Introducing virtue ethics concepts into the decision processes of information systems trusted workers: a Delphi study

John M. Gray*

Nova Southeastern University,
C/234, 610 Dowell St.,
Keyport, WA 98345, USA
Email: jg1553@mynsu.nova.edu
*Corresponding author

Gurvirender P.S. Tejay

Centre for Cyber Security Studies,
St. Thomas University,
O'Mailia Hall, Room 111,
16401 NW 37th Avenue,
Miami Gardens, Florida 33054, USA
Email: gtejay@stu.edu

Abstract: Human factors affect the incorporation and efficiency of information systems security (ISS). This study examined various factors which affect and shape the ethical perspectives and decision making processes of individuals with access to personal, sensitive, and classified information maintained in information systems. A two-round web-based Delphi survey was completed by a ten member panel of ISS subject matter experts who were convened to identify and establish the key indicators of four virtue ethics based formative constructs for ISS trusted worker decision making and conduct. Consensus was reached on the applicability of a set of indicators for each construct. The high level of agreement among panel members indicates that these constructs can be used to promote conceptual thinking about the influences and implications to the ISS culture in an organisation. The controls lay the foundation for future research as they can be incorporated into a new theoretical model of ISS trusted worker ethical behaviour.

Keywords: information system security; ISS; trusted workers; virtue ethics; Delphi study; formative construct development.

Reference to this paper should be made as follows: Gray, J.M. and Tejay, G.P.S. (2020) 'Introducing virtue ethics concepts into the decision processes of information systems trusted workers: a Delphi study', *Int. J. Information and Computer Security*, Vol. 12, No. 1, pp.1–19.

Biographical notes: John M. Gray received his PhD in Information Systems Security from the Nova Southeastern University and is employed in the US Defense Industry as an information systems security analyst. His areas of research interest include the effects of human factors on information assurance and cyber security, insider threats, and information systems ethics.

Gurvirender P.S. Tejay is a Gary Goldbloom Endowed Distinguished Chair in Cyber Security Management at the St. Thomas University, Florida. His research interests include information security, privacy and technological change. He received a PhD from the Virginia Commonwealth University. He also holds a MS in Computer Science from the University of Chicago, and MA in Economics from the University of Wisconsin – Milwaukee. He has served as co-editor for special issue on cybercrime, for *Computers and Security Journal*. He also served as the Co-Chair for Emergent Research Forum for Americas Conference on Information Systems 2015.

1 Introduction

Organisations are increasingly dependent upon information systems (IS) to maintain and control their intellectual property and business sensitive information. These systems are threatened by a variety of attackers from inside and outside the organisation. While organisational security efforts historically focus on external threats or in response to legal or regulatory requirements and mandates (Jabbour and Menascé, 2009; Wiant, 2005) the most significant threat is that posed by trusted insiders, those individuals who have legitimate access to the IS (Warkentin and Willison, 2009). Information system administrators, networking technicians, users with access to business sensitive information, and information systems security (ISS) personnel all hold positions of trust, have legitimate access to systems, and are tasked with protecting organisational data and IT assets. Most have some degree of physical access or elevated privileges on the system. Trusted workers who attack a IS understand the system security protections and typically do not arouse the suspicions of co-workers. They either accidentally or intentionally compromise the confidentiality, integrity, or availability of that information by abuse, illegal actions, sabotage, or unauthorised release (Colwill, 2009; Greitzer and Hohimer, 2011). Trusted IS workers account for well over 50% of computer crimes with most of those violations being committed by employees who have intentionally bypassed or subverted security controls. As a result these personnel, known as insider threats, pose the greatest threat to the IS and its data as their actions can be among the most damaging and costly to an organisation (Greenemeier and Gaudin, 2007; Kraemer et al., 2009).

Managers and ISS professionals' indicate that the insider threat is what they are the most concerned with because IS workers are placed in trusted positions, know what data is important or sensitive, and have access to the system as well as the technical knowledge to exploit the system's security controls (Greenemeier and Gaudin, 2007). Malicious actions by these individuals can result in serious damage to an IS, loss or compromise of data, denial of services, or damage to the organisation's reputation.

Damage due to insider threats is not limited to employees filling technical positions. By virtue of their powerful management positions senior executives have the ability to affect the implementation and oversight of security policies. Senior executives are generally all considered to be in trusted positions and any decisions they make regarding the configuration, operation, or management of an IS can affect its security. Consequently they have the capability of inflicting significant damage to the organisation even to the point of causing the failure of the company as demonstrated in the cases of Enron Corporation and WorldCom Incorporated (Sogbesan et al., 2012; Taylor, 2008).

Organisations devote the largest part of their ISS efforts to developing, implementing, and using various security technologies, controls, formal policies, and procedures; however, past research demonstrates that these methodologies alone fail to adequately protect an IS (Cowill, 2009; Dhillon, 2001; Wiant, 2005; Zeadally et al., 2012). And as almost all modern organisations rely on IS to conduct operations, their pervasive use means that most organisations are vulnerable to insider threats. The use of system security policies, technical solutions, and access controls have proven to be particularly ineffective against motivated insiders (Boss et al., 2009; D'Arcy and Hovav, 2009; Dhillon, 2001). It is also noted by Kraemer et al. (2009) that preventative approaches such as technical solutions and policies have not been effective in addressing malicious acts by IS trusted workers, and that those types of acts are attributed to the worker's ethical commitment. Investigation into what affects insider motivations, their decision making processes, and how these can be influenced is called for in order to develop new methods of addressing the associated vulnerabilities, threats, and risks.

This study represents continuing research by the authors into virtue ethics as an avenue in which to better understand the personality and motivations of individuals who pose as insider threats by providing an analysis of the character traits which influence the ethical behaviour and decision making processes of trusted workers. Focusing on ISS trusted workers, it explores the conceptualisation of various virtue ethics based human and organisational factors which may affect the security of an information system. The objective of this Delphi study was to identify the most important indicators of four proposed virtue ethics based ISS constructs. Preliminary content collected for presentation to the panellists was selected through a literature review on the topics of virtue ethics, information ethics, and information security

2 Virtue ethics as a foundation for ISS decision making

Deeper insight into ethical decision making is essential to the protection of IS from insider threats. Past ethical failures by individuals such as Robert Hanssen, Bradley Manning, and Eric Snowden, each who used their privileged access to an IS to commit security violations, demonstrates that an individual's ethical commitment will likely over-ride any organisational guidance provided through security training, directives, or policies. How individuals use the information they are entrusted with is solely determined by their beliefs, ethics, and values (Pollack and Hartzel, 2006). It has been noted that ISS should be addressed from more than just a technical aspect; it needs to consider human issues such as culture, ethics, and training (Eloff and Eloff, 2003). There is a need for investigating the influences on ethical decision making processes and their effect on compliance with IS organisational security policies and procedures (Myyry et al., 2009). The implications of research by Hu et al. (2007), Myyry et al. (2009), and Pollack and Hartzel (2006) are that an understanding of the ethical foundations of socio-organisational ISS can lead to the development of ethics based normative controls. These controls would instill employees with dispositions that result in desirable computer security decision making skills. One of the essential factors for management is to realise that one of the dimensions of ISS is ethics; therefore they must consider new approaches such as virtue ethics in order to develop an understanding of how to influence and align

the moral values and behaviour of ISS workers with those of the organisation (Von Solms and Von Solms, 2004; Whetstone, 2005).

Normative ethics is a moral philosophy which 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; Dyck and Wong, 2010; 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 or rewards and punishments. Virtue ethics focus on the development of desirable character traits to guide and motivate an individual's moral deliberations and actions (Whetstone, 2005). They are a group of personal traits and qualities that through repeated inculcation and practice become the basis of an individual's character and the cause of their future actions. They are considered a prescriptive approach which can be used by organisations to institute cultural change with the goal of providing benefit to the organisation by shaping the actions of employees (Moore, 2005a, 2005b; Trevino and Weaver, 1994). Normative controls based on virtue ethics present a unique approach to the challenge of protecting IS and their assets. Previous research concludes that moral considerations and decisions impact IS design, use, and security; consequently they affect the security posture and culture of the organisation (Colwill, 2009; D'Arcy et al., 2009; Greitzer and Hohimer, 2011). Ethics and norms can shape an individual's decisions, and the factors that influence decisions can be identified and therefore affected by other influencers such as leadership, training, and continual practice (Dyck and Wong, 2010).

It is recommended by Siponen and Iivari (2006) that virtue theory should influence the application of ISS and that virtue ethics can help guide the application of security policies and guidelines. Ethical theories that are directed towards character formation and development such as virtue ethics are more applicable to IS 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 that individual to internalise ethics (Grodzinsky, 2001). In contrast, virtue ethics can help to address the changing nature of ISS because it is based on developing enduring character traits within the individual making the ethical choice.

It is also asserted that formal policies and procedures which outline how employees should conduct themselves are meaningless if the persons they are directed at are insensitive to ethical matters; and it is advocated that virtue ethics is an appropriate model for the development of personal ethics and character that in turn will carry into an individual's professional ethics (Grodzinsky, 2001; Harris, 2008). Numerous ethics studies state that a failure to understand the human context has been the cause of many information system failures and it is recognised that increased attention must be placed on the part played by organisational culture and the human element because the primary factor in ISS is people (Colwill, 2009; Kraemer et al., 2009; Wiant, 2005). Previous research also emphasises the importance of virtue ethics and their effect on the actions of ISS professionals, and details the many factors that affect an individual's decision making. The conclusion is that all decisions made by people are influenced and driven by ethics (Stamatellos, 2011). It is also contended that virtue ethics may be an effective

approach to addressing the ethical behaviour of IS trusted workers; therefore, further research is warranted regarding the utilisation of virtue ethics concepts in ISS (Myyry et al., 2009). However, despite the significant role of human behaviour on systems and the recognised applicability of ethics to IS and their security, the importance of the effect of ethics on an individual's decision making processes has been ignored or minimalised 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).

3 Research method

This research project involved the use of the Delphi method to anonymously engage a panel of subject matter experts (SMEs) in order to reach consensus on the indicators of four proposed virtue ethics based ISS formative constructs which guide the decision making processes of IS trusted workers. The constructs under study were identified as formative through the use of decision rules as detailed by Petter et al. (2007). A formative construct assumes that indicators cause the construct; therefore the direction of the causality is from the indicator to the construct (Jarvis et al., 2003; MacKenzie et al., 2011). The indicators may or may not be correlated or have an effect on each other. They are considered formative or casual because changes in them determine the characteristics of the associated construct. The goal of this study was to generate a comprehensive list of indicators that form the four proposed constructs.

3.1 Delphi technique

The Delphi method is a group process that was developed in the 1950's by the RAND Corporation in support of a US Department of Defense (DOD) military project as a way to handle opinions when objective facts are not available, and it is considered a proven and flexible technique used in research where the knowledge about a particular subject is incomplete (Skulmoski et al., 2007; Snyder-Halpern et al., 2000; Worrell et al., 2013). The Delphi method is widely used to generate ideas and aggregate opinions and solutions via group interactions between experts, specialists, or informed advocates rather than through random population samples and has a rich tradition in IS research (Avery et al., 2005; Lummus et al., 2005; Worrell et al., 2013). Statements regarding the subject under study are prepared and distributed for evaluation; and through Delphi's iterative process information is consolidated and distilled from the judgments and inputs of the Delphi participants through a series of data collection and analysis iterations. Feedback enables the participants to modify, reaffirm, or add new information to their original opinion. The technique provides for consensus on major points and reveals minority opinions. The process stops when consensus among the participating experts has been reached.

This study solicited input on the key elements of virtue ethics based ISS constructs for ISS trusted workers – who are defined as individuals who hold elevated access privileges or who can make decisions which affect the security posture or configuration of an IS. These constructs consist of the desired ethical characteristics of trusted workers that if exercised or not, affect the security of an IS. The proposed IS security constructs were:

Astuteness	Skill in making assessments and in the application of professional knowledge, experience, understanding, common sense, or insight in regards to ISS.
Conviction	Fixed or firmly held beliefs regarding ISS that affect decisions regarding compliance.
Rectitude	Rightness/correctness of conduct and judgments that could affect ISS.
Self-discipline	Willpower and control over one's personal desires and conduct when considering actions that affect ISS.

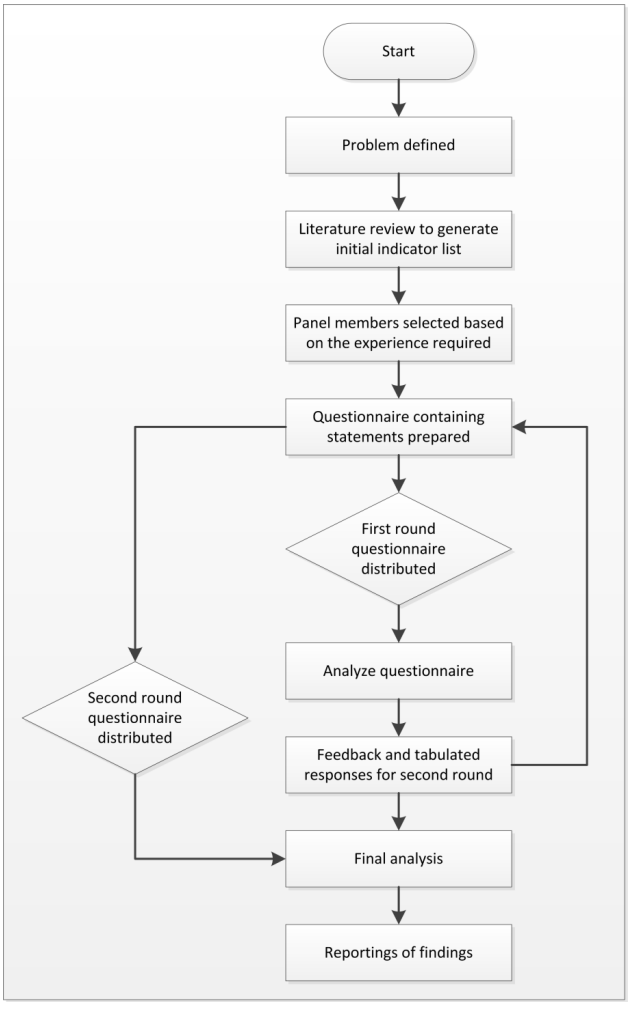
It is contended by the researchers that these four new constructs collectively form the concept of ISS virtue ethics; and through processes internal and external to the organisation they exert influence on the moral character of trusted IS workers.

While traditional Delphi studies are conducted with four rounds, the number of rounds in a Delphi study is actually variable, with two or three iterations usually being sufficient to provide consensus (Day and Bobeva, 2005; Skulmoski et al., 2007). One advantage of using a two round study is that it decreases in the time needed to collect data (Snyder-Halpern et al., 2000). In this study, in lieu of an initial Delphi round in which to generate indicators, construct conceptualisation was accomplished through a literature review of previous theoretical and empirical research. This resulted in the identification of potentially relevant construct elements or indicators as they related to virtue ethics based ISS concepts. This approach was considered valid by this study's researchers as Webster and Watson (2002) advocated that literature reviews facilitate theory development and provide a foundation for advancing knowledge. Worrell et al. (2013) also consider the use of seed data from literature reviews as common practice in Delphi studies. Petter et al. (2007) add that in the case of formative constructs, content validity is established through literature reviews as well as from the determinations of expert panels. Specifics' regarding this study's associated literature review and how the four ISS virtue ethics based constructs and their associated indicator items were derived from the four cardinal virtues of prudence, fortitude, justice, and temperance are detailed in Gray and Tejay (2014). A summary of the source literature which facilitated item generation of potential indicators for each of the proposed formative constructs of astuteness, conviction, rectitude, and self-discipline as they relate to IS security is provided in Table 1, ISS trusted worker ethical behaviour constructs.

Table 1 ISS trusted worker ethical behaviour constructs

IS security construct	*Associated cardinal virtue*	*Source literature*
Astuteness	Prudence (practical wisdom)	Stamatellos (2011), Myyry et al. (2009), Adam and Bull (2008), Pahnila et al. (2007), Artz, (1994), Alfawaz et al. (2010), Siponen and Iivari (2006) and Siponen (2000)
Conviction	Fortitude (courage)	Stamatellos (2011), Myyry et al. (2009), Artz (1994) and Alfawaz et al. (2010)
Rectitude	Justice	Stamatellos (2011), Myyry et al. (2009), Adam and Bull (2008), Alfawaz et al. (2010) and Dhillon and Torkzadeh (2006)
Self-discipline	Self-discipline	Stamatellos (2011), Myyry et al. (2009), Pahnila et al. (2007), Alfawaz et al. (2010), Siponen, (2000) and Dhillon and Torkzadeh, (2006)

Figure 1 Two round Delphi study



The construct elements identified in the literature review were subsequently used as a starting point for the Delphi panel.

Consistent with the Delphi design, for this study an anonymous electronic survey delivered via an internet website was chosen as it was considered to be less threatening to responders and would potentially increase the response rate and validity of answers. This also eliminated the long turnaround time incurred by mailing multiple surveys and waiting for their return. The survey consisted of two rounds, conducted to achieve expert

consensus on items considered relevant for the development of virtue ethics based IS security constructs and their indicators. The flow process and steps used, based on that of similar studies as noted by Avery et al. (2005), Day and Bobeva (2005), and Skulmoski et al. (2007) are illustrated in Figure 1.

4 Data collection and analysis

A critical component of the Delphi technique is the selection of survey participants as it is their expert opinions that form the basis of the survey output. Their selection is considered the most important aspect of a Delphi survey as noted by Okoli and Pawlowski (2004). There is no agreement among researchers as to what size a Delphi study panel should be, however it is suggested that the size of the panel should range from as few as 4 to more than 50 individuals with lower numbers being appropriate if the participants have a deep understanding of the subject (Hatcher and Colton, 2007; Worrell et al., 2013). According to Skulmoski et al. (2007) there are no rules on the number of panel members. Instead, factors such as whether the sample is drawn from a homogenous or heterogeneous group, the manageability of the survey because of group size, and confidence in results should play a role in determining the number of participants; with homogeneous groups requiring fewer survey participants. Goodman (1987) advocated that the Delphi group size should not be based on perceived statistical power, but instead on the group dynamics for obtaining consensus, concluding that 10–18 experts is a recommended number. Additionally, potential survey participants should not be randomly targeted, but rather identified as being either experts or informed advocates (Day and Bobeva, 2005; Skulmoski et al., 2007; Goodman, 1987).

The panel members in this study were recruited from military, civil service, and contractors at a large DOD facility located on the west coast of the USA. All participants were employed in the information technology (IT) field and were designated as members of the information assurance workforce (IAWF), which is a group of cyber-security and ISS professionals. While not considered experts in ethics, all panellists were experienced with ethical concepts as it is a part of their professional certification and organisational training programs. Panel eligibility and selection criteria included:

- employed as a member of the IAWF
- position title that reflected direct involvement with ISS in an oversight capacity
- experience with decision making
- serving in a project manager or higher level position.

Sixteen SMEs were initially identified to take part in the Delphi panel and were emailed an invitation to participate. Consent to participate was obtained from 13 of the SMEs, and ten actually participated in the study. The survey collected demographic data of the participants in order to further establish validity that they were SMEs in the field of information assurance (IA) and ISS. This was important because if the panellists can be shown to have knowledge of the topic under study then validity of their responses can be assumed (Goodman, 1987; Skulmoski et al., 2007; Worrell et al., 2013). The demographic data of the participants is shown in Table 2. Based on the demographic data the expertise level of the Delphi panel was confirmed.

Table 2 Delphi panellist demographic data

Professional characteristic	*Frequency*	*Percentage*
Employed directly in the ISS field	10	100
Professional roles:		
C-level executive	2	20
Information assurance manager/officer	6	60
IT program manager	2	20
Highest level of education:		
High school	1	10
Bachelor's degree	4	40
Master's degree	5	50
Degree major:		
Computer Engineering/Science	2	20
Information systems	4	40
Management/security	3	30
Other	1	10
N/A		
Years of IA/ISS experience:		
0–5	1	10
6–10	3	30
11–15	2	20
16+	4	40
Holds a professional computer security certification	9	90

4.1 Data collection

The survey consisted of 61 questions divided into two sections. Part one was used to gather the demographic data of the participants in order to establish the credibility and validity of their expert status. Part two of the survey instrument, which presented the security indicators, was based on quantitative research. This is important because it provides a means of making a mathematical connection between the observed data and the proposed relationships.

The survey questions were rated on a five point Likert-type scale with answers ranging from strongly agree to strongly disagree, reflecting the extent of the respondents' feelings or strength of agreement in regards to the question statement. Individual survey responses were consolidated into an average response rating to determine the group level of agreement. There was also a free text section for participants to make suggestions or comments regarding the proposed indicators, associated constructs, study, or the survey instrument.

The study's survey was delivered to selected individuals in an organisation that had an IT component which has government mandated ISS requirements. The data was collected from personnel in trusted IT positions including executives, program managers, managers, and supervisors. Each was provided a website link to access the questionnaire.

Of the 13 SMEs who were sent the survey link, ten actually completed the survey for a 77% response rate, resulting in ten usable responses. The three individuals who did not respond to the first round were excluded from the second round. Nine out of ten participants completed the second round survey for a 90% response rate. The participation rate in both rounds fell within the 70% acceptability recommended by Hasson et al. (2000) and Hatcher and Colton (2007), who also noted that use of the Delphi technique rarely achieves a 100% response rate.

The researcher's identity was known to the participants. The identity of the participants was not revealed to each other even after the completion of the final report so as to prevent individual participants from dominating the process and to encourage unreserved expressions of opinion. The goal of round one was to gain consensus on the applicability of each of the indicators which were identified in the literature review as they related to their associated virtue ethics based security construct, identify points of difference, and to suggest new indicators or construct associations if desired. The panel of experts were asked to indicate their level of agreement that the proposed indicator was valid as part of the definition of the IS security construct. They were encouraged to reflect upon their past experience when responding and if desired to provide additional input, propose new construct elements, or suggest reassignment of an indicator to another construct. Round two of the study was used to refine and obtain increased majority consensus on the indicators of the constructs.

Table 3 ISS construct indicator statements considered important

Proposed indicator: ISS security astuteness	*Round 1 agree/strongly agree percentage*	*Round 2 agree/strongly agree percentage*
Ethical computer behaviour involves intellect	80	100
Ethical computer behaviour involves right decisions	100	100
Ethical computer behaviour involves responsibility	100	100
Information system security (ISS) compliance is determined by workers making impartial decisions when designing or deploying an IS	67	89
ISS is affected by a person's practical wisdom	80	100
ISS is affected by awareness of the correct use of the IS	90	89
Employees values affect ISS compliance	70	89
Employee knowledge affects ISS compliance.	70	89
Employee skill affects ISS compliance	90	100
Consistent behaviour is needed when addressing ISS issues	90	100
Ability to resolve conflicts between policies and organisational goals is important to ISS	90	100
Recognition of ethical issues is important to ISS	80	100
Making logical and rational decisions affects ISS	90	100
Being consistent when performing security actions is important to ISS	100	89
Proposed indicator: ISS security conviction		
Computer ethics involves self-determination	80	100
Computer ethics involves right decisions	90	100

Table 3 ISS construct indicator statements considered important (continued)

Proposed indicator: ISS security astuteness	*Round 1 agree/strongly agree percentage*	*Round 2 agree/strongly agree percentage*
Computer ethics involves development of character based development, focusing on the greater good over personal desires	100	100
IS policy compliance is determined by an individual to be able to make right judgments	80	89
Individuals rationalise the ethical use of information systems	70	89
Security compliance involves clarity of actions	90	100
Proposed indicator: ISS security rectitude		
Ethical computer behaviour involves netizenship, (awareness of civic responsibility while participating on the internet)	70	88
Ethical computer behaviour involves decisions that may affect society	80	89
Ethical use of an information system is important to an organisation	100	100
Ethical use of an IS involves being sensitive to loss of Information System data	80	100
Ethical computer behaviour involves safeguarding sensitive information	90	100
Proposed indicator: ISS security self-discipline		
Ethical computer behaviour involves self-guidance	80	100
A person's attitudes and beliefs affect information system security compliance	80	100
A willingness to follow rules contributes to security compliance	100	100
Employee professionalism promotes IS security	90	100

4.2 Results

The survey instrument consisted of proposed indicators as derived from information identified in the previously accomplished literature review. Each indicator was represented by a one line Likert type scale which summarised its description. There were a total of 51 Likert items. For each item statement the panel of experts was asked to indicate their level of agreement that the item was an applicable element of the associated construct. The criterion used for determining the consensus level of agreement was in keeping with percentages used in other Delphi studies (Von der Gracht, 2012; Worrell et al., 2013). In round one, any statement receiving less than a 60% consensus rating as either agree or strongly agree was dropped and not included in round two. After calculating the average results of round one, ten proposed indicators were eliminated. The results and comments were summarised and emailed back to the participants along with the round two survey website link.

Table 4 ISS construct indicator statements considered unimportant

Proposed indicator: ISS security astuteness	*Round 1 agree/strongly agree percentage*	*Round 2 agree/strongly agree percentage*
IS policy compliance is determined by skill	60	63
IS policy compliance is determined by creativeness	40-eliminated	n/a
IS policy compliance is determined by priority for moral values over personal values	40-eliminated	n/a
IS policy compliance is determined by correctly interpreting situations as involving moral issues	60	50
IS policy compliance is determined by being motivated to act morally	50-eliminated	n/a
IS policy compliance is determined by rationalising importance of policies	60	78
Security policy compliance is determined by IS workers performing their job well	80	44
Proposed indicator: ISS security conviction		
IS policy compliance is determined by an individual's courage.	20-eliminated	n/a
IS policy compliance is determined by an individual be able to work under pressure	60	33
IS policy compliance is determined by an individual having willpower	50-eliminated	n/a
Individuals internalise policy requirements	60	33
Proposed indicator: ISS security rectitude		
Ethical computer behaviour involves a feeling of caring	50-eliminated	n/a
Ethical computer behaviour involves consideration of personal and social policies and decisions that may affect society	50-eliminated	n/a
IS policy compliance involves making fair judgments	60	78
Ethical use of an information system is part of treating workplace colleagues well	60	56
Organisational loyalty promotes security	56-eliminated	n/a
Trust and respect for co-workers promotes security	60	67
Proposed indicator: ISS security self-discipline		
Ethical computer behaviour involves moral selfhood (individuality)	60	56
Ethical computer behaviour involves being self-centred, focused on understanding and intellect	20-eliminated	n/a
Security policy compliance is determined by self-discipline	60	63
Rational acts by employees contribute to security compliance	70	78
The ability to justify actions contributes to IS security	50-eliminated	n/a

The respondents were asked to score the second round questionnaire after considering the scores and comments from other participants in round one. Consensus was defined as being reached if 80% of panel members rated the statement as either agree or strongly agree. In round two of the study 12 additional indicators were eliminated. Based on the results of the two round Delphi study, applicable indicators of the four proposed virtue ethics based ISS constructs were established as detailed in Table 3. Indicator statements that were considered unimportant and therefore eliminated are shown in Table 4.

Use of the Delphi technique capitalised on the professional experience and subject matter understanding of the participating SMEs in order to identify the key indicators of virtue ethics based security constructs by facilitating the aggregation and distillation of opinions through controlled feedback. The Delphi panel of IA and ISS SMEs reached agreement on the applicability of a set of indicators for each of the proposed constructs. Three statements; 'IS policy compliance is determined by rationalising importance of policies,' 'IS policy compliance involves making fair judgments', and 'rational acts by employees contribute to security compliance', garnered a 78% majority agreement by the panel but in keeping with the established benchmark for retention, they were eliminated. For the most part the indicators that were identified through the literature review were confirmed by the panel. Additionally, participants provided several feedback comments regarding the concept of virtue ethics as it relates to ISS, its potential effectiveness, and how it might be implemented into an organisation.

5 Discussion and conclusions

This research is the first step in empirically validating the indicators of the four proposed formative constructs for ISS based on the concept of virtue ethics. The primary purpose of the Delphi study was to identify and obtain a level of agreement on the construct elements. The panellists reached consensus on the key indicators which defined each of the proposed constructs, thereby contributing to understanding causal relationships and establishing construct validity as noted by Okoli and Pawlowski (2004).

Feedback regarding virtue ethics based ISS concepts, its potential, possible implementation, and effects were also obtained – with the viewpoints being generally positive. Some panellists expressed concerns regarding how a virtue ethics based approach to making computer security decisions might be operationalised, as well as the amount of time that would be required to achieve results. Also, while some statements questioned the effectiveness of virtue ethics against existing employees who may be insider threats; they supported the supposition that the concept could be used for pre-employment screenings of potential new hires in order to identify desirable or undesirable personality traits. This was identified in the literature review as one of its potential uses and is considered to be a preventative approach to addressing insider threats.

The narrative input received from panellists, the highlights of which are detailed in Table 5, provided a practitioner based perspective on the concepts of virtue ethics based security controls including both positive and negative aspects. Together with the information obtained regarding the applicable indicators for the proposed ISS constructs they help form a more complete picture of what the concept may consist of and its potential acceptance and use in support of ISS.

Table 5 Delphi panel comments and concerns

Delphi panellist comments
The concept of virtue ethics seems reasonable for ISS constructs…businesses require a level of trust from employees
While implementing virtue ethics based ISS constructs would require different tools and introduce unique challenges to a workplace, the results are superior in many regards over reliance solely on technical controls
It is certainly reasonable that virtue ethics would play a role in ISS…to a degree it already is a part. When individuals are granted access to an IS there is a level of trust that is placed in them
Currently virtue ethics and associated constructs play a supporting role in ISS. Virtue ethics could be used to identify those insiders that lack the ethics required for their position
Because virtue ethics cannot be taught over a short period of time, implementation would first require screening for individuals who already possess certain ethical qualities
Virtue ethics is probably the most effective control for addressing insider threats
I question whether virtue ethics could be an effective control against insider threats, however, it could be used to identify those insiders that are more likely to lack the ethics required for their position
If current policy or processes are not effective against threats, we should try virtue ethics concepts
I do not feel virtue ethics could be an effective control against addressing insider threats, IT workers are often highly introverted individuals who have rigid belief systems
Virtue ethics could be an effective control in addressing the insider threat and to prevent senior management from committing ethical violations
I do believe ISS virtue ethics can be used to develop shared sets of organisational values for senior management and other trusted workers. The medical community has done so…I think the IT industry should do the same

5.1 Limitations

Several limitations of this study were identified which may have influenced the results. The first is that even though care was taken ensure the panel composition reflected a broad range of experience, the data was collected from the professional workforce of a single organisation; therefore the findings may be specific to that organisation and not generalisable to a broader population of ISS workers, managers, and senior executives. Replicating the study in other organisations could address this potential issue. The second limitation is that the pool of SMEs who consented to participate in the study and actually completed the surveys was on the lower end of the accepted size of a Delphi panel. While the number of participants on this study's Delphi panel met the minimum generally accepted by the research community, an expansion of the size as well as the inclusion of panellists from a broader cross-section of the IA/ISS profession could potentially provide improved validity to the results. Also, including several SMEs with a stronger background in ethics may provide differing insights.

Third, while there was consensus on the applicability of the indicators for each construct, respondents were not asked to rank order the elements according to perceived importance which may have suggested which element had a stronger effect. A fourth limitation is that the concept of virtue ethics may not have been clear to some members of the Delphi panel participants. The background of the panellists was that of practitioners,

and perhaps they did not have the benefit of being familiar with the relevant research literature on the subject. Additionally, the predominant mindset of the Delphi panellists for addressing ISS issues was likely through the use of technical controls. This may have affected their consideration or acceptance of ethical concepts and solutions as a method of addressing ISS issues.

5.2 Contributions

The purpose of this study was to define the characteristics of four virtue ethics based ISS constructs by having SMEs generate a list of indicators for each. The study establishes practitioner consensus on those characteristics viewed as important and which can be explored, expanded upon, and empirically validated by both the researcher and practitioner communities. With further testing, the constructs and their associated indicators can be used to better understand influences on the decision making processes of ISS workers who, through their operation, configuration, and actions ultimately affect the security of an information system. The results also contribute to the identification of a theoretical foundation for incorporating virtue ethics concepts into the information security domain. The implications of this study are that it provides researchers with evidence that virtue ethics has the potential for application in the field of ISS, assuming that practitioners concerns can be addressed. It also provides practitioners with alternatives to technical controls, checklists, and formal procedures – which are currently accepted as being generally ineffective against determined insiders. Several of the panellists identified as senior management provided reactions and insight regarding the concepts of virtue ethics and how it may be incorporated into ISS. Their feedback regarding a virtue ethics based approach to ISS was generally positive and suggests that the concept did hold promise to be effective.

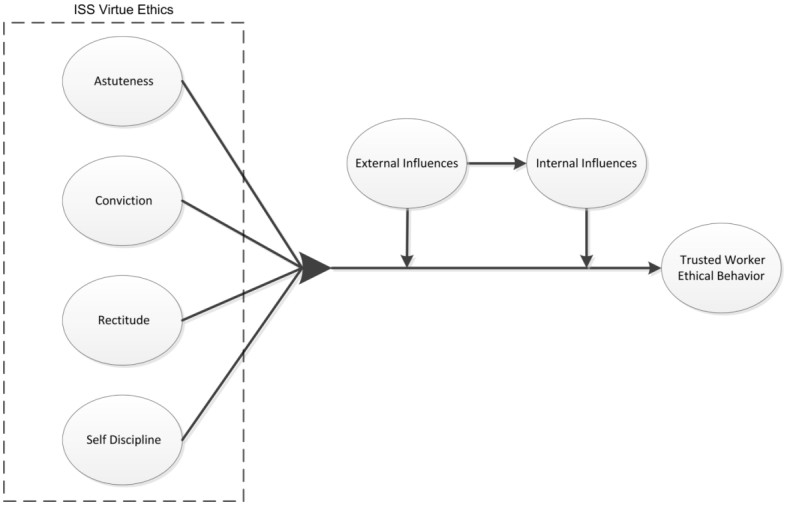
5.3 Future research

The results of the Delphi survey were used to refine the construct indicators down to the most applicable, content valid indicators of four ISS constructs. The next critical step in advancing this research is the continued refinement and validation of the indicators, analysing any empirical distinctions. After further construct indicator refinement is performed it is proposed that the constructs be incorporated into a new theoretical model which provides a framework to demonstrate the influences on trusted worker ethical behaviour. In addition to the four virtue ethics based ISS constructs, other components of the trusted worker ethical behaviour model, Figure 2, include internal organisational and external societal influences. It is advocated by this study's researchers that these internal and external influences moderate and affect the ethical makeup, behavioural intentions, and moral choices of individuals and ultimately influence employee behaviour within an organisational setting. The model's development, derived from virtue ethics principles, is further elaborated on by Gray and Tejay (2014).

Future research will be to empirically assess the relationship between the model's components and investigate their impact and contribution to improving ISS. The focus will be on identifying the factors that influence the ethical commitment of IS professionals through examination of the various components and their relationships. The model will be tested by conducting and interpreting confirmatory factor analysis and

structural equation modelling in order to determine if utilising a virtue ethics based approach to affect a moral agent's ethical decision making is valid in an ISS setting.

Figure 2 Trusted worker ethical behaviour model



6 Summary

The findings of the Delphi panel regarding virtue ethics as they are applicable to ISS present a solid initial understanding of the concepts and provide a foundation for further research into construct development and the operationalisation of virtue ethics into ISS. The expectation of the researchers in this study was to better understand the character of individuals who pose an insider threat by validating the proposed construct indicators; thereby providing a conceptual analysis of character traits which influence the ethical behaviour of trusted workers, and ultimately ISS.

The failure of the practitioner community to address IS insider threats, particularly the ethical failures of trusted workers – those individuals with privileged access who can affect an information system's security posture, indicates that solutions beyond technical controls, checklists, and formal procedures need to be explored. With the understanding that these individuals have elevated access to system information and knowledge of how to circumvent security controls or conceal illegal actions; an ethical methodology which appeals to their internal motivations may provide more effective protection of system information. An understanding of these motivations has the potential to be used by organisations to better comprehend and predict employee behaviour, develop pre-employment screening questionnaires which can identify an individual's character traits, and implement more effective ethics training for ISS workers in order to positively

influence their ethical intentions and commitment. The results of this research study suggests that virtue ethics based concepts have the potential to influence and align the moral values, behaviour, and decision making of ISS professionals and IS managers with those of an organisation in order to provide increased protection of IS assets.

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.

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.

Artz, J.M. (1994) 'Virtue vs. utility: alternative foundations for computer ethics', *Proceedings of the Conference on Ethics in the Computer Age*, Gatlinburg, TN, USA, pp.16–21, DOI: 10.1145/199544.199553.

Avery, A.J., Savelyich, B.S.P., Sheikh, A., Cantrill, J., Morris, C.J., Fernando, B., Bainbridge, M., Horsfield, P. and Teasdale, S. (2005) 'Identifying and establishing consensus on the most important safety features of GP computer systems: a Delphi study', *Informatics in Primary Care*, Vol. 13, No. 3, pp.3–11.

Boss, S.R., Kirsch, K.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009) 'If someone is watching, I'll do what I'm asked: mandatoriness, control and information security', *European Journal of Information Systems*, Vol. 18, No. 2, pp.151–164.

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, DOI: 10.1007/s10551-004-6591-2.

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, DOI: 10.1016/j.istr.2010.04.004.

D'Arcy, J. and Hovav, A. (2009) 'Does one size fit all? Examining the differential effects of IS security countermeasures', *Journal of Business Ethics*, Vol. 89, No. 1, pp.59–71, DOI: 10.1007/s10551-008-9909-7

D'Arcy, J., Hovav, A. and Galletta, D. (2009) 'User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach', *Information Systems Research*, Vol. 20, No. 1, pp.1–20, DOI: 10.1287/isre.1070.0160.

Day, J. and Bobeva, M. (2005) 'A generic toolkit for the successful management of Delphi studies', *The Electronic Journal of Business Research Methodology*, Vol. 3, No. 2, pp.103–116.

Dhillon, G. (2001) 'Violation of safeguards by trusted personnel and understanding related information security concerns', *Computers & Security*, Vol. 20, No. 2, pp.165–172, DOI: 10.1016/S0167-4048(01)00209-7.

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, DOI: 10.1111/j.1365-2575.2006.00219.x.

Dyck, B. and Wong, K. (2010) 'Corporate spiritual disciplines and the quest for organizational virtue', *Journal of Management, Spirituality & Religion*, Vol. 7, No. 1, pp.7–29, DOI: 10.1080/14766080903497565.

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 2003)*, Wilderness, South Africa, pp.130–136.

Goodman, C.M. (1987) 'The Delphi technique: a critique', *Journal of Advanced Nursing*, Vol. 12, No. 6, pp.729–734, DOI: 10.1111/j.1365-2648.1987.tb01376.x

Gray, J.M. and 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, pp.256–264, DOI: 10.13140/2.1.1946.4328.

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.

Greitzer, FL. and Hohimer, R.E. (2011) 'Modeling human behavior to anticipate insider attacks', *Journal of Strategic Security*, Vol. 4, No. 2, pp.25–48, DOI: 10.5038/1944-0472.4.2.2.

Grodzinsky, F.S. (2001) 'The practitioner from within: revisiting the virtues' in Spinello, R.A. and Tavani, HT. (Eds.): *Readings in Cyberethics*, pp.580–592, Jones and Bartlett, Sudbury, MA.

Harris, C.E. (2008) 'The good engineer: giving virtue its due in engineering ethics', *Science and Engineering Ethics*, Vol. 14, No. 2, pp.153–164, DOI: 10.1007/s11948-008-9068-3.

Hasson, F., Keeney, S. and McKenna, H. (2000) 'Research guidelines for the Delphi survey technique', *Journal of Advanced Nursing*, Vol. 32, No. 4, pp.1008–1015.

Hatcher, T. and Colton, S. (2007) 'Using the internet to improve HRD research', *Journal of European Industrial Training*, Vol. 31, No. 7, pp.570–587.

Hu, Q., Hart, P. and Cooke, D. (2007) 'The role of external and internal influences on information systems security – a neo-institutional perspective', *Journal of Strategic Information Systems*, Vol. 16, No 2, pp.153–172, DOI: 10.1016/j.jsis.2007.05.004.

Jabbour, G. and Menascé, D. (2009) 'The insider threat security architecture: a framework for an integrated, inseparable and uninterrupted self-protection mechanism', *Proceedings of the 12th IEEE International Conference on Computational Science and Engineering (CSE'09)*, Vancouver, Canada, pp.244–251, DOI: 10.1109/CSE.2009.278.

Jarvis, C.B., MacKenzie, S.B. and Podsakoff, P.M. (2003) 'A critical review of construct indicators and measurement model misspecification in marketing and consumer research', *Journal of Consumer Research*, Vol. 30, No. 2, pp.199–218, DOI: 10.1086/376806.

Kraemer, S., Carayon, P. and Clem, J. (2009) 'Human and organizational factors in computer and information security: pathways to vulnerabilities', *Computers & Security*, Vol. 28, No. 7, pp.509–520, DOI: 10.1016/j.cose.2009.04.006.

Lummus, R.R., Vokurka, R.J. and Duclos, L.K. (2005) 'Delphi study on supply chain flexibility', *International Journal of Production Research*, Vol. 43, No. 13, pp.2687–2708, DOI: 10.1080/00207540500056102.

MacKenzie, S.B., Podsakoff, P.M. and Podsakoff, N.P. (2011) 'Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques', *MIS Quarterly*, Vol. 35, No. 2, pp.293–334.

Moore, G. (2005a) 'Humanizing business: a modern virtue ethics approach', *Business Ethics Quarterly*, Vol. 15, No. 2, pp.237–255, DOI: 10.5840/beq200515212.

Moore, G. (2005b) 'Corporate character: modern virtue ethics and the virtuous corporation', *Business Ethics Quarterly*, Vol. 15, No. 4, pp.659–685, DOI: 10.5840/beq200515446.

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, DOI: 10.1057/ejis.2009.10.

Okoli, C. and Pawlowski, S.D. (2004) 'The Delphi method as a research tool: an example, design considerations and applications', *Information & Management*, Vol. 42, No. 1, pp.15–29.

Pahnila, S. and 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, DOI: 10.1109/HICSS.2007.206.

Petter, S., Straub, D. and Rai, A. (2007) 'Specifying formative constructs in information systems research', *MIS Quarterly*, Vol. 31, No. 4, pp.623–656.

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.

Shanahan, K.J. and Hyman, M.R. (2003) 'The development of a virtue ethics scale', *Journal of Business Ethics*, Vol. 42, No. 2, pp.197–20, DOI: 10.1023/A:1021914218659.

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.

Siponen, M.T. (2000) 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security*, Vol. 8, No. 1, pp.31–41, DOI: 10.1108 /09685220010371394.

Skulmoski, G. J., Hartman, F. T. and Krahn, J. (2007) 'The Delphi method for graduate research', *Journal of Information Technology Education*, Vol. 6, pp.1–21.

Snyder-Halpern, R., Thompson, C.B. and Schaffer, J. (2000) 'Comparison of mailed vs. internet applications of the Delphi technique in clinical informatics research', *Proceedings of the American Medical Informatics Association, (AMIA) Annual Symposium*, pp.809–813.

Sogbesan, A., Ibidapo, A., Zavarsky, P., Ruhl, R. and Lindskog, D. (2012) 'Collusion threat profile analysis: review and analysis of MERIT model', *Proceedings of the World Congress on Internet Security, (WorldCIS-2012)*, Ontario, Canada, pp.212–217.

Stamatellos, G. (2011) 'Virtue, privacy and self-determination: a Plotinian approach to the problem of information privacy', *International Journal of Cyber Ethics in Education*, Vol. 1, No. 4, pp.35–41, DOI: 10.4018/ijcee.2011100104.

Taylor, P. (2008) 'Insider threat-The fraud that puts companies at risk', *Information Systems Control Journal*, Vol. 1, pp.46–47.

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, DOI: 10.2307/3857484.

Von der Gracht, H.A. (2012) 'Consensus measurement in Delphi studies: review and implications for future quality assurance', *Technological Forecasting and Social Change*, Vol. 79, No. 8, pp.1525–1536, DOI:10.1016/j.techfore.2012.04.013.

Von Solms, B. and Von Solms, R. (2004) 'The 10 deadly sins of information security management', *Computers & Security*, Vol. 23, No. 5, pp371–376, DOI: 10.1016/ j.cose.2004.05.002.

Warkentin, M. and Willison, R. (2009) 'Behavioral and policy issues in information systems security: the insider threat', *European Journal of Information Systems*, Vol. 18, No. 2, pp.101–105, DOI: 10.1057/ejis.2009.12.

Webster, J. and Watson, R.T. (2002) 'Analyzing the past to prepare for the future: writing a literature review', *MIS Quarterly*, Vol. 26, No. 2, pp.xiii–xxiii.

Whetstone, J.T. (2005) 'A framework for organizational virtue: the interrelationship of mission, culture and leadership', *Business Ethics: A European Review*, Vol. 14, No. 4, pp.367–378, DOI: 10.1111/j.1467-8608.2005.00418.x.

Wiant, T.L. (2005) 'Information security policy's impact on reporting security incidents', *Computers & Security*, Vol. 24, No. 6, pp.448–459, DOI: 10.1016/j.cose.2005.03.008.

Worrell, J.L., Di Gangi, P.M. and Bush, A.A. (2013) 'Exploring the use of the Delphi method in accounting information systems research', *International Journal of Accounting Information Systems*, Vol. 14, No. 3, pp.193–208, DOI: 10.1016/j.accinf.2012.03.003.

Zeadally, S., Yu, B., Jeong, D.H. and Liang, L. (2012) 'Detecting insider threats: solutions and trends', *Information Security Journal: A Global Perspective*, Vol. 21, No. 4, pp.183–192, DOI: 10.1080/19393555.2011.654318.