# Anatomy of the Information Security Workforce

**JinKyu Lee**
*Oklahoma State University*

**Sharmistha Bagchi-Sen, H. Raghav Rao, and Shambhu J. Upadhyaya**
*University at Buffalo – SUNY*

> ***Survey results indicate that the information security workforce, one of the fastest growing subgroups in IT, is a unique professional niche with distinctive task responsibilities, job market conditions, and training needs.***

A recent IT job projection report named 30 IT job titles that have an average salary ranging in the six figures.[1] Among these, six are security-related titles, including chief security officer (US$150,000), data security analyst (US$104,000), systems security administrator (US$103,500), network security administrator (US$103,000), senior/entry-level IT auditor (US$114,750/US$102,750), and business continuity analyst (US$100,250). Why are these jobs suddenly grabbing the eyes and ears of recruiters, managers, and prospective IT professionals? What are this profession's distinctive characteristics?

Although much prior research has focused on the IT workforce, researchers have hardly explored the cybersecurity subset of IT. To address this gap, we conducted a research study to understand the information security workforce's unique characteristics and environment**.** Our research found that this particular workforce requires a distinctive skill set and thus should be considered separately from the general IT workforce. Our work explores issues such as tasks specific to information security professionals, job-market conditions, and necessary training. This article also provides an in-depth understanding of information security careers such as job responsibilities at various professional-managerial levels as well as motivations for entering this niche and employee turnover.

Given the demand for the information security workforce, this survey offers useful insight to various stakeholders, including prospective information security professionals, employers, educational institutions, and industry steering (government) authorities. Specifically, our study results should help companies, prospective information security professionals, and educational institutions alike understand the issues pertaining to this labor niche and fulfill the increasing labor demands.

## Prior Research and Study Objectives

To get an understanding of the different issues that we needed to consider[2] and to show how we framed our cybersecurity workforce study, we begin by reviewing the considerable research in the IT workforce area.[3–17] Table 1 is a snapshot of key prior literature in the area. We classified the prior literature as dealing with skill set, education and curriculum issues, career motivations, or turnover issues. We then identified and classified the information security workforce's current skills and examined their educational backgrounds to understand the supply side; we utilized many of these concepts in our study.

**Table 1. Prior IT workforce research.**

| Topic | Sample findings from prior research | Research methods |
|---|---|---|
| **Skill sets**<br>Business and interpersonal skills | Practitioners place significant importance on people skills, technical skills,[3] and business knowledge.[4] IS professionals are required to cross | Brainstorming sessions with CIOs, vendors, and consultants; telephonic interviews; open forums; and mail-in surveys.[3,5] |

This is a pre-print version of Lee, J., Bagchi-Sen, S., Rao, H. R., and Upadhyaya, S. J. (forthcoming) "The Anatomy of Information Security Workforce," *IEEE IT Professional*

|  |  |  |
|---|---|---|
|  | political, organization, and national boundaries to solve problems.[6] Requires ability to carry out enterprise-wide tasks and projects and deal with issues such as competitive advantage and technology usefulness.<br><br>IS professionals need a strong contextual orientation, including interpersonal skills to work with end users and abilities to articulate, present, and communicate ideas to developers and end users.[7] |  |
| Technical skills | The most important skills include analysis and design, programming, environment, and application and language skills. | Field study[8] |
| **IS education and curriculum** | The development process: determining goals, developing a plan of action, and determining a curriculum consisting of new computer science and interdisciplinary synthesis courses.<br>Emphasis on career-driven IS programs.<br>The design of more relevant IS programs[10] will require cooperative efforts and multidisciplinary approaches that cut across university departments.[11–14] | Report[9]<br>Open forums, focus group discussions, and mail-in survey[3] |
| **Career motivations** | Analysts and programmers are motivated by the work, opportunity for achievement, opportunity for advancement, pay and benefits, recognition, increased responsibility, technical supervision, interpersonal relations, job security, work conditions, and company policies. Nonsalary incentives (promotion, recognition from others, and personal growth and development) were also important. | Survey[15] |
| **Turnover** | Several factors were negatively correlated with turnover intentions: age, organizational level, organizational tenure, job tenure, and number of years in the computer field, commitment, job satisfaction, | Survey[16] |

www.manaraa.com

| | satisfaction with progress, promotion, pay, status, and project.[17] Education and career opportunities were factors positively correlated with turnover intentions.<br><br>Project leaders are more likely to leave the organization, and IS managers are less likely. | |
|---|---|---|

Our research study aims to understand the information security workforce's characteristics and environment in relation to the four issues focused on in previous work. The past IT workforce research shows that career motivation and turnover are at the center of interest in the industry, especially when there's a gap between labor supply and demand. Our research attempts to identify major motivators for IT professionals to move in and out of the information security field.

## Survey

For our survey, we used a Web-based questionnaire to collect data from North American information security and nonsecurity IT professionals. Because a gray area exists between such IT professions, we used a self-reported response to categorize survey participants into the two groups, rather than using their affiliation with the data sources. (That is, we asked survey participants if they considered themselves IT professionals specialized in information security or another area.) The information security sample group mainly consisted of International Information Systems Security Certification Consortium $(ISC)^2$ members in the US and Canada, including but not limited to $(ISC)^2$ certified information security professionals. $(ISC)^2$ is a nonprofit international organization dedicated to training and certifying information security professionals worldwide. In addition, we invited female information security professional members from the Syster of Anita Borg Institute and attendees of the Grace Hopper Women-in-IT Conference to participate in the survey to minimize the gender and specialty asymmetries in the data. (We excluded these subgroups from some analyses [such as gender composition], however, to avoid biased results.) Thus, we consider the subjects in our sample groups to be "key informants" of our target population: the current and future IT security professionals based in North America.[18]

Some of the concepts we measured in the survey include information security tasks (extracted from the Certified Information Systems Security Professional Common Body of Knowledge) and required skills (which we adapted from the skill lists at http://ualr.edu/itreport/) for various information security jobs, job-market conditions, turnover intentions, formal education, and previous job experience. (Measurement items are available from the contact author [Jinkyu Lee] upon request.) The survey didn't include any questions related to the research partners' products or services, which was specified in survey invitation emails and Web site popup messages. We collected the data on a third-party survey site that only we were allowed to access. Survey participation was voluntary, which might have introduced some nonresponse biases.[19] For example, IT professionals with a high level of privacy concerns (such as those worried about IP addresses sent to the survey server) were less likely to participate, although we didn't record any personally identifiable information. Nevertheless, we tried to make the study objectives on the call for survey participation as neutral as possible to minimize the negative influence of such biases on the analysis results.

### About the Responders

The survey yielded 215 responses with 171 usable responses from the $(ISC)^2$ sample group, and 65 responses with 41 usable responses from the women-focused sample groups. The dropped cases included incomplete responses, redundant responses from the same or adjacent IP addresses (to assure response independence), and obviously insincere responses (such as extremely low variance or patterned responses). After the data cleaning, the data set included responses from 177 or more unique zip code areas, based on the respondents' primary workplace zip codes. (Eighteen responders didn't provide their zip codes.)

Among the 212 total usable cases, 165 respondents (77.8 percent) considered themselves information security professionals, and the other 47 (22.2 percent) identified themselves as IT professionals outside the information security field. Due to the limited data sources and sample size, the results of the statistical analysis possibly include some biases. In particular, the large number of responses from (ISC)[2] members might have resulted in a nonsecurity group that's more interested or involved in information security tasks than the typical IT workforce. Also, combining all nonsecurity IT professionals into a single group could cancel out some distinctive characteristics of different specialty areas within the group. Nevertheless, these issues shouldn't weaken the findings about between-group differences.

The respondents ranged from 22 to 63 years old, with an average age of 41.5 years. Their average work experience in the IT field was 15.4 years, and the information security subgroup had 9.3 years of average work experience in the field. They had been in their current position for an average of 3.4 years, and their approximate annual salary ranged from US$20,000 to $200,000, with an average of $86,000. The proportion of female respondents from the (ISC)[2] data source is strikingly small. Only 14 out of 171 (8.4 percent) in the (ISC)[2] sample are female. (Four chose not to identify their gender.) Only 10 out of 38 (26.3 percent) female respondents in the women-focused sample groups identified themselves as an information security professional. This extremely small footprint requires further investigation with respect to gender asymmetry in this specific workforce.

## A Workforce Comparison

Does the information security workforce have a distinctive characteristic that sets it apart from the rest of the IT workforce? If they do differ, then we'll need to look at different ways to nurture these professionals. Our survey asked the IT professionals in both the information security and nonsecurity areas about the skills and knowledge required to fulfill their current job responsibilities. We first compared the two groups' responses to identify any distinctive characteristics. The results show that the information security area requires significantly higher IT and business skills than the general IT area. We also examined requirements for specific skills in the overall IT, business, and soft skills categories in the survey. Table 2 compares the specific skills required by both sets of professionals.

**Table 2. Skill and knowledge requirements comparison.**

| More require of information security | No difference |
| --- | --- |
| **IT skills and knowledge** (Mean: 6.32 versus 5.81, $F = 9.779$**) | |
| Hardware equipment (4.94 versus 4.12**) Software tools (5.26 versus 4.51**) Operating systems and server software (5.48 versus 4.86**) | Programming languages Software development tools |
| **Business skills and knowledge** (Mean: 5.51 versus 4.70, $F = 11.921$ ***) | |
| Business processes (4.47 versus 3.79*) Strategies and planning (5.32 versus 4.58**) Law and legal systems and processes (4.45 versus 2.56***) | Business application software |
| | **Soft skills** (Mean: 5.69 versus 5.26, $F = 3.216$) |
| Interpersonal relationship building and management (5.85 versus 5.21**) Communication and presentation of facts, opinions, and | Research, analysis, and novel idea or solution generation Intuitive and heuristic decision making |

| ideas (6.20 versus 5.74*) | Time and stress management |
| | Leadership and teamwork |

Mean difference significant at * $p \leq .05$, ** $p \leq .01$, *** $p \leq .001$

Further analyses identified noticeable differences in skill-set requirements among different positions—that is, management position versus nonmanagement employees or consultants. (We excluded from this analysis responses that indicated Faculty/Teacher/Trainer, Student, and Other roles [$n = 17$].) We used a general linear model (GLM) with several post hoc comparison techniques to pinpoint the location of the differences among these subgroups. The results suggest a significant difference between the information security and nonsecurity IT areas in the level of IT skill requirements, but the requirements for business and soft skills are contingent more on the managerial roles within each area, rather than across the whole career spectrum.

Figure 1 shows the subgroup differences of the three overall skill types. These profile plots indicate that high-level managers in the information security area need to keep their technical skills high, whereas the requirement is relatively low for the corresponding managerial level in nonsecurity IT areas. Business and soft skill requirements generally increase as the managerial level goes up in both areas, although the nonmanagement employee and consultant/auditor groups in the information security area seem to require more business skills than their nonsecurity counterparts.
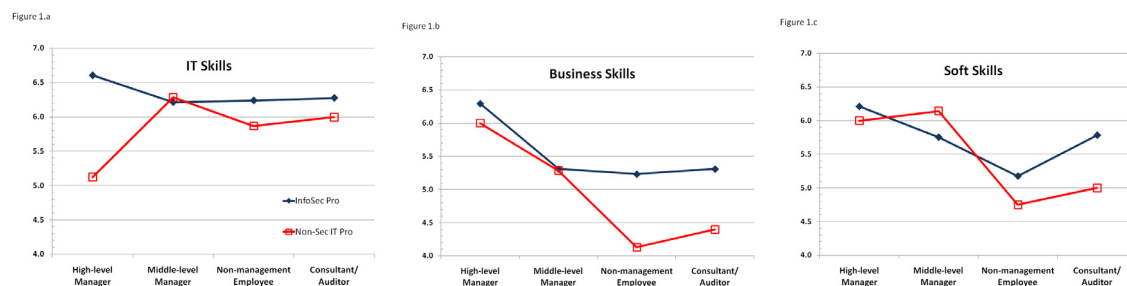


*Figure 1. Information security versus nonsecurity skill-set requirements by role group: (a) IT, (b) business, and (c) soft skills. Estimated marginal means plotted due to the asymmetric group sizes.*

## Job Tasks

To determine information security professionals' specific job duties, we categorized them into four clusters based on their security-task responsibilities, as Figure 2 shows. After closely analyzing the job responsibilities, we labeled the clusters as frontliners, directors, developers, and soldiers in the trenches. The cluster analysis revealed that information security professionals are categorized by the level of involvement in information security tasks in general, as opposed to the area of specialty. The *frontliners* represent the professionals who are highly involved in most information security tasks. They assume stronger responsibilities for almost every security task examined, compared to the other groups, but they particularly focus on

- designing and implementing access controls,
- monitoring user access and identifying security events,
- managing security equipments and software, and
- recovering business operations in response to security events, among others.

This group also ensures systems users comply with security policies, collects information from the information security community, and interacts with information security product and service vendors or customers.
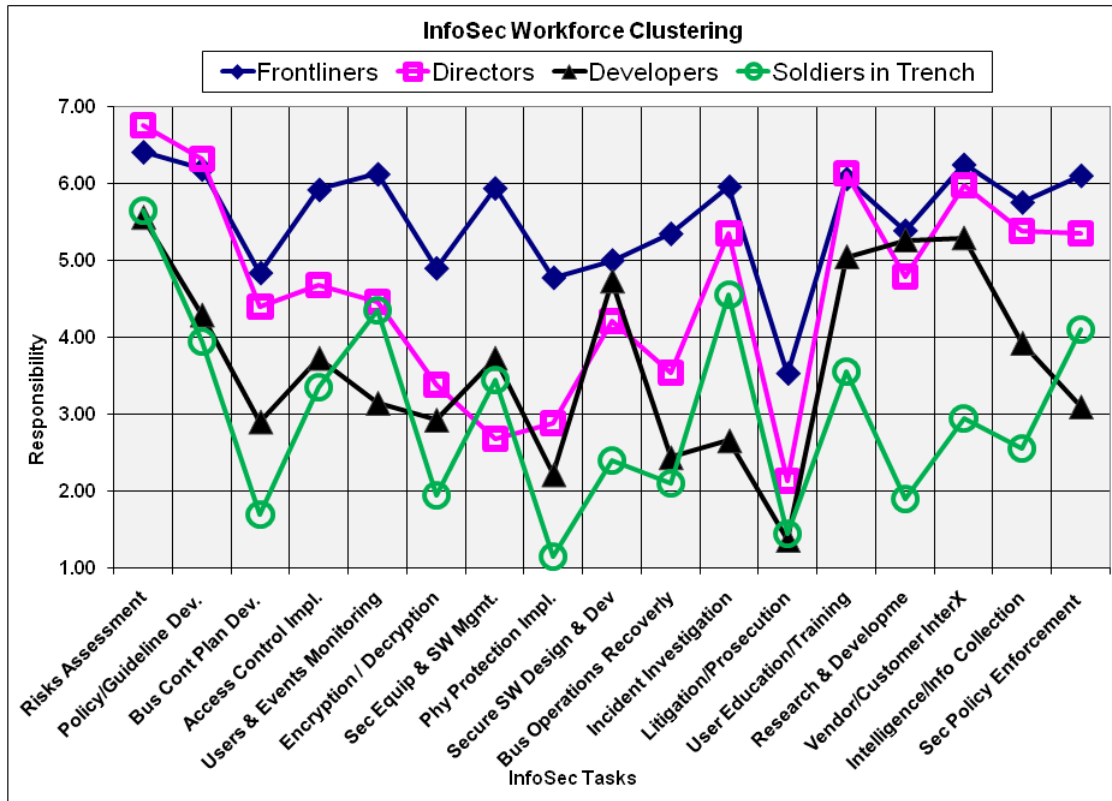
Figure 2



*Figure 2. Categorization of information security workforce. The clustering shows which security-task responsibilities are most relevant for the four types of professionals: frontliners, directors, developers, and soldiers in the trenches.*

*Directors* are less responsible than the frontliners but more responsible than the other two for most information security tasks. Interestingly, directors tend to be less associated with the tasks that frontliners are focused on (such as access control, user/event monitoring, security hardware and software management, and business operations recovery).

*Developers* show the most distinctive pattern of information security task responsibilities. Unlike the others, this group is primarily responsible for R&D and less concerned with operational support, such as user and event monitoring, incident investigation, and policy enforcement. Developers are also responsible for security in software design and development, user security education and training, and interactions with security vendors and customers.

The last group, *soldiers in the trenches*, shows somewhat limited security task responsibilities. They mainly focus on operational-level security tasks such as user and event monitoring, access control, incident investigation, policy enforcement, and security hardware and software management. This cluster is less involved in planning, development, and interpersonal activities (with users, vendors, customers, and the community).

Figure 2 also reveals that some tasks are generally more or less relevant to the information security workforce as a whole. The survey results revealed that risk assessment, security vendor and customer relation, user education and training, security policy and guideline development are core information security tasks, regardless of the cluster. On the other hand, litigation and prosecution, physical security, data encryption/decryption, and business continuity planning are at the periphery. Table 3 presents the average relevance of the surveyed tasks to the information security professionals' job responsibilities in descending order.

**Table 3. Information security task relevance.**

| Information security task* | Average relevance |
|---|---|
| 1. Assess security risks of information assets. | 6.13 |
| 2. Interact with information security product and service vendors or customers. | 5.47 |
| 3. Educate and train users regarding information security. | 5.38 |
| 4. Develop organizational information security policies and guidelines. | 5.35 |
| 5. R&D (secure network, cryptology, security devices, and so on). | 4.84 |
| 6. Ensure all system users comply with the organizational information security policy. | 4.77 |
| 7. Intelligence and information gathering in the information security community. | 4.75 |
| 8. Design and implement access controls. | 4.6 |
| 9. Audit and monitor user access and identify security events. | 4.6 |
| 10. Investigate information security incidents. | 4.6 |
| 11. Enforce information security in software design and development. | 4.27 |
| 12. Install and manage security equipments and software. | 4.13 |
| 13. Develop the business continuity plan (BCP). | 3.76 |
| 14. Encrypt and decrypt classified information. | 3.6 |
| 15. Recover business operations in response to security events. | 3.49 |
| 16. Implement physical protection for information system resources. | 3.05 |
| 17. Prosecute unlawful users or information system abusers. | 2.28 |

\* Tasks are sorted by relevance to job responsibility: 1 unrelated, 4 moderately related, 7 very closely related.

## Education and Training

Where do information security professionals learn the skills and knowledge required for their jobs? Is there any academic qualification required for the career? Our survey found interesting patterns of formal education among different age groups in the information security workforce. When we divided the respondents into three equivalently sized groups—namely, younger (under 38), middle (38 to 45), and older (over 45) age groups—the middle-age group has a significantly higher proportion of people with lower than a bachelor's degree, whereas the older-age group has a significantly higher proportion of people with graduate degrees. People with bachelor's degrees dominate the younger-age group. In terms of the major or concentration in the respondents' highest degrees, we encoded the areas into five disciplines: information assurance (IA), computer science (CS), MIS/information science (MIS), management (MGT), and other. CS dominates the younger- and middle-age groups, but MIS shows a dramatic increase and ties with CS in the older-age group. MGT majors are also popular in the younger-age group. The newer IA major is also found in younger- and older-age groups but not in the middle-age group. When we considered each age group separately, the CS bachelor's dominates the younger, followed by MGT and "other" bachelor degrees; in the middle-age group, other diplomas and CS bachelor's dominate. The older-age group is dominated by MIS graduate degrees, followed by other bachelor's, CS bachelor's, and CS graduate degrees.

Do different roles require different levels of formal education? A (role group × education level) chi-square test didn't support such an argument. In terms of majors, high-level managers have a relatively high proportion of MGT majors and low proportion of other majors, but the differences aren't statistically significant. Furthermore, a (role group × age group) chi-square test's results suggest that the proportions of the age groups are constant across all role groups, which means there are many young high-level managers and many older nonmanagement employees.

On further analysis, we discovered a couple of other interesting findings; from (role × education level × age), we see that many high-level managers in the middle-age group have low formal education, which might indicate that they were more like veterans-in-the-trenches types who learned their skills and

knowledge on the job. This applies to the younger-age group where high-level managers have the lowest formal education level. In contrast, the high-level managers and consultants/auditors in the older-age group have high education levels, and there are as many graduate degree holders as bachelor's degree holders among the nonmanagement employees in the older-age group. We derived two assumptions from these patterns.

First, in the past, the importance of formal education wasn't as strong as it is today, partly because educational institutions hadn't built enough capacity to train the information security workforce. However, the recent investment in information security education has successfully substantiated the educational capacity of many schools, and most young information security professionals start their career with a bachelor's degree.

Second, after a certain period in the field, information security professionals require additional formal education. Such re-education often occurs between 38 and 45 years of age, and the most popular choice seems to be a graduate degree program that delivers a mixture of technical and managerial skills and knowledge (such as a master's degree in MIS with information security components).

## Professional Environment Transformation

Do potential information security professionals need to worry about unfavorable transformations in the job market, external and internal, that might render them uncompetitive or the career field unattractive? The answer is "Not much!" We asked nonmanagerial information security professionals to indicate how favorable the job position and market conditions were at the beginning of their information security career. (We excluded the managerial-level information security workforce in this analysis, with the assumption that job-market conditions for managerial and nonmanagerial positions aren't the same.) We further divided this nonmanagerial group (which included 89 nonmanagerial employees, consultants/auditors, and others) into three generations based on their work experience: *new generation* (started an information security career within the past five years), *midgeneration* (entered the field five to 10 years ago), and *first generation* (entered the field more than 10 years ago).

We measured the following conditions: job-market demand; salary level; long-term job security; gender equity; prospect for career advancement; job image in society; work-hour flexibility; fit with personal interest, lifestyle, previous knowledge, and family duty; and proximity to home. Among the 12 conditions, job security was the only one that showed a statistically significant change. Nevertheless, the big improvement in job security occurred between the midgeneration whose job security conditions had deteriorated from the first generation and the new generation. Coincidently, information security professionals also reported a significantly higher level of perceived job security (at present) than nonsecurity IT professionals.

## Job Transitions and Turnover

It's important to understand what encourages prospective IT professionals to decide on an information security career and what makes them move, from both the industry's perspective and an employer's perspective. Table 4 lists the three most favorable and unfavorable conditions of the information security job, compared to other positions that were available to our survey respondents.

**Table 4. Three most (un)favorable conditions.**

|  | New generation | Midgeneration | First generation |
|---|---|---|---|
| **Most favorable conditions** |  |  |  |
| Fit with personal area of interest | 1 (tie) | 1 | 2 |
| Market demand for the profession | 1 (tie) | 2 |  |
| Fit with previous knowledge |  | 3 | 1 |
| **Most unfavorable conditions** |  |  |  |
| Equal opportunity for both genders | 1 | 3 | 1 |

| Flexibility of work hours | 3 | 1 | |
|---|---|---|---|
| Fit with family duty | 1 | | 3 |

The list suggests that gender inequity, flexible work hours, and family duty weren't concerns when professionals were deciding to join the information security field. Nevertheless, these unfavorable issues could have repelled some others who might have considered an information security career. In addition to the situational conditions, the survey also captured up to four previous positions of the 165 professionals, yielding a total of 527 primary reasons for job change. Figure 3a gives the primary reasons that current information security professionals move from a nonsecurity area (such as general IT or non-IT) into the field, if such a cross-area move occurred within the last three moves ($N = 112$). This chart shows that the favorable conditions we've mentioned have positive effects on promoting information security careers. For example, personal interest in information security, together with previous knowledge, would have projected the new career as a learning opportunity and made the new job more enjoyable. High market demand would have resulted in a higher salary level and better working environment.
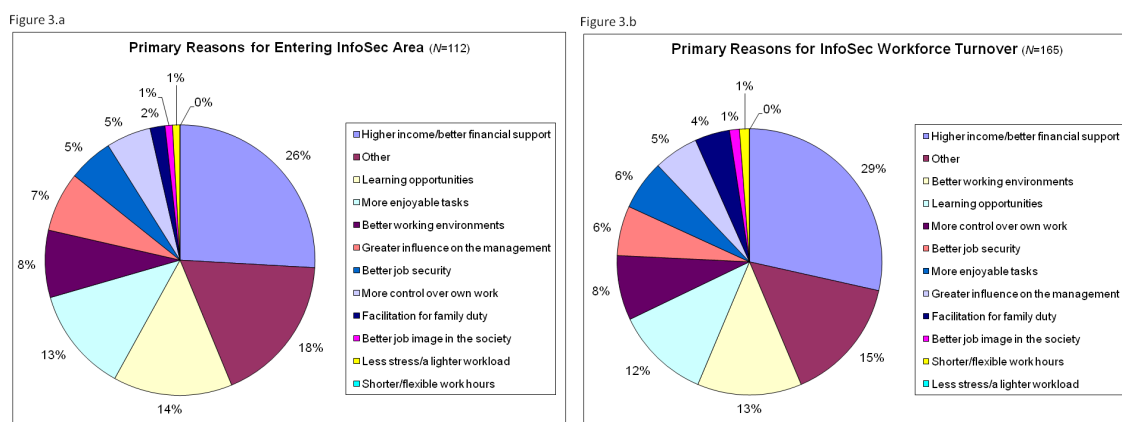


*Figure 3. Primary reasons for workforce changes: (a) why current information security professionals entered the field (N = 112) and (b) turnover trends within the field (N = 165).*

The survey also shows an extremely low-level of career turnover intention but polarized employer turnover intention—that is, professionals aren't likely to leave the information security field, but more than half are ready to move to a new employer. Figure 3b summarizes the reasons for 165 job changes within the information security area. Again, salary, working conditions, and learning opportunity are the dominant reasons, while enjoyable tasks aren't a major reason for within-field mobility.

As one of the first studies to explore the information security workforce, this research shares some limitations with many other studies in the developmental stage. First, our study conceptualizes the nonsecurity IT workforce as a homogeneous group. Although information security is the first subarea of the IT field to spin off the IT department and have a separate reporting channel (for example, to the CSO), treating all the other subareas of IT as a single group could have downplayed the distinct characteristics of the individual nonsecurity subareas. It might be good for future research to focus on other comparable subareas—for example, IT versus information security departments within a company, application programmers versus secure programming auditors, help-desk staff versus CERT team staff, and so on. Second, because our sample size was relatively small, the data-collection method includes several uncontrolled factors such as the limited authority, and thus limited representativeness, of the sampling sources over the target population and lack of control over nonrespondents.

Although these are often observed and sometimes inevitable limitations in survey studies,[19] follow-up studies that replicate this research with different sampling sources, including samples from different countries, will certainly clarify the generalizability and boundary conditions of our findings. Nonetheless, we believe that this research has made an important contribution to the information security field by

This is a pre-print version of Lee, J., Bagchi-Sen, S., Rao, H. R., and Upadhyaya, S. J. (forthcoming) "The Anatomy of Information Security Workforce," *IEEE IT Professional*

providing an empirical baseline and foothold for future research.

**References**

1.  *2008 Salary Guide*, Robert Half Technology, 2008; www.roberthalftechnology.com.

2.  J.C. Brancheau and J. Wetherbe, "Key Issues in Information Systems Management," *MIS Quarterly*, vol. 11, no. 1, 1987, pp. 23–45.

3.  D. Lee, E.M. Trauth, and D.W. Farwell, "Critical Skills and Knowledge Requirements of IS Professionals: A Joint Academic/Industry Investigation," *MIS Quarterly*, vol. 19, no. 3, 1995, pp. 313–340.

4.  K.J. Fisher, M. Lobaugh, and D.H. Parente, "An Assessment of Desired "Business Knowledge Attributes for Engineering Technology Graduates," *J. Eng. Technology*, vol. 23, no. 2, 2006, pp. 10–15.

5.  D. Lee, E.M. Trauth, and D.W. Farwell, "The Is Expectation Gap: Industry Expectations versus Academic Preparation," *MIS Quarterly*, vol. 17, no. 3, 1993, pp. 293–307.

6.  C.L. Noll and M. Wilkins, "Critical Skills of Is Professionals: A Model for Curriculum Development," *J. Information Technology Education*, vol. 1, no. 3, 2001, p. 143.

7.  P.H. Cheney and N.R. Lyons, "Information Systems Skill Requirements: A Survey," *MIS Quarterly*, vol. 4, no. 1, 1980, pp. 35–43.

8.  R.L. Leitheiser, "MIS Skills for the 1990s: A Survey of MIS Managers' Perceptions," *J. Management Information Systems*, vol. 9, no. 1, 1992, pp. 69–91.

9.  T. Bacon and R. Tikekar, "Experiences with Developing a Computer Security Information Assurance Curriculum," *J. Computing Sciences in Colleges Archive*, vol. 18, no. 4, 2003, pp. 254–267.

10. M. Igbaria, J.H. Greenhaus, and S. Parasuraman, "Career Orientations of MIS Employees: An Empirical Analysis," *MIS Quarterly*, vol. 15, no. 2, 1991, pp. 151–169.

11. D. Kaputa, "Design and Implementation of a Portable Educational Network to Teach Cyber Security Curricula and Digital Forensics at a Community College," *Proc. 23rd Ann. Computer Security Applications Conf.* (ACSAC), IEEE Computer Society, 2007, http://www.acsac.org/2007/wip/WiP%20Kaputa%20ACSAC07.pdf.

12. E. Crowley, "Information System Security Curricula Development," *Proc. 4th Conf. Information Technology Education* (formerly CITC), ACM Press, 2003, pp. 249–255.

13. M. Dark, "Defining a Curriculum Framework in Information Assurance and Security," Center for Education and Research, Information Assurance, and Security, Purdue Univ., 2003.

14. C.W. Reynolds, "An Undergraduate Information Assurance Curriculum," *Proc. Information Assurance Workshop*, IEEE Systems, Man, and Cybernetics Soc., 2003, pp. 10-16.

15. R.G. Crepeau et al., "Career Anchors of Information Systems Personnel," *J. Management Information Systems*, vol. 9, no. 2, 1992, pp. 145–160.

16. M. Igbaria and S.R. Siegel, "The Career Decision of Information Systems People," *Information & Management*, vol. 24, no. 1, 1992, pp. 23–32.

17. M. Igbaria and S.R. Siegel, "The Reasons for Turnover of Information Systems Personnel," *Information & Management*, vol. 23, no. 6, 1991, pp. 321–330.

18. J. Goo et al., "The Role of Service Level Agreements in Relational Management of Information Technology Outsourcing: An Empirical Study," *MIS Quarterly*, vol. 33, no. 1, 2009, pp. 119–145.

19. R. Rosenthal and L.R. Ralph, *Essentials of Behavioral Research: Methods and Data Analysis*, McGraw-Hill,

1991.

*JinKyu Lee (Ph.D. 2007, SUNY Buffalo) is Assistant Professor of Management Information Systems in Spears School of Business, Oklahoma State University. His current research interests include Inter-organizational information sharing and Information security. He has also been involved in several NSF, NSA, and DoD funded research in e-government and information assurance areas. Prof. Lee can be reached at jinkyu_lee@hotmail.com*

*S. Bagchi-Sen (Ph.D. 1989, University of Georgia) is professor of Geography at the University at Buffalo. Her research interests are in technology-led development with a focus on the role of information technology in labor markets. She is the editor-in-chief of The Professional Geographer, one of the flagship journals of the Association of American Geographers.*

*H. Raghav Rao (Ph.D. 1987, Purdue University) is a Professor at the Management Science and Systems department in the School of Management and an Adjunct Professor at the Computer Science and Engineering department, University at Buffalo, His research interest includes Information and Decision Theory, e-Government and e-Commerce, Information Assurance, and Economics of Information. He is a Co-Editor-in-Chief of Information Systems Frontiers.*

*Shambhu Upadhyaya received his Ph.D. in Electrical and Computer Engineering from the University of Newcastle, Australia in 1987. He is currently Professor of Computer Science and Engineering at University at Buffalo. His research interests are computer security, information assurance, fault-tolerant computing, distributed systems and reliability. His research has been funded by NSF, U.S. Air Force Research Laboratory, DARPA and National Security Agency.*

**The information security workforce is one of the fastest growing subgroups in IT, but little is known about the field's characteristics and educational and professional environments. This article reports on a survey that sheds light on the information security workforce's task responsibilities, job market conditions, and training needs. The study's results should help companies, prospective information security professionals, and educational institutions alike understand the issues pertaining to this labor niche and fulfill the increasing labor demands**

**information security workforce; skill requirements; job responsibility; job market conditions; turnover intention**