A quantitative examination of perceived promotability of information security professionals with vendor-specific certifications versus vendor-neutral certifications

Greg Gleghorn
Capella University

Jean Gordon
Capella University

ABSTRACT

Human capital theory suggests the knowledge, skills, and abilities one obtains through experience, on-the-job training, or education enhances one's productivity. This research was based on human capital theory and promotability (i.e., upward mobility). The research offered in this article shows what effect obtaining information security certifications, whether vendor-neutral or vendor-specific, has on one's perception of promotability. This study surveyed a sample population of information security managers from the North Carolina chapter of the Information Systems Audit and Control Association to gauge their perceptions of promotability for information security professionals who possess either vendor-neutral or vendor-specific security certifications. The descriptive results leaned toward vendor-neutral information security professionals as more likely to be promoted, but hypothesis testing did not show an overall perception of promotability for either group. The research does show information security certification having some influence in the promotion process.

Key Words: Promotability, Human Capital Theory, It Certifications

INTRODUCTION

An information security program has a mandate to protect data, whether spoken, written, printed, or electronic (IT Governance Institute [ITGI], 2008). *Information security technology* and *information security program* are sometimes used interchangeably to reflect the same meaning. These two terms are mutually exclusive within the information security industry. Information security technology is concerned with the confidentiality, integrity, and availability of data in the form of voice, video, or written data within the technology domain (ITGI, 2008). A disclosure of confidential information between two people having a conversation is outside of the scope of information technology (IT) security. A comprehensive information security program, on the other hand, protects all information assets, which include the following: risk, business impact analysis, business continuity, abuse, unauthorized access, compliance, legal liability, disaster recovery, information security technology, physical security, and access control.

The purpose of this study was to evaluate the perceived promotability of two groups of information security professionals: vendor-specific security certified professionals and vendor-neutral security certified professionals. One of the problems associated with these two areas is vendor-specific security certification may be too narrow in scope, whereas vendor-neutral, while broad in scope, may not address specific areas of concern in depth. Two of the major leading certifications representing both groups are Cisco Certified Network Professional Security (CCNP Security) and Certified Information Systems Security Professional (CISSP). As of 2008, the number of CISSPs (vendor-neutral) worldwide was 57,602, with 56,892 being CISSP certified and 810 System Security Certified Practitioner, compared to 1,828 security Cisco Certified Internetwork Experts (CCIEs, vendor-specific; BradReese.com, 2011; CCCure.org, 2005).

The problem is the lack of knowledge about the relative values of vendor-specific and non-vendor-specific information security certifications, resulting in a gap in skills needed in the workplace. The information security industry is currently undergoing change where technical aspects of information security must also incorporate the business aspects of information security, such as risk management (ISACA, 2009). According to Ayoub (2011) of $(ISC)^2$, there is a definite skills gap in the information security industry. Ayoub (2011) cited social media and cloud computing as new technologies that businesses are adopting but information security professionals are resistant to embrace. Ayoub (2011) also asserted that information security professionals are so engulfed in their current duties that they are ill prepared to address advances in technology. This study may address the concerns alluded to by Ayoub by conducting a comparison analysis through survey to address the perceived skill sets of two groups of information security professionals—those who are vendor-neutral security certified and those who are vendor-specific security certified—and determine which is perceived as more promotable.

There are numerous research articles, editorials, and trade magazine articles that debate IT certification versus college degree (Brookshire, 2001; Cegielski, 2004; Hitchcock, 2007), where the argument stems from an education to product-specific training. Setting this debate aside, there is a lack of research debating the quality of the skills acquired from obtaining either vendor-neutral or vendor-specific certification as it pertains to information security. According to O*Net OnLine (2010), the Bureau of Labor Statistics (BLS) categorizes *information security* under *computer security specialists*, which may add more ambiguity because the job titles associated with computer security specialists, according to the BLS, range from information

technology specialist to information security manager. The BLS (2009) showed the outlook for computer security specialists as being bright, but this term is broad and includes skills from both vendor-neutral and vendor-specific categories, which may cause confusion for those seeking a distinct career within information security or for those seeking qualified employees with either vendor-neutral or vendor-specific skill sets. This study evaluated which skills from either group are perceived as more promotable.

BACKGROUND

Professional certifications such as Certified Public Accountant (CPA), Certified Nurse Assistant (CNA), Certified Internal Auditor (CIA), or a Certified Financial Planner (CFP) have been part of the work force for some time now (Shore, 2002). CPA is a certification administered by the American Institute of Certified Public Accountants. By passing an exam, a professional accountant is able to practice as long as he or she has met the requirements of a particular state (BusinessDictionary.com, 2010). The other certifications, such as CNA, CIA, and CFP, allow an individual to practice once he or she attains the certification. On the other hand, a lawful license is granted to a CPA.

Certification is the act of certifying; certifying is the written representation or guarantee that something or someone is authentic (Clapp, 2000). The authenticity comes from an individual or group of individuals who have shown competency in their chosen field of labor by passing an examination(s) set forth by a governing body that provides measurements, standards, and criteria to determine who is eligible for certification (Shore, 2002).

IT certification is provided to individuals along the same lines as other certifying institutions but from an industry perspective. For example, in the information security industry, there are certifying institutions, such as the International Information Systems Security Certification Consortium ([ISC]^2) and ISACA. (ISC)^2, CompTIA, and ISACA are three organizations that represent vendor-neutral certifying bodies, whereas Microsoft, Cisco, and Checkpoint are organizations that represent vendor-specific certifying companies.

IT certification has its origins in the latter half of the 1980s, started by Novell, Inc., a networking vendor out of Provo, Utah (Shore, 2002). Novell started what is now called *vendor-specific certification* to build market share and manage support costs by increasing the skill level of those who worked on and with Novell products (Shore, 2002). Novell developed the Certified Novell Engineer (CNE) certification that would measure the skills needed and provided validity to those who attained this certification. This in turn decentralized the support staff's responsibilities at Novell by having qualified certified engineers in the field, which alleviated total reliance on the support staff in Provo (Shore, 2002). With the success of Novell's certification processes, other companies during the early 1990s followed suit, such as Microsoft, Cisco Systems, Nortel, and Compaq. These companies created certifications for their products to increase demand, value, and loyalty (Shore, 2002).

According to Shore (2002), a good certification should have measures that are valid, consistent, and fair. The results from this study may also impact which group of information security professionals' certification, vendor-neutral or vendor-specific, measures the perceived validity, consistency, and fairness more effectively, which in turn may have an impact on the information security professional's perception of promotability.

The information security industry began its own certification process with $(ISC)^2$, which began in 1988 ($[ISC]^2$, 2011). ISACA was established in 1969. ISACA's Certified Information Security Manager (CISM) was introduced in 2003 (ISACA, 2009). These two organizations provide vendor-neutral security certifications. Vendor-specific security certifications, such as Cisco Certified Security Professional (CCSP), were first offered circa 2003 (Bastien, Nasseh, & Degu, 2003).

LITERATURE REVIEW

This article is based on human capital theory, which asserts that knowledge, skills, and abilities attained by individuals through investment, in education, experience, and on-the-job training, raise individual worker productivity (Marshall, 1998). This study compared the human capital investment in either vendor-neutral or vendor-specific certifications within the information security field as well as the perceived promotability of each group. *Promotability*, in this study, refers to the ability of an individual's capacity to rise to higher job responsibility or rank due to his or her individual investment in human capital. In the context of this study, the human capital investment is in becoming either vendor-neutral or vendor-specific security certified.

Security practitioners often obtain security certifications either to show competency in order to enter the field of information security or as continuing professional education credit toward established certification ($[ISC]^2$, 2011). A holder of an IT certification should indicate to an employer that the holder has the knowledge, ability, and skill to perform a job associated with that certification (Heise, 2009). Vendor-specific certifications such as MCSE (Microsoft Certified Systems Engineer), CNE, or CCNA (Cisco Certified Network Associate) are proprietary certifications where holders become certified with skills necessary to address proprietary applications and systems. Vendor-neutral certifications, such as those granted by CompTIA, are broad and not necessarily associated with any one vendor but rather the basic and advanced skills of a technology such as internetworking are tested to see if an individual can grasp the concepts (CompTIA, 2011).

The information security industry also provides certification testing, both vendor-specific and vendor-neutral (CompTIA, 2011; ISACA, 2008; Microsoft, 2011; Symantec, 2011). These types of certifications are usually advanced certifications requiring industry experience. ISACA (2008) conducted a survey on the information security profession. A subset of this survey compared the differences between professional certifications (vendor-neutral) such as CISSP and CISM and technical certifications (vendor-specific) such as CCNP and MCSE, and discovered some wide-ranging disparities between the two groups (ISACA, 2008). For instance, 78% of the professionally certified group valued education; 86.9% of the polled participants in this group had at least a bachelor's degree. When the survey asked participants the importance of technical certifications, 38% acknowledged having technical certification was important (ISACA, 2008).

In February 2003, the president released the *National Strategy to Secure Cyberspace*, a framework for strengthening the U.S. critical infrastructure. Another document released by the DHS (2008), *IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development*, works in conjunction with the president's strategy by developing requirements and standards for the information security work force. This document states it has taken advice and best practice information from academia and public and private sectors to advance information security training and certification to ensure the training of

the most qualified IT security work force possible (DHS, 2008). The purpose of the document was to create a unifying framework for IT security training and professional development (DHS, 2008). The document contains five sections: an introduction; IT security competency areas; IT security key terms and concepts; IT security roles, competencies, and functional perspectives; and IT security, competency, and functional matrix (DHS, 2008). The document relates to this study by providing additional information to measure which group is more promotable. For example, the section on IT security roles provides a ranking of roles while the section on IT security competency areas provides the skills associated with obtaining those roles (DHS, 2008). Table 1 shows a comparison of four IT security roles and the functional responsibilities for each (e.g., manage, design, implement, or evaluate; DHS, 2008).

Table 1. IT Security Roles and Functional Responsibilities

	Executive*	Functional*		Corollary*
IT security roles	Information security officer	IT security professional	IT security engineer	Privacy professional
Data security	M, D, E	M, D, E	D, E	D, E
Digital forensics	M, D	N/A	N/A	N/A
Enterprise continuity	M, E	E	N/A	N/A
Incident management	M, D, E	E	N/A	N/A
Personnel security	M	D	N/A	I, D
Physical security	M	D, E	N/A	N/A
Procurement	M, D, E	N/A	N/A	N/A
Regulatory and compliance	M, D, E	I	N/A	M, D, I, E
Risk management	M, D, E	D, E, I	I	M, D, I, E
Strategic security management	M, D, E	N/A	N/A	N/A
Systems and application security	M, E	N/A	D, E, I	N/A

Note. Data are from *Information Technology (IT) Security Essential Body of Knowledge (EBK)*, by Department of Homeland Security, 2008. Retrieved from http://www.us-cert.gov/ITSecurityEBK/EBK2008.pdf
*M = manage, D = design, I = implement, E = evaluate.

From Table 1, the roles closely associated with this study's comparison analysis are IT security professional and IT security engineer. The IT security professional has more functional responsibilities than the IT security engineer. The IT security engineer's responsibilities are geared more toward securing the network infrastructure. The IT security professional, on the other hand, is also responsible for securing the network infrastructure but also has business-related responsibilities (DHS, 2008).

CISSP is a vendor-neutral certification offered by $(ISC)^2$ (Harris, 2005). According to Harris (2005), CISSPs are expected to have knowledge of 10 security domains: access control, network security, security management, applications/systems development, cryptography, security architecture, operations, business continuity/disaster recovery, telecommunications law, and physical security. CISSPs are not expected to have expert knowledge in each domain but are expected to have familiarity with each domain (Harris, 2005). CISSPs are also expected to have the skills necessary for effective security management, such as risk management, information security policies, procedures, standards, guidelines, baselines, information classifications, security organizations, and security education (Harris, 2005).

CCSP is a vendor-specific certification offered by Cisco (n.d.). In order to obtain the CCSP certification, an individual is required to pass four exams. Each exam focuses on a specific area of network security, such as securing routers and switches, firewall technology, virtual private network, and intrusion prevention and detection systems (Cisco, n.d.). CCSPs are responsible for network security. What this means is CCSPs are responsible for the implementation of security devices, security policies, and processes to prevent unauthorized access to network resources, voice, video, or data as they pertain to Cisco proprietary network security devices (Bastien et al., 2006). Table 2 compares the roles and responsibilities of a CISSP to those of a CCSP.

Table 2. Comparing Roles and Responsibilities of CISSPs and CCSPs

IT security roles	CISSP*	CCSP*
Data security	M, D, E	D, E
Digital forensics	N/A	N/A
Enterprise continuity	E	N/A
Incident management	E	N/A
Personnel security	D	N/A
Physical security	D, E	N/A
Procurement	N/A	N/A
Regulatory and compliance	I	N/A
Risk management	D, E, I	I
Strategic security management	N/A	N/A
Systems and application security	N/A	D, E, I

Note. Data are from *Information Technology (IT) Security Essential Body of Knowledge (EBK)*, by Department of Homeland Security, 2008. Retrieved from http://www.us-cert.gov/ITSecurityEBK/EBK2008.pdf
*M = manage, D = design, I = implement, E = evaluate.

Table 2 shows the differences in responsibilities assigned to vendor-neutral CISSPs and vendor-specific CCSPs. These roles and responsibilities are similar to the information security professional and IT security engineer in Table 1.
Table 3 shows the top 15 IT certifications and the average salary, according to a survey conducted by ZDNet's Tech Republic organization (Schneider, 2011).

Table 3. Top 15 IT Certifications and Average Salary

IT certifications	Certification rank: Vendor-neutral	Certification rank: Vendor-specific	Average Salary
1. Project Management Professional (PMP)	X		$101,695
2. PMI—Certified Associate in Project Management (CAPM)	X		$101,103
3. ITIL v2—Foundations	X		$95,415
4. CISSP	X		$94,018
5. Cisco CCIE (Routing and Switching		X	$93,500
6. Cisco CCVP (Voice)		X	$88,824
7. ITIL v3—ITIL Master	X		$88,600
8. MCSD—Microsoft Certified Solutions Developer		X	$84,522
9. Cisco CCNP		X	$84,161
10. Red Hat Certified Engineer		X	$83,692
11. MCITP—Microsoft Certified IT Professional		X	$82,941
12. Cisco CCSP		X	$80,000
13. MCAD—Microsoft Certified Applications Developer		X	$79,444
14. MCITP—Database		X	$77,000
15. MCDBA—Microsoft Certified Database Administrator		X	$79,960

Note. Data are from *Top 15 Highest Paying Certifications in the Technology Industry*, by L. Schneider, 2011. Retrieved from http://jobsearchtech.about.com/od/educationfortechcareers/tp/HighestCerts.htm

Vendor-specific certifications outnumber vendor-neutral certifications, but the top-ranked certifications are vendor-neutral. In addition, the ranking of CISSP at number 4 compared to CCSP at number 9 also shows some disparity between these two certifications.

Table 4 further breaks down this comparison analysis by the top five information security certifications for 2011, according Gupta (2010). Of the top five information security certifications, four fall under the vendor-neutral specification, according to Gupta (2010).

Table 4. Top Five Information Security Certifications

Certification rank	Vendor-neutral	Vendor-specific
1. CISSP	X	
2. CEH—Certified Ethical Hacker	X	
3. CISM—Certified Information Security Manager	X	
4. GIAC—Global Information Assurance Certification	X	
5. Vendor Certifications—CCSE Checkpoint Certified Security Expert		X

Note: Data are from *Top 5 IT Security Certifications for 2011*, by U. Gupta, 2010. Retrieved from http://secureninja.com/news/3/Top-5-IT-Security-Certifications-for-2011-CISSP-CISM-CEH-training-certification/

A similar study by Heise (2009) sought to determine if there is a relationship between passing and obtaining an IT certification and the applicant's skills to perform a specific IT job. Heise's (2009) study focused on IT certificate holders who held vendor-specific Microsoft certifications and vendor-neutral CompTIA certifications in the field of PC support and networking. Heise (2009) conducted a mixed-method study with an open-ended survey to gather the opinions of employers on the value of IT certifications. The quantitative section of the methodology sampled a population of students from a community college by survey that asked

closed-ended questions on the value of obtaining IT certifications (Heise, 2009). Heise (2009) used the emerging themes from the qualitative section, which were then used in a quantitative instrument (i.e., the Likert-style survey questionnaire). Heise (2009) compared the results obtained from employers and applicants on the value of IT certifications using a *t* test, with some disparity appearing between groups that were dependent upon a specific survey question. For example, on required job experience, employers desired experienced IT professionals with 1–3 years of experience, but IT applicants thought employers required 1–2 years of experience (Heise, 2009). Employers also expressed a blend of experience, education, and certification were ideal credentials for applicants (Heise, 2009). The limitations of Heise's (2009) study are the sample return rate, where 200 employers and 400 employees were asked to participate but less than 90 from each group participated; also, the population was located in a specific region of the United States and the results may not be indicative of the population at large, so generalizability may or may not be applicable.

According to Hunsinger (2005), 6.5 million people in the United States held some type of computer certification, and that number was predicted to exceed 20 million by 2010. There is also a growing trend to begin to offer IT certification programs geared toward certifying students within secondary and postsecondary institutions (Randall & Zirkle, 2005).

Information security is a recent concept and, as this literature review has shown, the field of information security is a nascent learning industry, gathering intelligence as it begins to grow (Shostack & Stewart, 2008). Although there is substantial literature on IT certification, literature based on information security certification is just beginning to appear (ISACA, 2008; Shostack & Stewart, 2008; Trinckes, 2010. This study addresses a gap in the literature by examining information security certifications and their impact, if any, on promotability. This study sought to explain the impact of either of two independent variables of information security certifications, vendor-neutral and vendor-specific, on the dependent variable of promotability. Current literature does not address this specific phenomenon; thus, this study fills the gap.

METHOD

This research surveyed information security managers who were associated with an ISACA North Carolina chapter and had either obtained a bachelor's degree or higher or had at least 7 years of experience in the information technology/security industry to answers questions from a survey that addressed the perceived promotability of vendor-neutral or vendor-specific information security professionals. The participants in this study may or may not have been information security certified. The responses were statistically analyzed through descriptive statistics and independent samples *t* tests. The results from this study may assist employers, employees, human resource specialists, and academia to determine where to direct their human capital investment as it pertains to information security professionals who were either vendor-neutral or vendor-specific security certified and their ability to be promoted within an organization.

This quantitative study surveyed members of a North Carolina ISACA chapter. The population under observation is information security professionals who managed both or either vendor-neutral or vendor-specific security certified information security professionals and currently worked in the information security industry. Members of the ISACA North Carolina chapter met the aforementioned requirements and were presumed to be representative of the information security professional population. Current membership of this group is approximately

200, which meet assumptions of normality as the sample size is greater than the 30 (Boslaugh & Watters, 2008).

The survey instrument was launched using SurveyMonkey, an online survey tool that has been commercially available since 1999 (Creswell, 2009). SurveyMonkey was used to post an electronic survey at LinkedIn, which was then posted under the ISACA chapter group, an exclusive association requiring membership of information technology and security professionals, to those who met this study's requirements. These requirements included experience in the information technology and/or security industry, had either vendor-neutral or vendor-specific certifications, or managed information security professionals who had vendor-neutral or vendor-specific certifications. The professionals in this sample were employed in various industries that range from small to large companies, with a heavy contingent coming out of the financial industry due to the large financial presence in North Carolina. Demographic information was recorded, such as job title, industry, years of experience, education, and current certifications. SurveyMonkey captured responses from the survey questionnaire, and the results were downloaded into SPSS in order to conduct further statistical analysis.

Research Questions and Hypotheses

R1: Are vendor-specific security certified information security professionals perceived as more promotable by information security managers who have earned a bachelor's or higher degree or information security managers with 7 years of experience?
Null Hypothesis 1: Information security professionals who are vendor-specific security certified are not perceived as more promotable by information security managers with a bachelor's degree or higher.
Alternative Hypothesis 1: Information security professionals who are vendor-specific security certified are perceived as more promotable by information security managers with a bachelor's degree or higher.
Null Hypothesis 2: Information security professionals who are vendor-specific security certified are not perceived as more promotable by information security managers with 7 years of experience.
Alternative Hypothesis 2: Information security professionals who are vendor-specific security certified are perceived as more promotable by information security managers with 7 years of experience.
Null Hypothesis 3: Information security professionals who are vendor-specific security certified are not perceived as more promotable by information security managers with a bachelor's degree or higher and 7 years of experience.
Alternative Hypothesis 3: Information security professionals who are vendor-specific security certified are perceived as more promotable by information security managers with a bachelor's degree or higher and 7 years of experience.

R2: Are vendor-neutral security-certified information security professionals perceived as more promotable by information security managers who have earned a bachelor's or higher degree or information security managers with 7 years of experience?
Null Hypothesis 4: Information security professionals who are vendor-neutral security certified are not perceived as more promotable by information security managers with a bachelor's degree or higher.

Alternative Hypothesis 4: Information security professionals who are vendor-neutral security certified are perceived as more promotable by information security managers with a bachelor's degree or higher.
Null Hypothesis 5: Information security professionals who are vendor-neutral security certified are not perceived as more promotable by information security managers with 7 years of experience.
Alternative Hypothesis 5: Information security professionals who are vendor-neutral security certified are perceived as more promotable by information security managers with 7 years of experience.
Null Hypothesis 6: Information security professionals who are vendor-neutral security certified are not perceived as more promotable by information security managers with a bachelor's degree or higher and 7 years of experience.
Alternative Hypothesis 6: Information security professionals who are vendor-neutral security certified are perceived as more promotable by information security managers with a bachelor's degree or higher and 7 years of experience.

Results

The survey instrument was delivered electronically by SurveyMonkey to 200 members of the ISACA North Carolina chapter. E-mails were also sent to all 200 members. E-mails also were sent to ISACA members who were dual members of the Information Systems Security Association. The overall response rate was just below 25% (48 participants). Of these 48 participants, 40 completed the survey, lowering the effective response rate to 20%. The sample fit normal distribution, as the effective response return was more than 30.

Participants were asked to provide the following information: job title, work experience in information technology/security, level of education, and type of certification, if any, they held. Two thirds (66.7%) of the participants had over 10 years of experience in the information technology/security industry, 14.6% had over 7 years, 12.5% had 4–6 years, and 6.3% had less than 4 years of experience.

Table 5. How Long Have You Worked in the Field of IT or Information Security?

	Years	*f*	%	Valid %	Cumulative %
Valid	1–3	3	6.3	6.3	6.3
	4–6	6	12.5	12.5	18.8
	7–10	7	14.6	14.6	33.3
	Over 10	32	66.7	66.7	100.0
	Total	48	100.0	100.0	

Participants were asked their job title. Following are the 48 individual responses. The majority of the participants are senior-level IT/information security professionals.

1. IT Project Manager
2. Advisory services manager
3. Sr. Manager IS Infrastructure
4. Senior Information Security Consultant
5. Sr. Account Manager

6. Electronic Messaging Eng.
7. Systems Engineer
8. Sr. Application Developer
9. Project Manager
10. Manager Publications/IT Prod & Software Dev.
11. Consultant
12. Project Manager 3
13. Information Security III
14. Vice President, Corporate Security
15. Remediation Tracking Specialist
16. Information Security and Risk Manager
17. Technology Support
18. Area Practice Manager
19. IT Operations Specialist
20. ISSO
21. Senior Auditor
22. Compliance Consultant
23. Sr. Director of Information Security
24. VP, Information Security Consulting
25. IT audit manager
26. IT Project Manager
27. IT Director
28. Product Marketing, Security Portfolio
29. Director of technical Operations
30. Manager Info Security
31. CTO
32. Director/CIO
33. Network Engineer
34. Senior Auditor
35. Software Developer
36. Principal Engineer
37. IT Specialist
38. Configuration Management Engineer 5
39. Senior System Analyst
40. IT Consultant
41. Chief Strategy Officer
42. Owner/Operator my own company
43. TCC-W Chief Engineer
44. CISO
45. VP Engineering and Technical Solutions
46. Consultant/Entrepreneur/Faculty
47. Designated Accrediting Authority
48. InfoSec Director

Less than half (45.8%) of the participants had a bachelor's degree, 29.2% had a master's/MBA, 6.3% had doctorates, 14.6% had obtained other types of educational

certificates/diplomas as wells associate's degrees, and 4.2% had obtained a high school diploma with no further education.

Participants were asked which IT security certifications, if any, they would like their IT security staff to hold. The response was overwhelmingly in favor of vendor-neutral security certifications. Participants were asked to choose from the following list: CISSP, CISM, Security+, GIAC, CCNP security, CCIE security, and other (please specify). The top three chosen by participants were CISSP, CISM, and GIAC, respectively. Of the vendor-specific IT security certifications, CCNP security tied with Security+ for the fourth spot with nine participants (19.1%). Only seven participants suggested CCIE security for the IT security staff, which is somewhat surprising as CCIE is one of the highest vendor-specific information security certifications in the industry.

Table 8. Which IT Security Certification(s), If Any, Would You Most Likely Want Your IT Security Staff to Hold?

	Certification	*f*	%	Valid %	Cumulative %
Valid	Certified Information Systems Security Professional (CISSP)	39	81.3	100.0	100.0
Missing	System	9	18.8		
Total		48	100.0		
Valid	Certified Information Security Manager (CISM)	19	39.6	100.0	100.0
Missing	System	29	60.4		
Total		48	100.0		
Valid	Global Information Assurance Certification (GIAC)	12	25.0	100.0	100.0
Missing	System	36	75.0		
Total		48	100.0		
Valid	Cisco Certified Network Professional Security(CCNP Security)	9	18.8	100.0	100.0
Missing	System	39	81.3		
Total		48	100.0		

Thirty-nine participants (81.3%) would like their IT security staff to hold a CISSP certification, 19 participants (39.6%) would like their IT security staff to hold a CISM certification, 12 participants (25%) would like their IT security staff to hold a GIAC certification, and nine participants (18.8%) would like their IT security staff to hold a CCNP security certification.

Hypothesis 1

H1: Information security professionals who are vendor-specific security certified are not perceived as more promotable by information security managers with a bachelor's degree or higher.

After independent samples t test was applied to the survey responses of those participants who had a bachelor's degree or higher against those who did not resulted in the null Hypothesis 1 not being rejected. Participants were asked different scale questions on the perception of promoting a vendor-specific security certified employee. The significance levels of the scale

variables were all above .05 and the value of 0 was contained in both confidence intervals. Thus, information security managers with a bachelor's degree or higher did not have a perception of vendor-specific information security professionals as being more promotable.

Hypothesis 2

H2: Information security professionals who are vendor-specific security certified are not perceived as more promotable by information security managers with 7 years of experience.

After independent samples t test was applied to the survey responses between those participants who had 7 years or more of IT/information security experience against those who did not resulted in the null Hypothesis 2 not being rejected. Participants were asked different scale questions rating their perceptions of promoting vendor-specific security certified professionals using years of experience as a grouping variable. The cut point was established between 6 and 7 years of experience. The significance levels of the scale variables were all above .05 and the value of 0 was contained in both confidence intervals. Thus, information security managers with 7 years of more of IT/information security experience did not have a perception of vendor-specific information security professionals as being more promotable.

Hypothesis 3

H3: Information security professionals who are vendor-specific security certified are not perceived as more promotable by information security managers with a bachelor's degree or higher and 7 years of experience.

After independent samples t test was applied to the survey responses between those participants who had 7 years or more of IT/information security experience with a bachelor's degree or higher against those who did not meet this criteria. The *t* test resulted in the null Hypothesis 3 not being rejected. Participants were asked different scale questions rating their perceptions of promoting vendor-specific security certified professionals using years of experience and bachelor's degree or higher as a grouping variable. The cut point was established between 6 and 7 years of experience.

Hypothesis 4

H4: Information security professionals who are vendor-neutral security certified are not perceived as more promotable by information security managers with a bachelor's degree or higher.

After independent samples t test was applied to the survey responses between those participants who had a bachelor's degree or higher against those who did not resulted in the null Hypothesis 4 not being rejected. Participants were asked different scale questions on the perception of promoting a vendor-neutral security certified employee. The significance levels of the scale variables were all above .05 and the value of 0 was contained in both confidence intervals. Thus, information security managers with a bachelor's degree or higher did not have a perception of vendor-neutral information security professionals as being more promotable. The

significance levels are closer to or lower than those compared to Hypothesis 1, which may indicate managers with a bachelor's degree or higher are willing to consider promoting vendor-neutral information security certified professionals more so than they are vendor-specific information security certified professionals.

Hypothesis 4, Vendor-Neutral Group Statistics for Participants with Bachelor's Degree or Higher

	Highest level of education	*n*	*M*	*SD*	*SEM*
Within the next 6 months, how likely are you to promote or recommend for higher position a vendor-neutral (e.g. Certified Information Systems Security Professional, CISSP) certified Information Security Professional?	≥ 1.00	38	3.4737	1.30977	.21247
	< 1.00	6	3.0000	1.09545	.44721
would save time and resources.	≥ 1.00	33	5.0606	1.24848	.21733
	< 1.00	5	4.2000	1.92354	.86023
would make it easier to match candidate's skills with department needs.	≥ 1.00	33	5.1212	1.11124	.19344
	< 1.00	5	4.8000	1.78885	.80000
would decrease the risk of making a poor promotion decision.	≥ 1.00	33	4.5758	1.45839	.25387
	< 1.00	5	3.8000	2.04939	.91652
would result in candidate's ability to "hit the ground running."	≥ 1.00	33	4.6364	1.43218	.24931
	< 1.00	5	4.6000	1.51658	.67823
would ensure candidate has at least the base level of knowledge for promotion to higher rank.	≥ 1.00	33	5.0909	1.28364	.22345
	< 1.00	5	4.4000	1.67332	.74833
My managers	≥ 1.00	33	4.5758	1.19975	.20885
	< 1.00	5	4.4000	2.19089	.97980

Hypothesis 4, Vendor-Neutral Group Statistics for Participants with Bachelor's Degree or Higher (*continued*)

	Highest level of education	*n*	*M*	*SD*	*SEM*
My coworkers	≥ 1.00	33	4.7273	1.25680	.21878
	< 1.00	5	4.0000	2.23607	1.00000
Other hiring managers within my company	≥ 1.00	33	4.5758	1.32359	.23041
	< 1.00	5	4.4000	2.19089	.97980
Hiring managers outside my company	≥ 1.00	33	5.0303	1.23705	.21534
	< 1.00	5	4.2000	2.16795	.96954
I intend to use vendor-neutral IT security certification	≥ 1.00	33	4.5152	1.62252	.28244
	< 1.00	5	4.0000	2.23607	1.00000
To the extent possible, I would use vendor-neutral IT security certification	≥ 1.00	33	4.7879	1.51570	.26385
	< 1.00	5	5.2000	1.30384	.58310
Using vendor-neutral IT security certification in the promotion process is a _____ idea.	≥ 1.00	33	5.0909	1.10010	.19150
	< 1.00	5	4.6000	1.51658	.67823

Hypothesis 5

H5: Information security professionals who are vendor-neutral security certified are not perceived as more promotable by information security managers with 7 years of experience.

After independent samples t test was applied to the survey responses between those participants who had 7 years or more experience in the information technology/information security against those who had less experience. The null hypothesis was not rejected for all of the scale variables, with the one exception. The alternative hypothesis was accepted for the question that asked, "Within the next 6 months, how likely are you to promote or recommend for higher positions a vendor-neutral (e.g., Certified Information Systems Security Professional [CISSP]) certified Information Security Professional?" The significance level for this question was .019. Thus, information security managers with 7 years or more experience are likely to promote or recommend for promotion vendor-neutral security-certified professionals within the next 6 months.

Hypothesis 6

H2: Information security professionals who are vendor-neutral security certified are not perceived as more promotable by information security managers with a bachelor's degree or higher and 7 years of experience.

After independent samples t test was applied to the survey responses between those participants who had 7 years or more of IT/information security experience with a bachelor's degree or higher against those who did not meet this criteria. The *t* test resulted in the null Hypothesis 6 not being rejected, with one exception. With a significance level of .04, the alternative hypothesis is accepted for the question that asked, "Within the next 6 months how

likely are you to promote or recommend for higher positions a vendor-neutral (e.g., Certified Information Systems Security Professional, CISSP) certified Information Security Professional?"

Participants were asked different scale questions rating their perceptions of promoting vendor-neutral security-certified professionals using years of experience and bachelor's degree or higher as a grouping variable. The cut point was established between 6 and 7 years of experience. The significance levels of the scale variables were all above .05 and the value of 0 was contained in both confidence intervals. A significance level of .09 and .08 for the responses to "Other hiring managers within my company and I intend to use vendor-neutral IT security certification in the promotion assessment process for higher ranking positions" was the closet to accepting the alternative. Thus, information security managers with 7 years of more of IT/information security experience with a bachelor's degree or higher did not have a perception of vendor-neutral information security professionals as being more promotable.

DISCUSSION

The individual human capital investment of obtaining information security certifications for information security professionals seems to have significant implications. For example, the descriptive statistics in this study showed that within the information security field, vendor-specific information security professionals are more inclined to come from the technical side of the industry (i.e., networking or telecommunications), whereas vendor-neutral information security professionals are more inclined to come from the managerial side of the industry (i.e., information assurance/compliance). Participants also acknowledged they would prefer information security professionals to obtain vendor-neutral certifications over vendor-specific certifications. This may imply a broad knowledge of the information security industry is preferred over specialized disciplines, such as those associated with vendor-specific information security certifications.

Twenty-four of the participants surveyed acknowledged they had used both vendor-neutral and vendor-specific information security certifications in the promotion process in the past 3 years. This may also imply information security certification has an impact on the promotional process, along with other promotable credentials. Of the two groups—vendor-neutral or vendor-specific certified security professionals—vendor-neutral information security professionals were more likely to be promoted; however, the survey results did not suggest vendor-neutral information security professionals are perceived as more promotable overall than vendor-specific information security professionals.

CONCLUSION

Information security certification has an impact on the information technology/security industry. IT/information security certification complements other credentials that information security professionals may have and is a solid investment in individual human capital. Vendor-specific security certification may lead to an information security professional obtaining one of the top positions, such as Chief Technology Officer (CTO). Vendor-neutral security certification, on the other hand, may lead to obtaining the position of CISO. The results from this study suggested there may be two tracks: specialization or overall comprehensive positions within the information security industry. Thus, the perception of promotability may be biased within the two tracks.

This purpose of this study was to determine which of the two certifications—vendor-neutral or vendor-specific—enhances an information security professional's promotional status.

RECOMMENDATIONS FOR FUTURE RESEARCH

Having or obtaining certifications does not imply that a professional has the ability to apply the knowledge garnered from attaining a certification, but it can be a factor in the decision process of promotability. Obtaining an information security certification is an individual human capital investment, as most individuals obtain these types of certifications on their own through self-study, whether vendor-neutral or vendor-specific. This individual initiative may require a study of its own or could be used as an influential factor in the promotion process. This individual human capital initiative captures the essence of human capital theory that Becker (1962) and Schultz (1961) put forth. It is also uniquely supported by Turner's (1960) contest mobility norm. Individual investment in one's own self-development is generally accepted as a positive action for one to take. The uniqueness of obtaining an information security certification along with maintaining such certification through continual professional education credits shows individual motivation and self-discipline, which are just two of the required factors for promotion to higher ranks in most professions. This alone could serve as a flag when searching for promotable information security professionals. Of course, other factors, such as advanced degree, experience, and soft and hard skills (essentially the other components of human capital theory), will have a major influence on the promotional status of an IS professional.

Information security is early in its development as it pertains to the electronic context of today. Thus, through trial and error and with studies such as this one, the organization of this industry is beginning to take shape. The confidentiality, integrity, and availability of information are now on the wire, so to speak. This study showed a pattern of two different tracks of information security professionals within the industry where vendor-specific professionals are more inclined to work in networking and telecommunications and vendor-neutral professionals in information assurance and compliance. This study may be used in placing candidates in the right information security positions due to the type of information security certifications an IS professional has. Of course, it will also aid in not placing or promoting IS professionals in positions in which their skills are not predicated toward their being successful. The more efficient the information security organization becomes by placing and promoting its human resources to proper positions, the more mature the organization becomes.

Information security professionals who have both vendor-neutral and vendor-specific certifications along with significant experience could be candidates for upper managerial or executive positions. This study leans toward promoting vendor-neutral certified professionals (although not definitively), but it also acknowledges the specialization nature of vendor-specific certified professionals. Information security professionals who are both vendor-neutral and vendor-specific security certified may have an overall information security perspective. Information security professionals who are either vendor-neutral or vendor-specific may have a one-sided information security perspective. Having both vendor-neutral and vendor-specific certifications may aid promotion decisions for information security professionals at the upper managerial to executive-level positions.

Future research may include surveying human resource departments and personnel to examine which information security certifications are more apt to enhance an applicant's upward mobility. This in turn will help in placing qualified candidates in proper information security

positions, thus increasing a business's chances of recouping its return on investment sooner. Employers of specific industries are another area for future research. Employers would be beneficial in that they are able to see trends on a daily basis and can discern the skills needed to address the trends in their industry from an information security perspective.

Future study could also be directed at academia, for example, how closely aligned are curricula with information security certifications and its implications for promotability. Also, if curricula are aligned with information security certifications, how flexible are the curricula due to the changing nature of the IT industry as a whole? These variables could be quantitatively measured and provide valuable insight. Future study might also include other demographic credentials, such as the impact of advanced degrees with information security certifications versus information security certifications without advanced degrees, or professional experience without information security certifications versus professional experience with information security certifications—and their impact on the perception of promotability.

REFERENCES:

Ayoub, R. (2011). *The 2011 (ISC)^2 Global Information Security Workforce Study: A U.S. government C-level perspective.* Retrieved from https://www.isc2.org

Bastien, G., Nasseh, S., & Degu, C. A. (2003). *CCSP Cisco secure pix firewall advanced exam certification guide.* Indianapolis, IN: Cisco Press.

Bastien, G., Nasseh, S., & Degu, C. A. (2006). *CCSP SNRS exam certification guide.* Indianapolis, IN: Cisco Press.

Becker, G. S. (1962). Investment in human capital: A theoretical analysis. *The Journal of Political Economy, 70*(5), 9–49.

Boslaugh, S., & Watters, P. A. (2008). *Statistics in a nutshell: A desktop quick reference.* Sebastopol, CA: O'Reilly.

BradReese.com. (2011). *Worldwide CCIE count.* Retrieved from http://bradreese.com /worldwide-ccie-count.htm

Brookshire, R. G. (2001). Information technology certification: Is this your mission? *Information Technology, Learning, and Performance Journal, 18*(2), 1–2.

Bureau of Labor Statistics. (2009). *Occupational outlook handbook, 2010–11 editions: Computer network, systems, and database administrators.* Retrieved from http:// www.bls.gov/oco/ocos305.htm

BusinessDictionary.com. (2010). *Certified public accountant definition.* Retrieved from http://www.businessdictionary.com/definition/assurance.html

Cegielski, C. G. (2004). Who values technology certification? *Communications of the ACM, 47*(10), 103–105.

Cisco. (n.d.). *CCNP security*. Retrieved from http://www.cisco.com/web/learning/le3/le2 /le37/le9/learning_certification_type_home.html

Clapp, J. E. (2000). *Dictionary of the law.* New York, NY: Random House.

International Information Systems Security Certification Consortium. (2011). *History of (ISC)^2*. Retrieved from https://www.isc2.org/isc2-history.aspx

CompTIA. (2011). *CompTIA Network+*. Retrieved from http://certification.comptia.org /getCertified/certifications/network.aspx

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed method approaches.* Thousand Oaks, CA: Sage.

Department of Homeland Security. (2008). *Information technology (IT) security essential body of knowledge (EBK): A competency and functional framework for IT security workforce development.* Retrieved from http://www.us-cert.gov /ITSecurityEBK/EBK2008.pdf

Gupta, U. (2010). *Top 5 IT security certifications for 2011 CISSP, CISM, CEH training & certification.* Retrieved from http://secureninja.com/news/3/Top-5-IT-Security -Certifications-for-2011-CISSP-CISM-CEH-training-certification/

Harris, S. (2005). *All in one CISSP exam guide* (3rd ed.). Emeryville, CA: McGraw-Hill/Osborne.

Heise, J. M. (2009). *Professional certifications versus skills: A study of professional certifications from the perspective of the certified and their employers.* Retrieved from ProQuest database.

Hitchcock, L. E. (2007). *Industry certification and academic degrees: Complementary, or poles apart?* Retrieved from http://portal.acm.org/citation.cfm?id=1235023

Hunsinger, D. S. (2005). *Predicting the intention of managers to use IT certification in the hiring process*. Retrieved from ProQuest database.

IT Governance Institute. (2008). *Information security governance: Guidance for information security managers.* Retrieved from www.itgi.org

Information Systems Audit and Control Association. (2008). *Information Security Career Progression Survey results.* Retrieved from http://www.isaca.org

International Information Systems Security Certification Consortium. (2011). *History of (ISC)*^{2}. Retrieved from https://www.isc2.org/isc2-history.aspx

Marshall, G. (1998). *Human-capital theory: A dictionary of sociology.* Retrieved from http://www.encyclopedia.com/doc/1O88-Humancapitaltheory.html

Randall, M. H., & Zirkle, C. J. (2005). Information technology student-based certification in formal education settings: Who benefits and what is needed. *Information Technology Education—SIGITE, 4,* 287–306

Schneider, L. (2011). *Top 15 highest paying certifications in the technology industry.* Retrieved from http://jobsearchtech.about.com/od/educationfortechcareers/tp /HighestCerts.htm

Schultz, T. W. (1961). Investment in human capital. *The American Economic Review, 51*(1), 1–17.

Shore, J. (2002). *Why certification? The applicability of IT certifications to college and university curricula.* Retrieved from http://www.db2-community.org/downloads /WhyCertification.pdf

Shostack, A., & Stewart, A. (2008). *The new school of information security.* Boston, MA: Pearson.

Trinckes, J. J., Jr. (2010). *The executive MBA in information security.* Boca Raton, FL: CRC Press.

Turner, R. H. (1960). Sponsored and contest mobility and the school system. *American Sociological Review, 25*(6), 855–867.