Information Security Employment: An Empirical Study

JAMES A. NELSON & DARLENE NELSON
Department of Accounting & Information Systems
New Mexico State University
UNITED STATES OF AMERICA
&
NICHOLAS J. NELSON
Cornell University
UNITED STATES OF AMERICA
jnelson@nmsu.edu

Abstract: - A popular internet employment database was used to try and provide structure to the classification of Information Security employment. Keywords for popular information security job titles and certifications were used to search the Monster.com database. Results indicate that educational requirements, experience, and career level vary by certificate and job title. The CISM certificate appears to be the most acceptable measure of job qualification.

Key-words: - Information Security, certification, employment, SABSA, CISM, CISA, CISSP

1 Introduction

The profession of IT security is evolving, un-focused, and ill-defined. Necessary skill sets, educational requirements, and experience are non-standard and un-regulated. We don't have mandatory licensing authorities or government oversight of the profession as in standard in other professions such as medicine or accounting. In medicine, the goal of the profession is the prevention and remediation of risks to health, just as in IT security our goal is the prevention and remediation of risks to information. Medicine requires many technicians with relatively low skill levels and entrance requirements and progresses to highly regulated and stringent educational, internship, and licensing requirements. Oversight bodies have complete control over who can and cannot perform certain duties and can withdraw the right to practice from individuals for performance, ethical, and personal reasons. Most job descriptions are defined by state regulatory boards and state law. Individuals that practice outside of their licensed limits can be subject to fines and imprisonment. Medicine has pink ladies, candy stripers, orderlies, LPNs, RNs, PAs, pharmacists, MDs, specialty board certified certificates, chiefs of staff, administrators, and more. The extremes of skill and power tend to have looser requirements and regulations. Candy stripers and hospital administrators are not as regulated as the majority of the medical profession.

IT security is another story, with little or no definition, and no standards or enforceable employment authorities. There are no state laws or regulations as to who can tune firewalls or monitor audit logs. If an IT security worker changes a firewall setting, she may get fired, but she won't be prosecuted for practicing security without a license. Who can tune a firewall? Who should? Should there be licensing boards that mandate who can perform IT security functions. What are IT security functions?

2 Problem Formulation

What skills, educational levels, certificates and other job requirements exist for IT security in the absence of state regulation? We can broadly identify IT security positions on scales of technical to managerial, operational to policy, short to long term decision making, low to high educational requirements, and possession of myriads of available certificates.

Our study is an attempt to get a "snapshot" of the profession by empirically measuring the state of the profession by statistically examining the IT security job requirements listed on a major Internet based employment service. We looked at all jobs IT security jobs advertised on one day on the popular job search site Monster.com. We did not use industry specific job sites such as Dice.com because we wanted to include employers that may not be aware of this more specialized site. Monster gives a broader view of the profession, because it attracts a wider group of employers.

3 Problem Solution

We searched Monster with a variety of terms that are common in the IT security filed and examined the results using Monster's scales of Career Level, Years of

Experience, and Education Level. A search for the keywords Information Security maxed out Monster's statistical display for any category with more than 5,000 hits. Figure 1 shows that for the 7,000 advertised IS positions the modal values were that 61% of all jobs required a Bachelor's degree, 37% asked for 2 to 5 years of experience, and 47% were for experienced non-managerial personnel. Table 1 describes the conversion of the data for the three scales of Career Level, Years of Experience, and Education Level to a High, Moderate, Low classification.

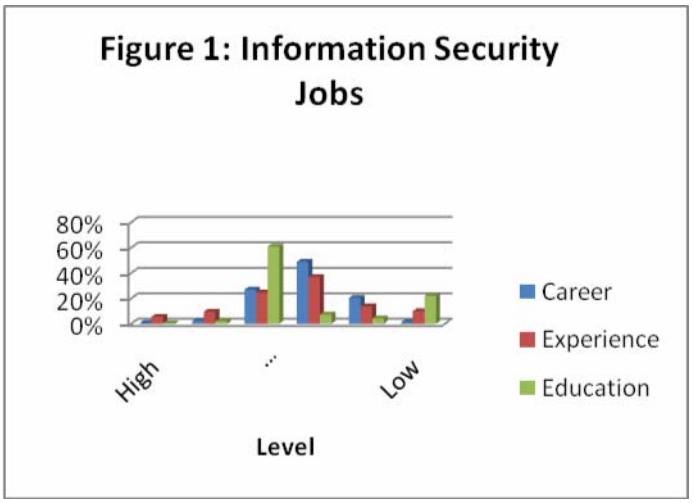
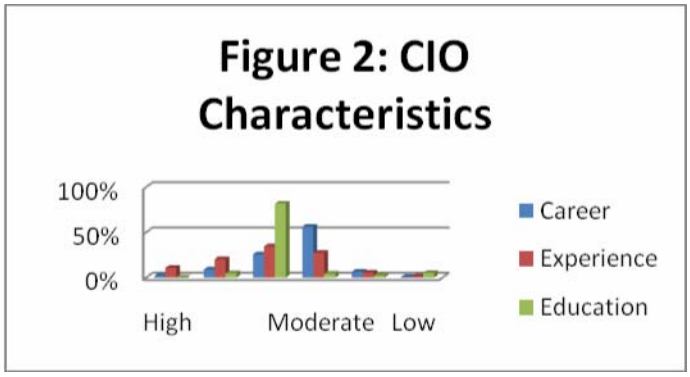


Table 1

Monster Category Ratings

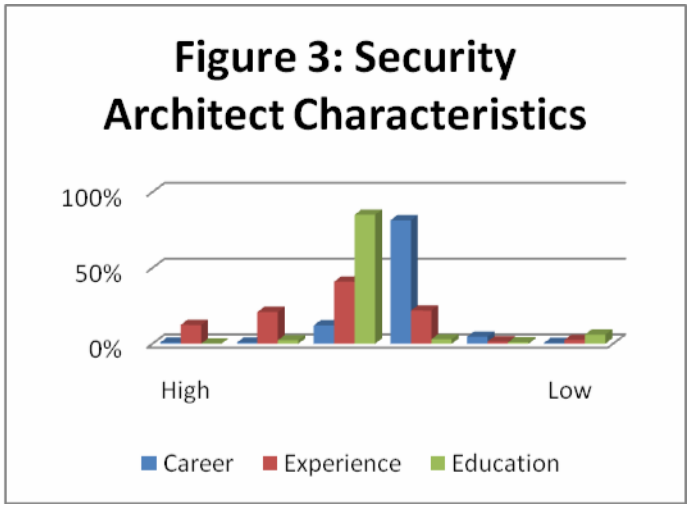
	Career Level	Years of Experience	Education Level
High	Senior Executive	">10"	PhD
	Executive	"7 - 10"	MS/MA/MBA
	Manager	"5 - 7"	BS/BA
	Experienced N MGT	"2 - 5"	Associates + Vocational
	Entry	"1 -2"	Some College
Low	Student	"<1"	High School

Refining the Monster search by using the keyword CIO, a common acronym for Chief Information Officer, resulted in 863 hits. As can be seen in Figure 2, 82% of CIO positions require a Bachelor's degree, with 35% requiring 5 to 7 years of experience and surprisingly, 56% were for a non-managerial position. Monster does not post by company size and this may account for very small organizations asking for a non-managerial CIO.



Searching for CISO (Chief Information Security Officer) resulted in only 20 hits. A review of the job descriptions for CISO showed that many of the 20 positions were not computer related such as sales and finance jobs. Another category that was not productive on Monster was CSO or Chief Security Officer. The advertised positions were primarily for physical security and safety.

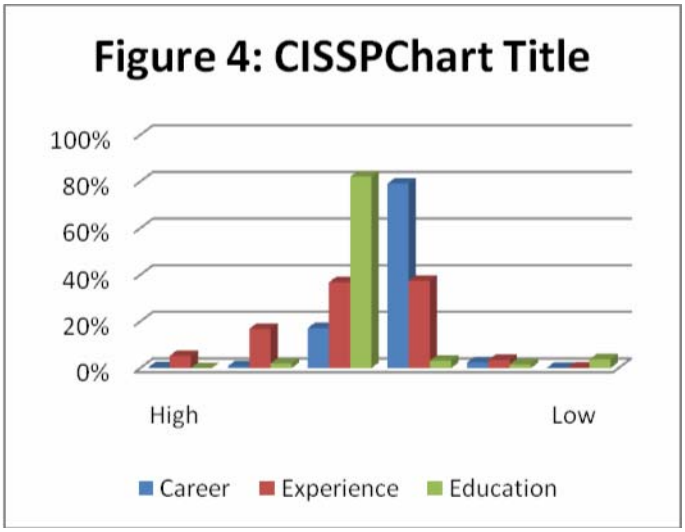
We then searched for higher level positions by using the keyword Security Architect and found that most of the 1557 hits were for information security architects. Architect has become a hot phrase in recent years for the general field of analysis and design. More variability and higher overall experience requirements are seen in Figure3 with 75% requiring more than 5 years of experience. Educational requirements are also higher with 85% requiring a Bachelor's degree. Interestingly the Career Level for Security Architects is 81% non-managerial. Perhaps they are expected to act alone while they architect security.



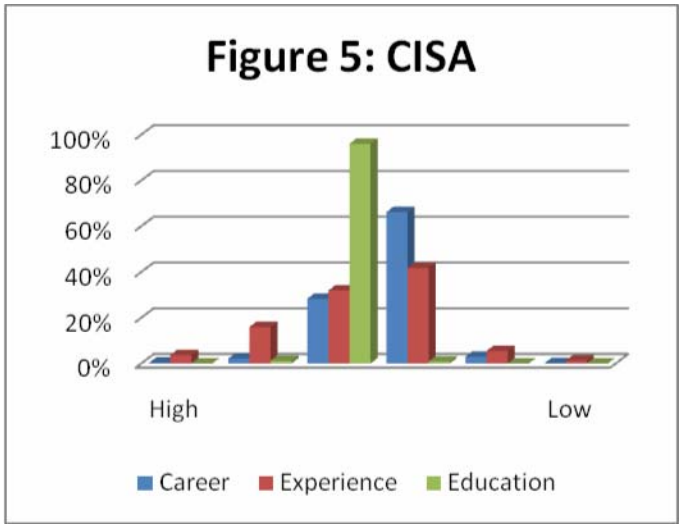
Our search for Information Security resulted in only 2.5% of the positions listing "Certificate" as an Educational requirement. With the number of IS certificate holders for CISSP (over 60,000), CISA (50,000+), and the higher level CISM (6,000+) in the

10s of thousands, it would seem that the keyword Certificate would be have many more hits. Perhaps the acronyms of the certificates would yield more information.

CISSP (Certified Information Systems Security Professional) is the most popular mid to high level information security certification. Our Monster search resulted in 1249 jobs with CISSP in the description. Of these positions which list the CISSP certificate as a requirement, only 7% use the keyword Certificate in the job description. From Figure 4 we can see that Educational requirements are very high with 84% requiring a Bachelor's degree or higher and almost 60% requiring 5 or more years of experience. Again most of the CISSP positions are listed as non-managerial (> 80%).

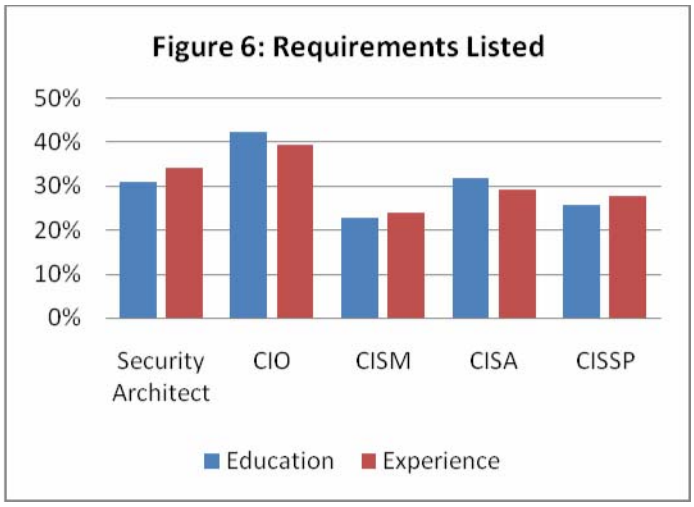


The Certified Information Systems Auditor or CISA is often included as an Information Security professional and our Monster search found 1117 positions available in the spring of 2008. Very high educational requirements were found for CISA, with 97% expecting a Bachelor's degree or higher. Experience requirements were also high, with over 50% expecting 5 or more years. A Managerial Career Level was listed for 28% of the positions.



As a high level certification for information security, the Certified Information Security Manager (CISM) implies that certificate holders are also managers. Our study found that the CISM is a rarer certification with only 288 listings as compared to the over 1,000 each for CISA and CISSP. Although the CISM implies a management position, only 24% of the listed positions were for management, while 30% of CISA were management and 18% of CISSP jobs were management level.

The CISM appears to be the certificate that overrides experience and educational requirements more than other certificates and titles. Only 23% of the CISM listed any educational requirement (Figure 6), whereas 42% of CIO jobs listed any educational requirement. Experience was also not listed as often for CISM holders, with 24% stating experience requirements, while 39% of CIO positions listing any experience qualifications. The CISM appears to be the most "respected" in that listings do not require specific education or job requirements as do other certifications.



Perhaps the highest level certification is the SABSA Certified Security Architect. This certification focuses on security as a business attribute independent of any hardware, software, policy or compliance standard. SABSA can incorporate any of the international standards such as ITIL or COBIT and encompasses the entire information world. Our Monster search for SABSA resulted in no hits. It may be that SABSA is at such a high level that employers and SABSA practitioners don't use Monster for job placement. As SABSA is relatively rare in North America with only a few hundred certificate holders, we may find more results in European databases.

4 Conclusion

Our research has identified rough educational, experience and career levels for the field of information security; however our study leaves us with little structure. There is a movement under study by the US government to try and certify university programs, but the variety and content of information systems education is as broad as the job requirements found in our study.

Further research will include other online employment databases that will allow us to refine our view of the information security field. As the information security world changes, job requirements including education, experience and certificate value will change. We are currently assessing a longitudinal study of information security employment that addresses these questions.