use in evaluating what ethical characteristics potential hires or current employees have obtained through societal or other external influences, and if any of the virtue ethics qualities are part of their character makeup. The model allows us to assess whether it is feasible and effective to incorporate, either individually or collectively, the four proposed ISS constructs into the internal processes of an organization in order to positively shape, guide, and influence the ethical choices and behavior of IS trusted workers. Recommended future research includes gaining consensus on the applicability of the new ISS constructs; content validation, purification and reliability testing of their indicators; and validation of the proposed theoretical model.

Through a screening process individuals identified as having these characteristics may be considered as good hires as their ethical values align with those of the organization. A virtue profile of existing employees, particularly those in trusted positions, can be evaluated for desired character traits and provided virtue ethics based security training designed to further develop and solidify their professional ethics. As noted by Shanahan and Hyman (2003) the profiles of valued employees could be used as a baseline for comparing and identifying desired traits in potential employees. Consequently, according to Weber (1981), ethical behavior should become the organizational norm, thereby providing a foundation for success when addressing insider threats.

References

Adam, A., and Bull, C. (2008) "Exploring MacIntyre's virtue ethics in relation to information systems"' *European Conference on Information Systems (ECIS),* Galway, Ireland, pp 1-11.

Alfawaz, S., Nelson, K., and Mohannak, K. (2010) "Information security culture: A behavior compliance conceptual framework", *Proceedings of the 8th Australasian Information Security Conference (AISC 2010),* Brisbane, Australia, pp 47-55.

Aquinas, T. St. (2005) *The Cardinal Virtues: Prudence, Justice, Fortitude, and Temperance,* Hackett Publishing, Indianapolis.

Artz, J. M. (1994) "Virtue vs. utility. Alternative foundations for computer ethics", *Proceedings of the Conference on Ethics in the Computer Age,* Gatlinburg, TN, pp 16–21.

Boss, S., Kirsch, K. J., Angermeier, I., Shingler, R. A., and Boss, R. (2009) "If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security", *European Journal of Information Systems,* Vol. 8, No. 2, pp 151-164.

Chang, S., and Ho, C. B. (2006) "Organizational factors to the effectiveness of implementing security management", *Industrial Management and Data Systems,* Vol 106, No. 3, pp 345-361.

Chun, R. (2005) "Ethical character and virtue of organizations: An empirical assessment and strategic implications", *Journal of Business Ethics,* Vol. 57, No. 3, pp 269-284.

Colwill, C. (2009) "Human factors in information security: The insider threat–Who can
you trust these days?" *Information Security Technical Report*, Vol. 14, No. 4, pp 186-196.

Dhillon, G. (2001) "Violation of safeguards by trusted personnel and understanding related information security concerns", *Computers & Security,* Vol. 20, No. 2, pp 165-172.

Dhillon, G., and Torkzadeh, G. (2006) "Value-focused assessment of information systems security in organizations", *Information Systems Journal,* Vol. 16, No. 3, pp 293-314.

Dunkerley, K. D., and Tejay, G. (2011) "A confirmatory analysis of information systems security success factors", *Proceedings of the 44th Hawaii International Conference on Systems Sciences (HICSS '11), HI, USA,* pp 1-10.

Eloff, J., and Eloff, M. (2003) "Information security management – A new paradigm", *Proceedings of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2008), Wilderness, South Africa,* pp 130-136.

Floridi. L. (1999) "Information ethics: On the philosophical foundation of computer ethics", *Ethics and Information Technology,* Vol. 1, No. 1, pp 37–56.

Floridi, L. (2006) "Information ethics, its nature and scope", *Computers and Society,* Vol. 36, No. 3, pp 21-36.

Greenemeier, L., and Gaudin, S. (2007) "The threat from within – Insiders represent one of the biggest security risks because of their knowledge and access. To head them off, consider the psychology and technology behind the attacks", *Insurance & Technology*, Vol. 32, No. 2, pp 38-41.

Grodzinsky, F. (1999) "The practitioner from within: Revisiting the virtues", *Computers and Society,* Vol. 29, No. 1, pp 9-15.

Harrington, S. J. (1991) "What corporate America is teaching about ethics", *Academy of Management Executive,* Vol. 5, No. 1, pp 21-30.

Leach, J. (2003) "Improving user security behavior", *Computers & Security,* Vol. 22, No. 8, pp 685-692.

Moor, J. H. (1985) "What is computer ethics?", *Metaphilosophy,* Vol. 16, No. 4, pp 266-275.

Moore, G. (2005) "Corporate character: Modern virtue ethics and the virtuous corporation", *Business Ethics Quarterly,* Vol. 15, No. 4, pp 659-685.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009) "What levels of moral reasoning and values explain adherence to information security rules? An empirical study", *European Journal of Information Systems,* Vol. 18, No. 2, pp 126-139.

Pahnila, S., Siponen, M., and Mahmood, A. (2007) "Employee's behavior towards IS security policy compliance", *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS '07), HI, USA*, pp 1-10.

Pollack, T. A., and Hartzel, K. A. (2006) "Ethical and legal issues for the information systems professional", *Proceedings of the 2006 ASCUE Conference, Myrtle Beach, SC, USA,* pp 172-179.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. (2005) *Insider threat study: Illicit cyber activity in the banking and finance sector,* Technical Report CMU/SEI-2004-TR-021, Carnegie Mellon University, Software Engineering Institute.

Shanahan, K. J., and Hyman, M. R. (2003) "The development of a virtue ethics scale", *Journal of Business Ethics,* Vol. 42, No. 2, pp 197-208.

Siponen, M. (2000) "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security,* Vol. 8, No. 1, pp 31-41.

Siponen, M., and Iivari, J. (2006) "Six design theories for IS security policies and guidelines", *Journal of the Association for Information Systems,* Vol. 7, No. 7, pp 445-472.

Stamatellos, G. (2011) "Computer ethics and Neoplatonic virtue: A reconsideration of cyberethics in the light of Plotinus' ethical theory" *International Journal of Cyber Ethics in Education,* Vol. 1, No. 1, pp 1-11.

Trevino, L. K. (1986) "Ethical decision making in organizations: A person-situation interactionist model", *Academy of management Review*, Vol. 11, No. 3, pp 601-617.

Trevino, L. K., and Weaver, G. R. (1994) "Business ETHICS/BUSINESS ethics: One field Or two?", *Business Ethics Quarterly,* Vol. 4, No. 2, pp 113-128.

von Solms, B. (2000) "Information security – The third wave?", *Computers & Security,* Vol. 19, No. 7, pp 615-620.

von Solms, B., and von Solms, R. (2004) "The 10 deadly sins of information security Management", *Computers & Security,* Vol. 23, No. 5, pp 371-376.

Weber, J. (1981) "Institutionalizing ethics into the corporation", *MSU Business Topics,* Vol. 29, No. 2, pp 47-52.

Weber, J. (1993) "Institutionalizing ethics into business organizations: A model and research agenda", *Business Ethics Quarterly,* Vol. 3, No. 4, pp 419-436.

Whetstone, J. T. (2001) "How virtue fits within business ethics", *Journal of Business Ethics,* Vol. 33, No. 2, pp 101-114.

Whetstone, J. T. (2003) "The language of managerial excellence: Virtues as understood and applied", *Journal of Business Ethics,* Vol. 44, No. 4, pp 343-357.

Wiant, T. L. (2005) "Information security policy's impact on reporting security incidents", *Computers & Security,* Vol. 24, No. 6, pp 448-459.