

Women in Cybersecurity: A Study of Career Advancement

Sharmistha Bagchi-Sen, H.R. Rao, and Shambhu Upadhyaya, *State University of New York, Buffalo*
Sangmi Chai, *Slippery Rock University*

Although cybersecurity is a critical IT area, women continue to be underrepresented among its ranks. This first study of female cybersecurity professionals examines the required skills, the existing challenges, and the key success factors for women in the field.

The US Department of Homeland Security's national strategy to secure cyberspace identifies cybersecurity awareness and training as one of five national security priorities. Indeed, one of the strategy's missions is to address the shortfall in trained and certified cybersecurity personnel (www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf). However, according to a 2006 IDC survey (www.isc2.org/uploadedFiles/Industry_Resources/wfs_gov.pdf), only 13 percent of US cybersecurity professionals are women—and this percentage is higher than in Europe and Asia. The US National Science Foundation's science and engineering indicator also acknowledges this gender disparity (www.nsf.gov/statistics/seind06/toc.htm). According to the IDC survey, males will continue to dominate the cybersecurity profession into the future.

To ensure a qualified, diverse, and plentiful cybersecurity workforce in the years to come, it's critical that we encourage women to join the field, and that we provide advancement opportunities for those who do. To further this goal, we conducted a study focusing on a sample from among the small group of women who have reached the level of chief security officers and chief information officers. Our study included in-person and paper-based interviews and focused on three main questions:

- What challenges/barriers exist at different stages of women's careers in cybersecurity?
- What skills and knowledge do cybersecurity professionals need?
- How do women cybersecurity professionals view "success" in their profession?

To our knowledge, this is the first study of women cybersecurity professionals. Our findings indicate that women require different hard and soft skills depending on their cybersecurity career stage. More importantly, women must evaluate the required skills and the existing barriers if they want to advance to executive levels.

Cybersecurity Overview

The US National Security Telecommunications and Information Systems Security Committee (www.cnss.gov) defines cybersecurity as the protection of information and the systems and hardware that use, store, and transmit that information. The term cybersecurity itself commonly refers to a set of activities to protect computer-related components and information from attacks; the state of being protected from threats; and the broad field of professionals who improve and implement those activities (see www.thecre.com/pdf/secure/20050404_cyber.pdf).

Cybersecurity is distinct from IT in general in several ways. First, cybersecurity's critical activity is to stop security breaches and attacks, which hamper production and disrupt the workplace. In contrast, critical IT issues aim to enhance organizational productivity. Second, compared to IT, cybersecurity work's value is difficult to quantify in terms of revenue because it's difficult to measure the value of preventing attacks and security breaches. Within organizations, the cybersecurity department is typically a cost center and thus its budget can be targeted for cuts during periods of financial downturn (<http://itmanagement.earthweb.com/secu/article.php/3595721>).

Third, the cybersecurity subfield follows a different pattern in terms of workplace demand and supply. In 2005, for example, cybersecurity received institutional investment and had a strong job market while investments and employment in general IT were stagnating or declining (www.isc2.org/uploadedFiles/Industry_Resources/2005_Global_WF_Study.pdf). Fourth, as an IT subfield, cybersecurity has a substantially more specific focus than IT. Cybersecurity professionals must merge broad IT knowledge with a high-level understanding of

- physical security, including forensic skills;
- privacy management (for fields such as finance and healthcare);

- business contingency; and
- legal matters, including policy creation and enforcement (see www.csoonline.com/analyst/report383.html).

In addition, cybersecurity professionals must manage network security, network security engineering, data security operations, investigations, information systems security, and risk management.

Women must evaluate the required skills and the existing barriers if they want to advance to executive levels.

Barriers to Career Advancement

The barriers to women's advancement in cybersecurity include social, institutional, and personal challenges. Examining these challenges sheds light on both the skills needed and the opportunities that exist for women to succeed in the cybersecurity field.

Social/Institutional Challenges

In the workplace, more women than men claim to experience institutional barriers.¹ Many blame IT's "hacker culture" and social expectations for isolating women from IT. The hacker culture is prevalent in the IT world, leading to exceptionally long hours, late nights, and highly focused, almost obsessive behavior.¹ This male-oriented culture raises concerns about safety and security for women working in computer laboratories alone at night and on weekends. The culture also plays an important role in producing male domination in higher education in computer science, which in turn, influences women's position within the computing field.

Because male faculty members dominate computer science and IT departments in colleges and universities, female students have limited guidance and mentoring opportunities.² Such opportunities play an important role in facilitating entry into the job market.³ Women also have less opportunity than men to build mentor-mentee relationships, and often take a passive role in

Table 1. Interview questions.

1	What motivated you to enter (a) information technology and (b) the information security field?
2	Please define “success” in your line of work.
3	Please describe the 3-5 most important technical and other skills that helped you reach your current position.
4	What personal and profession-specific factors facilitated your transition from (a) a student to a professional (b) a professional to an executive?
5	What barriers did you have to overcome in your transition from a student to a professional and a professional to an executive? Please list 3-5 barriers for each stage.
6	What are the 5 most important decisions you have made as a student, an IT professional, and an executive (such as changing jobs)?
7	Can you provide 5 suggestions to an early career professional to succeed in the IT and information security field? (Please specify any gender-specific differences.)
8	Where do you plan to go from here (your current position)?

initiating them. Because social identity—that is, individual’s perceived similarity or identification with a social group⁴—is an important factor in mentoring success for women, the lack of female mentors can hinder their professional advancement.² The Computing Research Association’s mentoring project for women exemplifies both the importance of mentoring and the need for additional opportunities (www.cra.org/Activities/craw/index.php).

Professional women often must balance home and career, and are responsible for a larger share of childcare and housework than male professionals.⁵ Women with family obligations are typically viewed as lacking strong career devotion compared to their male colleagues. Finally, the IT workforce’s “old boys’ network” contributes to the under representation of women in IT: directly or indirectly, informal networks based on masculine activities isolate women and limit their opportunities.⁶

Personal Challenges

Personal factors can include educational background, personality traits, interests and abilities, IT identity (such as the “geek” or “nerd”), gender identity (such as which jobs are perceived as “feminine” versus “masculine”), and perceived self-efficacy—in this case, a woman’s belief in her ability to accomplish a task. These personal characteristics are partially a product of the family/social environment; in the cybersecurity context, a negative manifestation of them can result from experiential knowledge and the dearth of exposure to computing role models and mentors.⁷

To be successful, cybersecurity professionals must use a holistic approach to link science, math, and engineering to policymaking.⁸ To advance in cybersecurity, professionals must have

a strong background in each of these technical fields and the ability to transform this knowledge into law and order, external regulations, and government policy. In addition, such professionals must possess technical knowledge of hardware and software systems, as well as social/soft skills (such as interpersonal and communication skills).

A gap in interest in math and science between girls and boys contributes to gender disparity in STEM disciplines (science, technology, engineering, and math). This gap arises in middle school (grades six to eight) and grows larger through high school.⁹ Several factors might contribute to this interest and confidence gap. Historically, society didn’t encourage girls to pursue science; in turn, women might have come to view science as a dry and lifeless subject. Second, a lack of female teachers in science and math limits access to classroom role models.¹⁰ Often, women show lower self-efficacy in computer/IT skills,¹¹ which can negatively influence their choice of IT as a career.³

Method and Data

Researchers studying high-level professionals typically adopt qualitative methods due to limited sample numbers and the difficulty of collecting meaningful data from busy CEOs.¹² Given that there are few high-level female cybersecurity professionals and there’s no prior research on cybersecurity and women, our study adopts an exploratory methodology focusing on establishing insights.

We base our data on face-to-face and paper-based interviews at the annual Executive Women’s Forum on Information Security. The forum was organized by Joyce Broccaglia, CEO of Alta Associates, a firm that places women in IS/cyber-

Table 2. A profile of cybersecurity female professionals.

Variables (occupation)	Number of respondents	Variables (industry)	Number of respondents
Chief officer (CIO, CSIO, chief privacy officer, chief security officer)	13	Security solution and information assurance	7
Vice president	2	Security and general consulting	7
Executive security advisor	2	Computer hardware	5
Director of data protection/privacy	3	Insurance and financial institute	4
Senior analyst in computing infrastructures group	1	Government	3
Security program manager	1	Manufacturing	3
President, partner, founder, CEO	9	Education	3
Information and privacy commissioner	1	Database and software	3
Chief strategist	1	Telecommunication	1
Broad occupational categories		Work experience (in years)	
Managerial	23	10-15	5
Technical	6	16-20	14
Other	4	21-25	7
		26-30	7
Educational background			
BA or BS	7	JD	4
MS	9	MBA	3
Other (n/a)	9	PhD	1

security jobs. The forum included senior female executives, including CIOs, chief IS officers, chief privacy officers, chief risk officers, and senior security architects. We limited our sample to female cybersecurity professionals, consistent with other studies that research female professionals.^{5,13} Among our survey respondents, two-thirds of them were in managerial positions.

After conducting in-depth, face-to-face interviews with 10 executive-level female professionals, we developed and distributed paper-based interview questions (see Table 1) to other cybersecurity professionals. To analyze the results, we used content analysis. In total, we used 33 paper-based interview results for our analysis. This sample size is acceptable and consistent with the sample size in other qualitative studies.¹² Table 2 shows the sample characteristics.

Results

Based on our interview results, we identified various factors affecting the careers of cybersecurity professionals. We categorized the factors by social factors (such as work–family conflict, informal networks, and social expectations for women) and institutional/structural factors (such as a lack of role models and mentors, occupational culture, institutional structure, and

demographic composition). We now describe each factor as it relates to barriers for female cybersecurity professionals in their career choices, persistence, and advancement.³

The 33 respondents saw similar social and institutional barriers for both IT and cybersecurity careers. However, the results showed that personal factors such as skills, cybersecurity knowledge, and job experience set cybersecurity professionals apart from other IT subfield job requirements (see Figure 1).

Early Career Barriers

We categorized social and institutional barriers early in a career into two groups: training and the work environment. First, in terms of training, we noted

- a lack knowledge about how to practically apply technology in business situations, and
- insufficient exposure to team work/collaboration.

One respondent—a graduate from a premier US institution—said that her education was “strong in theory, light on practice. Had to relearn things in a pragmatic way.” Another respondent said the following about teamwork: “Fitting into an

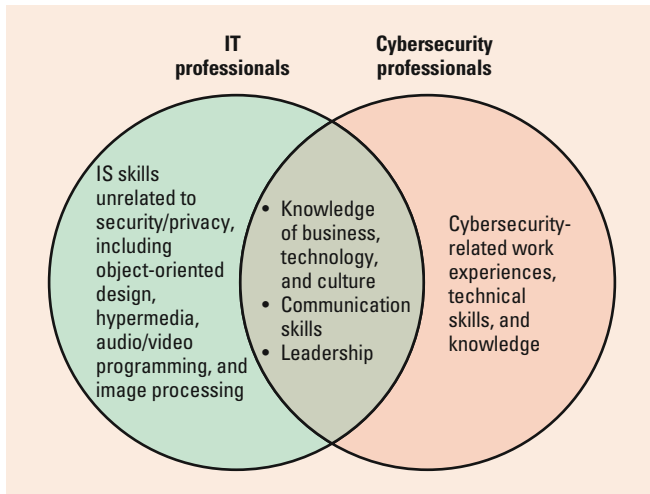


Figure 1. Factors affecting career advancement of women in IT versus those in cybersecurity.

organization and working in a team after being an independent student was especially hard.”

According to the survey results, the cybersecurity-specific work environment—described as “be ready for 24x7”—was also a barrier for female personnel. Such a work environment made it difficult to manage a work–family balance for women, who are often in charge of household work and raising children. The discussion of the work environment corroborates findings of other studies of women working in male-dominated professions. Most also had to overcome stereotyping, such as getting mistaken for a secretary or support staff rather than being recognized as a professional.

In addition, our results show that women face difficulty in building and belonging to a network of like-minded peers. Respondents mentioned that without such a network, it’s difficult to establish trust, to know about and understand “political landmines” in a corporate setting, and to confront/challenge an experienced superior who is clearly wrong or about to make a wrong decision.

Career Advancement

We grouped barriers to career advancement into three categories: skills, work environment, and personal. The most critical skill barrier was a lack of effective training in communication skills. Many respondents understood technical talk, but lacked the vocabulary for business. Furthermore, transitioning from technical to managerial positions entailed changing from being an aggressive problem solver to being an assertive manager.

Several respondents commented on this transition’s requirements:

- “Ruthless prioritization—saying no, meaning no, and acting on no.”
- “Don’t say no; say yes and explain costs and risks.”
- “Selling (putting the spin on) versus telling it like it is.”
- “More is less—communicating what needs to be said, versus what I’d like to express.”

The final difficulty respondents said they faced was in marketing themselves as high-skilled workers—or, as one put it, in “tooting my own horn.” Gender issues and the difficulty in managing work–family balance clearly complicated the transition from professional to executive levels. One respondent said that she had limited herself to her current level (which was still very senior) “due to my desire to have work–life balance and raise my family.” Another noted that, a “male-dominant work environment and gender bias to women in this area are obstacles to overcome as a female professional.”

Required Skills and Knowledge

The paper-based interview results differentiated IT job skills and cybersecurity-specific skills for early and mid/advanced career levels. Table 3 outlines the skills for each group.

Early on in a career, technical and analytical skills can be quantified to some extent. However, assessing other skills is subjective and the interpretation can vary from person to person. One respondent, for example, interpreted common sense as “the ability to sink or swim with little guidance.” Another said that having people skills meant that you could easily establish client confidence.

As Table 3 shows, the skills essential to further advancement fall into 10 categories. One respondent summed up the difference between early and advanced career demands as follows: “As you move up the ladder, the technical skills are overshadowed by the strong management skills needed. However, you must remain conversant technically.”

Success Factors

We used responses to both the in-person and paper-based interviews to categorize “success.”

Table 3. Essential skills for early career and career advancement.

	General IT job skills	Cybersecurity-specific skills
Early career skills	Technical skills (system administration, database, networking, programming languages)	Technical skills (security packages, networks and network security components, firewall management skills, understanding security processes and controls)
	Problem-solving skills	Problem-solving skills (investigation and forensic analysis to detect intruders)
	System development methodology	Support skills (24x7 availability to protect information security)
	Analytical aptitude	Communication skills (explain security in simple language and to non-IT personnel)
	Ability to work hard (staying up-to-date on new technology)	
	Common sense	
	People skills (establish client confidence, be a team player, encourage loyalty)	
Additional skills for career advancement	Breadth of knowledge	Understanding cybersecurity project strategies and relating them to business and technical requirements
	Ability to learn new technology	Establish and implement security policies
	Continuous skill improvement	Audit and review security skills
	Communication skills	
	Project design	
	Understanding enterprise-level infrastructure	
	Ability to relate business and technical requirements to project strategies	
	Multitasking skills	
	Expertise in outsourcing	
	Ability to satisfy clients and customers	
	Loyalty, honesty, and ethical behavior	
	Leadership skills	
	Management aptitude	
	Industry networking skills	

The women perceived “success” not just as something measured by certain metrics (such as salary), but also as reflecting recognition for both innovative and visionary functions and routine preventive tasks that were essential to information security.

Among the innovative and visionary functions, respondents identified three unique tasks:

- developing new solutions, products, or processes to enhance operations;
- creating and operationalizing risk management teams; and
- incorporating feedback from staff to operationalize security.

Respondents also provided two indicators of job recognition as a measure of success: their reputation among peers and having clients regularly seek their advice on security protection issues. The two most common preventive routine tasks, which are somewhat quantifiable, are

- preventing security breaches and reducing risk, and
- performing within budget or efficiently managing expenditures.

Metrics for measuring success aren’t always tangible. Among the criteria respondents considered were salary, designation/rank, opportunities to serve on boards/panels, position within the management team, recognition by company executives, the tenacity to stay in business (often mentioned by owners/managers of small- and medium-sized companies), and the ability to create industry standards.

Our findings show that context is extremely important when evaluating skills and barriers. One of the main contexts is a respondent’s career stage: as careers advance, women face different barriers. Early on, technical skills are important, but for cybersecurity professionals, the ability to relate technical knowledge to business

goals is far more important to survival. For career advancement, critical skills include teamwork, organizational loyalty, and client relationships. In cybersecurity, hard and soft skills—such as solving problems to manage risk and effectively communicating with vendors and clients—complement each other. Career advancement is directly related to acquiring new technical knowledge and communication skills; that is, to knowing the four Ps of product, process, people, and policy. Among the key soft skills are the abilities to manage relationships within and outside the organization and to be assertive in decision-making without alienating clients, vendors, and peers.

Career advancement is directly related to knowing the four Ps of product, process, people, and policy.

As cybersecurity provides more jobs and becomes central to company operations, women's advancement to executive and managerial positions will have serious consequences for gender equity in the overall IT sector. As our results show, addressing the needs of women at the beginning of their careers—starting at educational institutions—is crucial to their successful entry and success in the field. Currently, the US government has responded to this issue by providing grants to attract and train women in cybersecurity at the university level. The success of such efforts in terms of furthering gender equality is a topic of future research. Also, several of the barriers we've identified obviously apply to men as well as to women. However, it's likely that such issues would affect men and women differently, which offers another topic for future research. ■

Acknowledgments

We're deeply grateful to Joyce Broccaglia of Alta Associates for her help with this research. The US National Science Foundation funded our research through grant 0420448, but the opinions expressed here are our own.

References

1. C.A. Heaton and E. McWhinney, "Women in Management: The Case of MBA Graduates," *Women in Management Rev.*, vol. 14, no. 4, 1999, pp. 136–145.

2. S. Parasuraman, Y. Purohit, and V. Godshalk, "Work and Family Variables, Entrepreneurial Career Success, and Psychological Well-Being," *J. Vocational Behavior*, vol. 48, no. 3, 1996, pp. 275–300.
3. M.K. Ahuja, "Women in the Information Technology Profession: A Literature Review, Synthesis and Research Agenda," *Euro. J. Information Systems*, vol. 11, no. 1, 2002, pp. 20–34.
4. B.R. Ragins, "Antecedents of Diversified Mentoring Relationships," *J. Vocational Behavior*, vol. 51, no. 1, 1997, pp. 90–109.
5. D.J. Armstrong et al., "Advancement, Voluntary Turnover, and Women in IT: A Cognitive Study of Work–Family Conflict," *Information & Management*, vol. 44, no. 2, 2007, pp. 142–153.
6. M. Gamba and B.H. Kleiner, "The Old Boys' Network Today," *Int'l J. Sociology and Social Policy*, vol. 21, no. 8, 2001, pp. 101–108.
7. E.M. Trauth, J.L. Quesenberry, and A.J. Morgan, "Understanding the Under Representation of Women in IT: Toward A Theory of Individual Differences," *Proc. SIGMIS Conf. Computer Personnel Research*, ACM Press, 2004, pp. 114–119.
8. A. Sharma, "A Holistic Approach to Physical and IT Security," *Security*, Nov. 2006, www.securitymagazine.com/Articles/Feature_Article/c805be157db0f010VgnVCM100000f932a8c0.
9. K. A. Frenkel, "Women and Computing," *Comm. ACM*, vol. 33, no. 11, 1990, pp. 34–46.
10. H. Dryburgh, "Underrepresentation of Girls and Women in Computer Science: Classification of 1990s Research," *J. Educational Computing Research*, vol. 23, no. 2, 2000, pp. 181–202.
11. K. Hartzel, "How Self-Efficacy and Gender Issues Affect Software Adoption and Use," *Comm. ACM*, vol. 46, no. 9, 2003, pp. 167–171.
12. D.F. Feeny, B.R. Edwards, and K.M. Simpson, "Understanding the CEO/CIO Relationship," *MIS Quarterly*, vol. 16, no. 4, 1992, pp. 435–448.
13. C. Cross and M. Linehan, "Barriers to Advancing Female Careers in the High-Tech Sector: Empirical Evidence from Ireland," *Women in Management Review*, vol. 21, no. 1, 2006, pp. 28–39.

Sharmistha Bagchi-Sen is a professor at the State University of New York, Buffalo, where she is director of graduate studies in the Department of Geography. Her research interests are in the high-technology industry, labor markets, organizational dynamics, and international business. Bagchi-Sen has a PhD from the University of Georgia. Contact her at geosbs@buffalo.edu.

H.R. Rao is a professor of management systems and science at SUNY, Buffalo. His research interests are in management information systems, decision-support systems, e-business, emergency-response management systems, and information assurance. He is an associate editor of Decision Support Systems, Information Systems Research, and IEEE Transactions in Systems, Man and Cybernetics, and co-editor-in-chief of Information Systems Frontiers. Rao has a PhD in management information systems from Purdue University. Contact him at mgmtrao@buffalo.edu.

Shambhu J. Upadhyaya is a professor of computer science and engineering at SUNY, Buffalo, where he directs the Center of Excellence in Information Systems Assurance Research and Education. His research interests include in-

formation assurance, computer security, fault diagnosis, fault-tolerant computing, and VLSI testing. He was guest co-editor of the book Managing Information Assurance in Financial Services (IGI Global, 2007). Upadhyaya has a PhD in electrical and computer engineering from the University of Newcastle, Australia, and is a senior member of IEEE. Contact him at shambhu@cse.buffalo.edu.

Sangmi Chai is an assistant professor in the College of Business, Information, and Social Sciences at Slippery Rock University. Her research interests include information security, ethical issues and information privacy in IT, and the IT and cybersecurity workforce. Chai has a PhD in management from the State University of New York, Buffalo. Contact her at schai2@buffalo.edu.