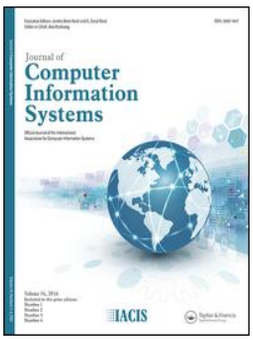

Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: http://www.tandfonline.com/loi/ucis20

Identifying Traits and Values of Top-Performing Information Security Personnel

Jordan Shropshire & Art Gowan

To cite this article: Jordan Shropshire & Art Gowan (2017) Identifying Traits and Values of Top-Performing Information Security Personnel, Journal of Computer Information Systems, 57:3, 258-268, DOI: 10.1080/08874417.2016.1184026

To link to this article: http://dx.doi.org/10.1080/08874417.2016.1184026

JOURNAL OF COMPUTER INFORMATION SYSTEMS
2017, VOL. 57, NO. 3, 258–268
http://dx.doi.org/10.1080/08874417.2016.1184026

Taylor & Francis
Taylor & Francis Group

Identifying Traits and Values of Top-Performing Information Security Personnel

Jordan Shropshire[a] and Art Gowan[b]

[a]University of South Alabama, Mobile, AL, USA; [b]James Madison University, Harrisonburg, VA, USA

ABSTRACT

Enterprise information security is a talent-centric proposition. Information assurance is a product of the combined expertise, attention-to-detail, and creativity of an information security team. A competitive edge can be obtained by hiring the top information security professionals. Therefore, identifying the right people is a mission-critical task. To assist in the candidate selection process, this research analyzes the enduring traits and values of top security performers. It identifies the personality traits and values which distinguish high-performing information security workers. In a laboratory study, a series of simulations were administered to 61 subjects to assess their ability to solve various information security problems. The characteristics of top information security performers were contrasted against the rest of the cohort. In terms of personality, the top performers have higher levels of conscientiousness and openness. With respect to values, the top performers have stronger theoretical and economic values.

KEYWORDS

Information security; personality; personnel selection; values

Introduction

Information security professionals are a critical talent group with disproportionate influence on global economic activities [1]. A team of information security professionals who proactively secure information resources and respond to incidents provides a decisive business advantage. News of major enterprise security breaches continues to make headlines [2]. The cost of a major data breach can figure in tens of millions of dollars [3]. In a recent survey of CEOs of Fortune 500 companies, cyber security ranked as the fifth most issue for executives. Attracting and hiring the best candidates for information security positions is a primary concern among chief information security officers, human resources executives, and senior managers.

As they build their information security capabilities, firms are taking a slower, more deliberate approach to hiring. Companies are not just settling for workers who are qualified, they are after individuals who stand out in ability and temperament [4]. They are seeking the best information security professionals from pools of qualified applicants. However, differentiating between good and excellent candidates remains a challenge. Human resource professionals and hiring managers have little objective data which can be used to compare candidates for information security positions. This study contends that pre-hire assessments of personality and workplace values could fill this gap and provide a valid, reliable addition to other techniques.

Currently, little is known about the characteristics of personality and values constructs as IT security performance predictors. Further, the extant literature contains little empirical evidence to suggest that it is possible to differentiate between skill levels at a highly granular level. Therefore, the present study uses personality traits and value attributes to distinguish excellent from good information security performers. To recreate the challenges that hiring managers are now facing, a sample consisting of subjects with IT work experience and information security training is compiled. The subjects complete personality and values assessments. The top information performers are identified by comparing subjects' performance across a battery of information security tasks. The tasks involve complex activities such as vulnerability analysis and system hardening.

Personality is assessed using a condensed measure of the Five Factor Model (FFM) of personality [5]. The FFM conceptualizes personality as consisting of five broad, global dimensions. Since the 1990s, a number of meta-analytic reviews have shown that the FFM personality dimensions are useful predictors of job performance [7]. Values are conceptualized using a six-factor model of values called the Study of Values (SOV) model. The SOV model has long been used to predict performance-related outcomes in a variety of fields [6, 7]. As a well-established measure [15], the SOV assessment used in this study has updated syntax and terminology [35].

The results of this research provide useful indicators of top information security performers. Organizations seeking to hire information security professionals can use this information to inform their hiring process and seek out candidates that will provide the best value over the long run. The remainder of this manuscript is organized as follows: The following section provides background on personality and values. The next section conceptualizes the hypotheses. For testing, the Methods section covers the subjects, measures, and procedures, followed by a section of the analysis and then results. The results are discussed in terms of the research hypotheses. The next section provides implications for research and practice. The last section provides concluding comments.

CONTACT Jordan Shropshire jshropshire@southalabama.edu University of Alabama, Shelby Hall, Room 1115, 150 Jaguar Drive, Mobile, AL 36688-7274, USA.
Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/ucis.

Background

Most organizations use a multiple-hurdle selection process for hiring. The purpose of this multi-stage procedure is to develop a final pool of qualified candidates from which a final selection is made. Applicants are subjected to a series of tests, interviews, and checks to assess their eligibility for a particular position. Failure at any step excludes the candidate from further consideration [8]. This approach is both time and resource efficient in that it eliminates unqualified candidates early in the selection process.

Distinguishing great from good applicants remains a challenge. One solution is to include values and personality assessments in the multiple-hurdle selection process [9]. Estimates of marginal utility associated with the use of valid assessments in personnel selection approaches have been modeled extensively [10]. It is believed that the inclusion of a late-stage assessments increases the validity of the selection process [11]. Carlson et al. [9] also called for the selection of highly validated instruments to be used in multiple-hurdle selection. Therefore, this study proposes the inclusion of validated personality and values assessments as a tool for distinguishing top information security performers from other qualified applicants.

Personality

Of the many characteristics of employees, personality has long ranked among the most considered [6]. Personality's appeal is based on the long-term applicability of its constructs. Compared with attitudes and emotions, personality traits are considered to be enduring psychological features. They are slow to change [12]. Thus, they are often used for predicting individual temperament, disposition, and future work performance. Despite these benefits, personality is an understudied concept in the information systems field.

As depicted in Appendix A, personality is infrequently used to predict human behavior in studies involving information systems or technology. When it is used, it is generally included in technology adoption studies. Thus far, personality has only been used in two studies in which the goal is to predict performance of IT-related tasks. In a 1992 study, the personality variable *locus of control* was included in a model for predicting performance at software development [13]. In a second study, a personality assessment was used to predict performance at database querying [14]. For a majority of the studies listed in Appendix A, the performance variable was measured using subjects' self-reports of their own behavior. As indicated in other research, individuals tend to report their own performance more favorably, skewing survey results. The present study fills in the gap by using personality to predict performance of IT realistic tasks using objective performance measures.

The FFM model is commonly measured using personality questionnaires. There are five broad dimensions of personality traits [15]: conscientiousness, openness, extraversion, agreeableness, and neuroticism. Together, these traits provide comprehensive framework of non-overlapping elements called the FFM. The five personality dimensions have been independently confirmed by several sets of researchers in the decades following their development.

The first dimension is conscientiousness. This is a tendency to show self-discipline, act dutifully, and aim for achievement against common measures of social conformity [5]. Conscientiousness is often considered a general predictor of job performance, while the other big five traits predict job performance in specific fields [16]. It is related to things such as achievement, perseverance, organization, and responsibility [17]. It governs the way in which people control, regulate, and direct their impulses.

The second personality dimension is openness. This is a general appreciation for creative works, emotion, adventure, new ideas, imagination, and variety of experience [18]. Those who are open to experience are intellectually curious, receptive to emotion, sensitive to aesthetics, and willing to try new things. One study found that there is a connection between politically liberal worldviews and openness to experience, however this finding has not been confirmed by other researchers [19].

The third dimension is extraversion. Extraverts enjoy talking, interacting with others, and are high in energy. They are the life of the party, enjoy being the center of attention, feel comfortable around people, easily start conversation, and like to mingle at parties. Extraverts often excel at sales, marketing, and communication positions [20]. Individuals high in extraversion prefer to do more things with more people than focus deeply on one thing. It includes traits such as sociability, activity, assertiveness, and positive emotionality. Extraversion is often associated with leadership behavior.

The fourth dimension is agreeableness. This dimension indicates a disposition to help others. It is another interpersonal construct. It reflects a general concern for social harmony. Agreeable individuals value group cohesion and getting along with others [19]. They are considered kind, generous, considerate, trusting, helpful, and willing to compromise in their interests. Agreeableness was been found to predict transformational leadership skills, good teamwork, and pro-social behavior [17].

The fifth dimension is neuroticism. This trait is characterized by a tendency to experience negative emotions such as anger, anxiety, vulnerability, and depression [21]. It may also be called emotional instability. This dimension tends to be viewed negatively and is associated with worry, self-pity, self-consciousness, emotional outbursts, and vulnerabilities. Those who score high in neuroticism are emotionally reactive and vulnerable to stress [5].

Workplace values

Values are broad long-term individual preferences concerning appropriate courses of action, behaviors, or outcomes. They provide an internal reference for guiding decision making. The link between workplace values and employee performance has been regularly confirmed over the past 70 years [7]. Values are desirable antecedents because they are relatively static over long periods of time. This stability increases their accuracy in long-term predictors. Surprisingly, the link

between values and performance is underexplored in the information systems field. Appendix B presents a listing of five studies which integrate some concept of values with information technology. Among these, only one study compared worker values with performance of an IT-related task [13]. As a result, little is known about the relationship between worker values and performance of IT work. The present study fills this gap by focusing on the values of top information security performers.

Although numerous models of values have been developed over the years, most trace back to a model called the SOV model [22]. The SOV model holds that the essence of a person is best captured by understanding the individual's value-philosophy. It purports six types of values: theoretical, economic, aesthetic, social, political, and religious [23]. Operationally, these six values are measured using a forced choice among pairs and quartets of choices. The values are presented in scenarios which are meant to represent core human experiences like choosing spouses and careers. This measure of human condition is valuable because of its relative permanence. People are slow to change their values. An employee's value attributes will remain consistent over a longer time period than less permanent attributes such as emotions and attitudes [24].

The first of the six values in the SOV model is theoretical. It is defined as an interest in the discovery of truth through reasoning and systematic thinking. The theoretical person is primarily interested in cognitive pursuits. Those who value truth above all make excellent researchers, scientists, analysts, and healthcare providers [25]. The second value is economic. It is classified as an interest in usefulness and practicality. It includes the accumulation of wealth. The economic person is most focused on that which has utility. These persons are practical and are often successful at business [26]. The third value is aesthetic. It derives from interest in beauty, form, and artistic harmony. The aesthetic person places highest value on form and harmony. These persons believe life is a series of events that are to be enjoyed for their own sake [27].

The fourth value is social. It is described as an interest in people and human relationships. The social person seeks love and most values relationships with other people. Individual with social values are strong teammates. They are willing to sacrifice to ensure the success of the organization or the group [28]. The fifth value is political. It is defined as an interest in gaining power and influencing other people. The political person's dominant drive is power. These individuals excel at convincing others to act or behave in such a way that supports their own motives [7]. The sixth value is religious. It is conceptualized as an interest in unity and understanding the cosmos as a whole. Religious persons place the highest value on unity. They seek to understand and experience the world as a unified whole.

Hypothesis development

Given that the purpose of this research is to identify the defining characteristics of top performing information security personnel, this section proffers a series of hypotheses driven by findings in previous studies. With respect to personality, it is predicted that the top information security workers will have higher levels of conscientiousness, agreeableness, and openness and lower levels of extraversion and neuroticism. In terms of values, the top information security performers are presumed to place greater emphasis on theoretical and economic values. Each hypothesis below is preceded with a critical argument and explanation of its importance in the information security domain.

In general, high levels of conscientiousness are associated with better on-the-job performance. Conscientious employees have greater attention to deal, do not accept substandard work, and rarely overlook or ignore errors [29]. These attributes are critical for information security professionals, who operated in a detail-oriented field [30]. These workers must consider a multitude of technical specifications when making decisions. A conscientious information security professional will check and confirm facts before modifying systems and settings. Thus,

H1: The top information security performers will have higher levels of conscientiousness.

Beyond conscientiousness, it is expected that top performers will also report higher levels of openness. People who are open to new experience are generally more creative, imaginative, and willing to think outside the box [20]. These are important traits for information security professionals because they must think like hackers in order to anticipate potential attacks. System weaknesses are often observed by testing and manipulating variables such communication streams, files, data, and packets [1]. Information security professionals must not only understand the inner workings of their respective systems but also be able to view them through the lens of a hacker [31]. Therefore, the following hypothesis is offered:

H2: The top information security performers will have higher levels of openness.

Extraversion has previously been used to predict performance of jobs requiring social interaction, such as sales and management. Those who find energy in interacting with others report higher levels of extraversion. This contributes to the performance of communication-oriented work. Extraversion is not expected to contribute to the performance of work which requires high degrees of concentration. For instance, extraversion is inversely related to performance at engineering and technical work [32]. Research has shown that top performing engineers are generally more introverted, and prefer to focus in depth on one project task at a time [33]. They carefully reflect on problems before taking action. It is expected that top information security professionals will share the same characteristics, since their work is similar in nature. Thus, the following hypothesis is offered:

H3: The top information security performers will have lower levels of extraversion.

Those who are high in agreeableness are good natured, flexible, cooperative, tolerant, and caring. Previous research has found that

agreeableness improves the performance of individuals who work on teams [5]. These people need to interact with others and create favorable impressions in order to excel at their work. This holds true for people in management and sales positions. Individuals high in agreeableness are usually liked; they tend to receive more attention and mentoring from experienced coworkers [7]. Thus, agreeableness generally translates into increased performance. To date, there is inconsistent evidence that agreeableness has any impact on performance of technical work. One study detected a significant correlation between agreeableness and performance among 230 engineers [34]. Therefore, it is assumed that this dynamic will apply to the field of information security. Accordingly, we suggest the following:

H4: The top information security performers will have higher levels of agreeableness.

Individuals higher in neuroticism are more likely to become distracted by a factor such as stress. This has generally been found to decrease factors related to task performance (e.g., time required to complete task, output quality, slower reaction time, etc.) [35]. In at least one study it was determined that lower levels of neuroticism improve the performance of technical work [36]. Based on this evidence, another hypothesis is given:

H5: The top information security performers will have lower levels of neuroticism.

In terms of work values, it is assumed that the top information security professionals place a greater emphasis on theoretical ideals. Previous research suggests that this group will be interested in the pursuit of truth. Their cognitive interests will lead to experimentation, testing, learning, and new perspectives on system vulnerabilities [23]. These are important qualities for information security professionals, because they lead to the identification of zero-day threats and previously unidentified vulnerabilities [16]. Thus, the following hypothesis is proposed:

H6: The top information security performers will place greater emphasis on theoretical values.

Further, this research holds that the top information security performers will place greater emphasis on economic values. An information security analyst may spend multiple days or even weeks auditing new software for potentially exploitable weaknesses [25]. It becomes easy to lose track of the main goals and pursue less critical or non-essential endeavors. Previous studies report that analysts and researchers who focus on abstract goals for long periods of time are motivated by extrinsic factors [29]. Therefore, the following hypothesis is presented:

H7: The top information security performers will place greater emphasis on economic values.

Although social values have long been used in consumer research, their impact on sales and management is subject to increasing attention. In a national survey of industrial salespeople, it was determined that an orientation to social values correlated with increased sales figures [37]. These individuals are oriented toward interpersonal interactions. They associate a high level of public esteem with work success. This increases their willingness to reach out to strangers and ask for new business [38]. While social values may increase the performance of salespersons and managers, they may actually be detrimental to workers who need to focus for long periods of time [23]. It is proffered that information security professionals must rank other factors over social values in order to focus on problem solving. This is summarized in the following hypothesis:

H8: The top information security performers will place less emphasis on social values.

Workers with high political values seek power. They want to control their surroundings and influence others. This value has been associated with task performance in a limited number of tests [39]. Often, it is associated with the personality attribute extraversion. Individuals with a high degree of political values are good at sales and management because they can convince others to act or behave in desirable ways [27]. This value has not been associated with success in engineering or any other technical disciplines. In one study, it was even assumed that political values may distract certain workers from achieving goals set by management [40]. It is therefore expected that top performers will have lower levels of political interest. Based on this evidence, another hypothesis is suggested:

H9: The top information security performers will place less emphasis on political values.

Those who place a premium on aesthetic values prefer balance, beauty, and tranquility. This value has not received much attention in studies of employee performance. In at least one case, it was not found to be significantly related to job performance [41]. The satisfaction received from successfully preventing a data breach cannot easily be construed as an aesthetic victory. Even if the definition of aesthetic values is expanded to include fulfilling experiences, top performers could not be expected to have higher levels than regular workers. These points lead to the following hypothesis:

H10: The top information security performers will place less emphasis on aesthetic values.

Religious workers place a high degree of value on unity. They seek a holistic understanding of their surroundings [42]. They are motivated by tasks which confirm their interpretation of their environment and are troubled by events which result in cognitive dissonance [43]. A major part of information security is seeking out imbalances and creating new controls. It requires workers to operate within the confines of task and information compartmentalization. These conditions are expected to trouble those who embrace religion as a primary value. Accordingly, we suggest a final hypothesis:

H11: The top information security performers will place less emphasis on religious values.

Methods

In order to evaluate the proposed hypotheses, a laboratory style test was performed. The purpose of the test was to identify the top performers in a cohort of information security workers and allow for a comparison of top performers' personality traits and workplace values against those who do not perform as well.

Subjects

To recreate the challenge of distinguishing between the top and acceptable information security performers, we compiled a relative homogenous sample. Subjects were recruited via email from a list of past and current undergraduates at mid-sized university in the southeastern United States. The sample was constructed to approximate the application pool for an entry-level position in information security in the late stages of the hiring process. Thus, the threshold criteria included IT work experience, familiarity with network and server operating systems, and formal training in information security. These criteria were modeled after the core job requirements for entry-level information security positions posted on various online employment boards. The sample was constructed by recruiting individuals who had recently completed an undergraduate course on information security, were familiar with server and network operating systems, and were presently employed in the IT field or had at least 3 months of work experience in the IT field. These individuals were theoretically qualified for entry level information security positions. Seventy-seven subjects were recruited via email. Of these, 61 attended the testing session, performed the evaluations, and completed the FFM and SOV instruments.

Assessments

Carlson et al. [9] called for the selection of highly validated instruments to be used in multiple-hurdle selection. They specify the use of selection device instruments which incorporate interval measurements with sufficient gradations in information. This study uses validate measures with appropriate scaling.

To operationalize the FFM, a widely accepted, condensed version of the original measure was used [44]. This measurement consists of 40 mini-markers, 8 for each personality dimension. To complete the inventory, respondents rate the extent to which they identify with each marker on a scale of 1–9. This instrument was designed to be completed in 15 minutes and is known to have high reliability.

In order to measure candidates' workplace values, an updated version of the original SOV measure was implemented [42]. This pen-and-paper measure contained 45 items. This metric yields 120 scores, 20 from each value domain. The first 30 items are couplets, while the last 15 items are quartets. Mean scores for all six domains are computed. A higher mean score is indicative of a stronger value preference. This measure was designed to be completed in 20 minutes.

Procedure

In order to operationalize the dependent variable—performance at entry-level security operations—a laboratory style test was performed (see Figure 1 for details). In this test, subjects were expected to analyze the security of servers and networking

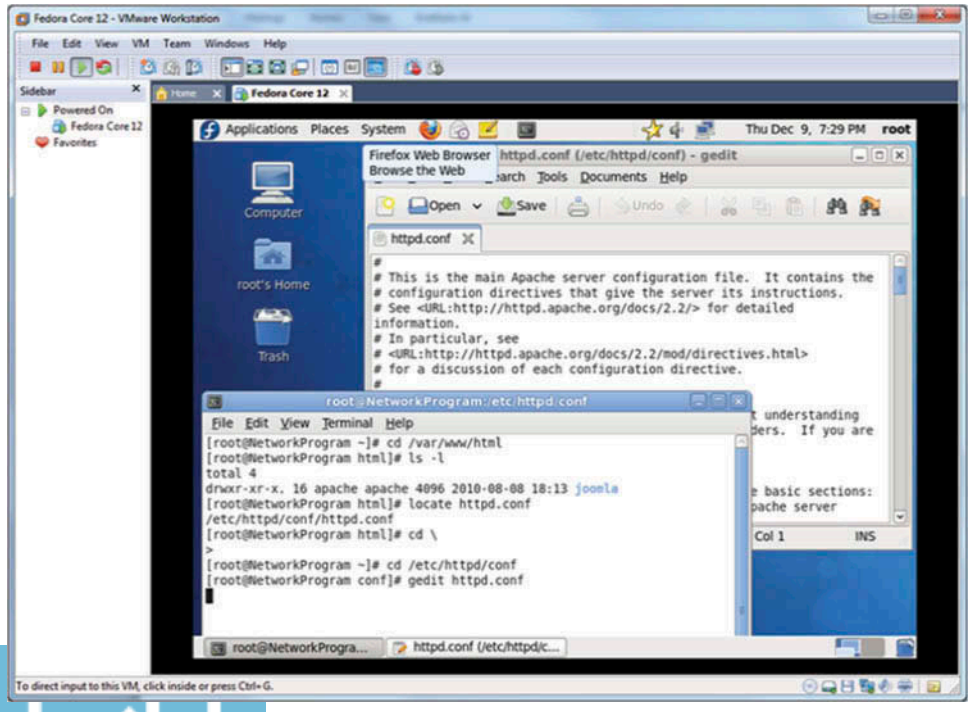

Figure 1. Evaluation of candidate performance.

operating systems, identify major vulnerabilities, and implement effective solutions as quickly as possible. Thus, subjects were compared according to the time taken to identify a vulnerability and implement a solution. Time-to-completion is a recognized method of scoring ability tests and has been cross-validated on both pen-and-paper and computerized tests [45].

Each subject completed three tests. One test involved a production Linux server, a second test involved a Windows Server, and the third test involved a Cisco IoS network operating system. The server and network operating systems were presented as virtual machine images. To create a more realistic environment, the virtualization platform was based on the ESXi hypervisor developed by VMware. This platform was selected because it is one of the most commonly used virtualization environments in the enterprise systems class that all subjects had successfully completed. It also includes a number of features which are useful in the present study, such as the snapshot feature. This function makes it possible to capture and assess the state of a virtual machine's configurations at any given point in time.

Each test image was preconfigured with a significant security vulnerability that an entry-level security analyst could reasonably be expected to identify and address. The Linux image contained unsecured configuration files. The Windows Server 2012 image allowed web-enabled directory browsing, and the IoS image allowed open ports. Aside from these vulnerabilities, all images were otherwise hardened. This step was taken to ensure that the intentional vulnerabilities presented the largest security gap.

Prior to each test, the subject was told to analyze the image and identify and mitigate the largest vulnerability as quickly as possible. If a subject did not identify the vulnerability or reconfigured some other aspect of the system, he or she received a score which correlated with the maximum amount of time allowed of 30 minutes. If a subject's attempted reconfiguration was unsuccessful, he or she also received a score of the maximum amount of time allowed. For each of the tests, a number of alternative approaches could be used to address the vulnerability. Any configuration was considered acceptable as long as it mitigated the vulnerability.

For automated scoring, virtual machine snapshots were analyzed using a modified version of Bastille—a security audit and hardening program which performs a third-party review of operating system images. In particular, Bastille reviews standard server settings and identifies weaknesses and security risks. The original software was updated and modified for this project to focus solely on the vulnerabilities included in the tests. For each test, the software determines if the preconfigured vulnerability were addressed from an outside perspective. Bastille did not consider how a vulnerability was closed—only that it was fully mitigated. Some further modifications were required to port the Bastille software to the Cisco and Windows operating systems. For output, Bastille provides a report of the status of each server's security profile. If an image's preconfigured vulnerability was closed, then it is assumed that the subject provided an effective mitigation. This allowed for multiple approaches to successful mitigation.

The subject's time spent in analyzing and auditing the image was then recorded. Time taken for each of the three tests was combined to create a composite variable. A subject that did not adequately address a vulnerability was given the maximum time of 30 minutes for the corresponding test. For instance, a subject who successfully completed her or his tests in times of 21, 15, and 12 minutes had an aggregate of 38. Thus, a lower number indicates better performance at identifying and fixing security vulnerabilities under pressure. This value was used as the dependent variable.

Analysis

Demographic data are depicted in Table 1. Individuals' survey responses were matched with their scores from the simulations. No significant differences were detected for age, gender, or ethnicity differences. The 61 subjects were sorted according to their composite performance measures. The top information security performers were defined as individuals with the lowest composite time metrics. This category was restricted to the one-third lowest scores. This demarcation was based on a previous study in which the classification of "top employees" was limited as a third of the workers in any given organization [46].

The personality and values attributes of top information security performers were compared against the rest of the subjects (see Table 2 for personality and Table 3 for values). For each personality dimension and workplace value, a *t*-test of significant differences was performed. *t*-Tests are traditionally used to determine if two sets of data are significantly different and assumes the test statistic follows a normal distribution. The purpose of this test is to compare and contrast top information security performers with the other information security performers on an item-by-item basis.

Results

In general, the results support initial assumptions about personality, workplace values, and performance. The purpose of this research is to identify traits and values which distinguish the top information security performers from their peers. This research is timely. Multinational organizations are developing in-house expertise to hedge against major data leaks. To accomplish this, they are taking an even more deliberate approach to hiring. They are seeking the best information security professionals from a broad talent pool. Distinguishing between good and the top candidates is challenging because they have much in common, including many psychological characteristics. Fortunately, this study finds that

Table 1. Demographic data.

Parameter	Summary	Value
Age (years)		
	Mean	21.4
	Median	21
	Range	20–22
Gender		
	Male	57
	Female	3
	Unreported	1
Ethnicity		
	Caucasian	49
	Black	8
	Hispanic	2
	Asian	1
	Other	1

Table 2. Mean personality dimension scores.

	Top performers		Rest of cohort			
	Mean	Standard deviation	Mean	Standard deviation	*t*	*p*
Openness	49.76	8.35				.009
Conscientiousness	52.20	7.48	47.88	7.16	2.18	.017
Extraversion	39.92	6.49	41.27	6.98	.725	.236
Agreeableness	36.59	8.03	36.68	7.45	.966	.169
Neuroticism	28.73	7.24	29.74	6.01	.575	.284

Table 3. Mean workplace value scores.

	Top performers		Rest of cohort			
	Mean	Standard deviation	Mean	Standard deviation	*t*	*p*
Theoretical	41.79	7.39	38.03	6.38	2.05	.022
Economic	48.38	6.65	44.98	7.17	1.77	.041
Social	42.67	5.78	47.98	7.05	2.91	.000
Political	38.73	6.98	39.97	6.94	.653	.259
Aesthetic	37.98	7.04	38.69	5.80	.418	.339
Religious	36.31	5.49	39.42	6.17	1.91	.030

different levels of information security work performance can be linked to subtle differences in personality traits and workplace values.

To recreate the challenge that companies are facing, a sample consisting of subjects with at least 3 months of IT work experience and formal training in information security was compiled. This resulted in a relatively homogenous talent pool. It was presumed that the top information security performers would differ with respect to their personality traits and workplace values. Specifically, it was predicted that they have higher levels of conscientiousness, openness, and agreeableness and lower levels of extraversion and neuroticism. It was also predicted that they place a greater emphasis on theoretical and economic values and less emphasis on social, political, aesthetic, and religious values. To identify the top information security performers, the subjects completed a series of exercises which recreate the type of tasks which information security professionals are expected to perform. Subjects were ranked according to their aggregate performance scores. Those with the highest one-third of scores were compared against the lower two-thirds in order to identify distinguishing characteristics. The results are described below.

The results of hypothesis tests are shown in Table 4. With respect to the first hypothesis, H1, it was found that top performers have significantly higher levels of conscientiousness. This finding confirms early expectations that close attention to detail will be an important factor in auditing systems. The second hypothesis, H2, presumed that top information security performers will report higher levels of openness. The results suggest that these individuals indeed have significantly higher levels of openness, related, for example, to more intellectual curiosity. The third hypothesis suggested that top security performers will have significantly lower levels of extraversion. However, in this test it appears that they do not significantly differ from the remaining performers. This is likely because all the subjects in the sample are of similar personality types who gravitate toward cyber security and information technology. The fourth hypothesis, H4, states that top performers will have higher levels of agreeableness. The results indicate that this is not the case. The levels of agreeableness were almost equal for both groups. The fifth hypothesis conjectured that top performers would have lower levels of neuroticism. The results of testing did not confirm this hypothesis. It appears that with respect to personality attributes, top security performers have higher levels of openness and conscientiousness, and do not differ otherwise.

Table 4. Results of hypothesis testing.

	Description	Significance	Result
H1	Top performers will have higher levels of conscientiousness	.009	Supported
H2	Top performers will have higher levels of openness	.017	Supported
H3	Top performers will have lower levels of extraversion	.236	Not supported
H4	Top performers will have higher levels of agreeableness	.169	Not supported
H5	Top performers will have lower levels of neuroticism	.284	Not supported
H6	Top performers will place greater emphasis on theoretical values	.022	Supported
H7	Top performers will place greater emphasis on economic values	.041	Supported
H8	Top performers will place less emphasis on social values	.000	Supported
H9	Top performers will place less emphasis on political values	.259	Not supported
H10	Top performers will place less emphasis on aesthetic values	.339	Not supported
H11	Top performers will place less emphasis on religious values	.030	Supported

The sixth hypothesis, H6, holds that the top performers will place a greater emphasis on theoretical values. The results confirm this expectation. Top performers are interested in the pursuit of truth. This is an asset because it encourages more in-depth analysis of mission-critical security issues. Next, the seventh hypothesis, H7, assumes that top information security professionals will place a greater emphasis on economic values. This hypothesis was based on the assumption that top workers will be influenced by economic incentives and rewards. The results confirm that this is the case. It appears that top information security workers can be distinguished by

their tendency toward economic values. The eighth hypothesis, which assumes that top security performers will places less emphasis on social values, was supported. This was an interesting finding given that the same individuals did not report lower levels of extraversion. Top performers are not shy, but prefer to focus on non-social pursuits.

The ninth hypothesis (H9) stipulated that top security performers will place less emphasis on political values. This hypothesis was not supported. It could be interpreted that both top performers and those who are least competent workers have relatively little interest in political values. The tenth hypothesis (H10) held that top performers will place less emphasis on aesthetic values. It was not supported. Throughout the sample, subjects placed relatively little emphasis on aesthetic values. The final hypothesis, H11, suggests that top performers will place less emphasis on religious values. This hypothesis was confirmed. Although the mean religious values for both groups were low, they were even lower for top performers. This does not imply that top information security performers are not religious. Only that they are less concerned with reconciling their environment with a priori world beliefs. To summarize the values hypotheses, the top security performers place a greater emphasis on theoretical and economic values, and significantly less emphasis on social and religious values.

The current study found two of the five personality traits significant predictors and four of the six workplace values significant predictors of job performance. Previous findings of studies involving personality traits are summarized in Appendix A. One can see a wide variety of results from none supported to all dimensions of personality supported. Previous studies involving workplace values tend to be more consistently supported as significant predictors of job performance as summarized in Appendix B. While results are mixed, it is probable that the context or varying domains may prove to be intervening factors. With respect to the extant literature, three comments are proffered. First, this study confirms previous findings that personality is a modest predictor of performance. Second, it demonstrates that values are reliable predictors of performance. Values have been previously overlooked within the information systems domain. In doing this, it lays the groundwork for future research on values. Third, it clarifies that organizations can and should integrate empirical tools within their recruitment processes to identify the top candidates.

Implications

Having reviewed the findings from the study, this section provides implications for researchers. It then reviews the implications for human resources professionals and hiring managers.

Implications for research

The purpose of this study is to identify the personality and workplace value attributes of top information security professionals so that they can be more easily identified by hiring managers. Differences between top and average information security workers are subtle. Subtle-but-significant differences in personality and workplace values were found to correspond with subtle-but-significant differences in performance. This finding is important for those who must discern between a myriad of qualified candidates for information security positions, before it provides an objective point of comparison.

To recreate the challenge of distinguishing between the top and acceptable information security performers, a relative homogenous sample was compiled. All subjects had formal information security training (at least one college course on information security) and relevant work experience (at least 3 months in the IT field). The sample approximates an application pool in which unqualified applicants have been culled and only those who meet predetermined levels of competence remain for consideration. To reach this level of competence, a person's psychological makeup must be compatible with the nature of information security work. For instance, those with extraverted personalities will have a difficult time focusing on technical minutia for long periods of time. Further, those who prioritize social values will prefer interpersonal interaction over the in-depth analyses the job often entails. Not surprisingly, it was found that individuals who met the threshold definitions of competence shared some general psychological similarities. Despite these generalities, it was shown that it is possible to distinguish top performers by focusing on differences in specific personality traits and workplace value attributes.

If the sample was expanded to include individuals with no training or experience, one would expect greater variation in personality and workplace value attributes along with significant differences in task performance. Such a sample would approximate an application pool in the initial stages in the hiring process, when the pool contains unqualified applicants. However, since the purpose of this study is to differentiate top information security workers from their peers, it was necessary to constrain the sample to those who met the competence criteria. The implications of this research are significant. It is difficult for hiring managers and HR professionals to discern the small differences in personality and workplace values by probing with typical interview questions, and harder still to make valid comparisons among candidates. This research indicates that assessments are a valid method for quantifying the subtle-but-important differences among candidates. The importance of the domain of information security is growing at an exponential rate which in itself is a call for increasing research opportunities.

Implications for practice

A 2014 study by RAND titled "H4CKER5 WANTED, An Examination of the Cybersecurity Labor Market" reported a significant rise in the demand for cybersecurity experts and pointed out the lag in supply as experts migrate through the typical process of education and/or training to become productive cybersecurity experts. They point out, currently it is a cybersecurity expert seller's market. This exacerbates the need for successful effective recruitment and selection [46]. Understanding the personality types and natural behavioral preferences of job candidates can substantially enhance the

candidate selection process. Aptitude and cognition tests are important but not sufficient predictors of worker performance. When interviewing candidates, hiring managers and human resource professionals often face the challenge of not knowing anything about the candidates' motives, creativity, determination, and ambitions. It can be difficult to develop questions which reveal each candidate's strengths and probe for weaknesses without introducing biases. Without an objective point of comparison, the task of identifying the top candidates becomes challenging.

RAND made note that cybersecurity experts are not a commodity. They note a "vast difference between good and great hackers." They make reference to the importance of finding the "best of the best" [46]. This is where the findings of this study indicate that personality and values assessments can be leveraged. When used in conjunction with other measures (e.g., reference checks, experience reviews, cognitive tests, etc.), they provide additional insight and add value in decision making. Pre-hire assessments have been used for decades, but they have primarily been used to screen candidates for management and sales positions. Recent studies indicate that enduring traits such as disposition and values also have a bearing on performance of technical work. We find that this is particularly true for information security work. The subtle differences in personality traits and value attributes correlate with different levels of information security worker performance. The good news is that the cost of pre-hiring assessments is at all-time lows. The rise of automated testing tools and the online application process have resulted in falling costs, more accurate results, and resurging use. Even small companies can afford to integrate online assessments into their hiring process. The additional information affords the ability to quickly pinpoint top information security performers from a pool of qualified candidates.

It should be noted that even though they can be used to predict performance, personality and workplace values assessments are most effective when combined with other measures of high predictive validity. Using well-designed and validated assessments provide a significant advantage in identifying top candidates.

Conclusions

The purpose of this research was to identify the traits and values of top information security personnel so that they could be more easily identified from within deep talent pools. The process of shifting between good and top candidates is challenging. We found differences in personality traits and values correspond with differences in performance. Within a relatively homogenous sample of competent test subjects, it was possible to predict the top performers of information security work. Pre-hire assessments provide a valid, objective point of comparison of applicants for information security positions. They are specifically encouraged to be used as part of a multi-method approach to candidate selection. This suggests opportunities for further research on additional factors to distinguish top information security performers.

References

[1] Baskerville R, Spagnoletti P, Kim J. 2014. Incident-centered information security: managing a strategic balance between prevention and response. Inf Manage. 51:138–151.
[2] Ruefle R, Dorofee A, Mundie D, Householder A, Murray M, Perl S. 2014. Computer security incident response team development and evolution. IEEE Secur Privacy. 12:16–26.
[3] Tøndela I, Lineb M, Jaatun M. 2014. Information security incident management: current practice as reported in the literature. Comput Secur. 45:42–57.
[4] Weber L. 2015. Today's personality tests raise the bar for job seekers. Wall Street J. http://www.wsj.com/articles/a-personality-test-could-stand-in-the-way-of-your-next-job-1429065001
[5] Mount M, Barrick M, Stewart G. 1998. Five-factor model of personality and performance in jobs involving interpersonal interactions. Hum Perform. 11:145–165.
[6] Judge T, Higgins C, Thoresen C, Barrick M. 1999. The big five personality traits, general mental ability, and career success across the life span. Personnel Psychol. 52:621–652.
[7] Kolodinsky R, Giacalone R, Jurkiewicz C. 2008. Workplace values and outcomes: exploring personal, organizational, and interactive workplace spirituality. J Bus Ethics. 81:465–480.
[8] Gatewood R, Field H, Barrick M. 2010. Human resource selection. Mason, OH: Cengage Learning.
[9] Carlson K, Connerley M, Mecham R. 2002. Recruitment evaluation: The case for assessing the quality of applicants attracted, Personnel Psychol. 55:461–490.
[10] Murphy K. 1986. When your top choice turns you down: effects of rejected job offers on the utility of selection tests. Psychological Bull. 99:128–133.
[11] Bobko P, Roth P, Potosky D. 1999. Derivations and implications of a meta-analytic matrix incorporating cognitive ability, alternative predictors, and job performance. Personnel Psychol. 52:561–589.
[12] Barrick M, Mount M, Judge T. 2001. Personality and performance at the beginning of the new millennium: what do we know and where do we go next?, Int J Sel Assess. 9:9–30.
[13] Rash H, Tosi H. 1992. Factors affecting software developers' performance: an integrated approach. MIS Q. 16:395–413.
[14] Ashkanasy N, Bowen P, Rohde F, Wu C. 2007. The effects of user characteristics on query performance in the presence of information request ambiguity. J Inf Syst. 21:53–82.
[15] Goldberg L. 1990. An alternative description of personality: the big-five factor structure. J Personality Social Psychol. 59:1216–1229.
[16] Seibert S, Kraimer M. 2001. The five-factor model of personality and career success. J Vocational Behav. 58:1–21.
[17] McCrae R, John O. 1992. An introduction to the five-factor model and its applications. J Personality. 60:175–215.
[18] McCrae R, Costa P. 1987. Validation of the five-factor model of personality across instruments and observers. J Personality Social Psychol. 52:81–90.
[19] Salgado J. 1997. The five factor model of personality and job performance in the European Community. J Appl Psychol. 82:30–43.
[20] Heslin P. 2005. Conceptualizing and evaluating career success. J Organiz Behav. 26:113–136.
[21] Hogan S, Coote L. 2014. Organizational culture, innovation, and performance: a test of Schein's model. J Bus Res. 67:1609–1621.
[22] Vernon P, Allport G. 1931. A test for personal values. J Abnormal Social Psychol. 26:231–248.
[23] Eccles J, Wigfied A. 2002. Motivational beliefs, values, and goals. Annu Rev Psychol. 53:109–132.
[24] Geare A, Edgar F, McAndrew I. 2009. Workplace values and beliefs: an empirical study of ideology, high commitment management and unionisation. Int J Hum Resour. 20:1146–1171.
[25] Jurkiewicz C, Giacalone R. 2004. A values framework for measuring the impact of workplace spirituality on organizational performance. J Bus Ethics. 49:129–142.

[26] Goodman S, Svyantek D. 1999. Person–organization fit and contextual performance: do shared values matter. J Vocational Behav. 55:254–275.
[27] van Beurdan P, Gossling T. 2008. The worth of values – a literature review on the relation between corporate social and financial performance. J Bus Ethics. 82:407–424.
[28] Milliman J, Czaplewski A, Ferguson J. 1988. Workplace spirituality and employee work attitudes: an exploratory empirical assessment. J Organizational Change Manage. 16:426–447.
[29] Horne B. 2014. On computer security incident response teams. IEEE Secur Privacy. 12:13–15.
[30] Whitman M. 2003. Enemy at the gate: threats to information security. Commun ACM. 46:91–95.
[31] Vroom C, von Solms R. 2004. Towards information security behavioural compliance. Comput Secur. 23:191–198.
[32] Felder R, felder G, Dietz E. 2002. The effects of personality type on engineering student performance and attitudes. J Eng Educ. 91:3–17.
[33] Culp G, Smith A. 2001. Understanding psychological type to improve project team performance. J Manage Eng. 17:24–33.
[34] Kamdar D, Van Dyne L. 2007. The joint effect of personality and workplace social exchange relationships in predicting task performance and citizenship performance. J Appl Psychol. 92:1286–1298.
[35] Cox-Fuenzalida L, Swickert R, Hittner J. 2004. Effects of neuroticism and workload history on performance. Personality Individual Differences. 36:447–456.
[36] Bono J, Vey M. 2007. Personality and emotional performance: extraversion, neuroticism, and self-monitoring. J Occup Health Psychol. 12:177–192.
[37] Swenson M, Herche J. 1994. Social values and salesperson performance: an emprical examination. J Acad Marketing Sci. 22:283–289.
[38] Arndt A. 2012. Is it better for salespeople to have the highest customer orientation or a strong fit with their group's customer orientation? Findings from automobile dealerships. J Retailing Consum Serv. 19:353–359.
[39] Kalleberg A. 1977. Work values and job rewards: a theory of job satisfaction. Am Socio Rev. 42:124–143.
[40] Leuty M, Hansen J. 2012. Building evidence of validity: the relation between work values, interests, personality, and personal values. J Career Assess. 21:175–189.
[41] Leim G, Martin A, Porter A, Colmar S. 2011. Sociocultural antecedents of academic motivation and achievement: role of values and achievement motives in achievement goals and academic performance. Asian J Social Psychol. 15:1–13.
[42] Kopelman R, Rovenpor J, Guan M. 2003. The study of values: construction of the fourth edition. J Vocational Behav. 62:203–220.
[43] Christian M, Garza A, Slaughter J. 2011. Work engagement: a quantitative review and test of its relations with task and contextual performance. Personnel Psychol. 64:89–136.
[44] Saucier G. 1994. Mini-markers: a brief version of Goldberg's unipolar big-five markers. J Personality Assess. 63:506–516.
[45] Mead A, Drasgow F. 1993. Equivalence of computerized and paper-and-pencil cognitive ability tests: A meta-analysis. Psychol Bull. 114:449–458.
[46] Mitchell T, Holtom B, Lee T. 2001. How to keep your best employees: developing an effective retention policy. Acad Manage Perspect. 15:96–108.

Appendix A

Table A1. Personality as a predictor of performance in the information systems field.

Authors	Year	Personality constructs	Context	Measurement	Sample	Results
Rash and Tosi	1992	Locus of Control	Software development	Subjects self- reported development performance on a nine-point scale	230 US software developers	Not supported
McElroy et al.	2007	Revised NEO Personality Inventory	Systems analysis	Subjects self-reported ability to use internet tools	92 US MBA students; 61 US undergraduate students	All dimensions supported
Ashkanasy et al.	2007	Five Factor Model	Database administration	Accuracy and time required to create a series of SQL queries	75 International undergraduate students	Neuroticism, openness, agreeableness, and conscientiousness were supported
Korzaan and Boswell	2008	Big Five Personality Dimensions	Computer Usage	Subjects self-reported extent of use of desktop computers	230 US undergraduate students	Agreeableness and neuroticism were supported
Devaraj et al.	2008	Five Factor Model	Contribution to collaborative IT projects	Frequency of use of a collaborative system	180 MBA students	Neuroticism, extraversion, agreeableness, and conscientiousness were supported
Basnal	2011	Big Five Personality Dimensions	E-book usage	Subjects self-reported frequency of use of e-books	123 US undergraduate students	Agreeableness and emotional instability were supported
Svensen et al.	2013	Big Five Personality Dimensions	Computer usage	Subjects self-reported extent of use of mobile devices	1,004 Norwegians	Conscientiousness and openness were supported
Shropshire et al.	2015	Conscientious-ness and Agreeableness	Systems administration	Frequency of use of an online logging system, recorded in logs	170 US undergraduate IS students	All dimensions supported
Srivastava et al.	2015	Five Factor Model	IT job engagement	Subjects self-reported level of job engagement and burnout	152 Senior managers of Asian firms	Neuroticism and agreeableness were supported

Appendix B

Table B1. Values as predictors of performance in the information systems field.

Authors	Year	Values constructs	Context	Measurement	Sample	Results
Rash and Tosi	1992	Achievement needs	Software Development	Subjects self-reported performance on a nine-point scale	230 US software developers	Supported
Meglino et al.	1989	Achievement, helping, concern for others, fairness, and honesty	Industrial system maintenance	Analysis of quarterly performance reports by managers	174 US industrial workers	Achievement and honesty were supported
Ticona	2015	Status, peer recognition	Knowledge work	Subjects self-reported extent of use of ICT	40 US service workers	Both constructs supported
Chou et al.	2008	Ethics, respect, effectiveness, attention to detail, and cohesion	Collaborative project management	Peer ratings of individuals' contribution to projects	130 Chinese knowledge workers from 72 teams	Effectiveness and attention to detail were supported
Siu	2003	Chinese Work Values (loyalty, power, reciprocity, and hierarchy)	Professional work	Subjects self-reported work performance on a series of five-point scales	588 Hong Kong business professionals	All constructs were supported