Winter 12-10-2023

What Technical and Professional Skills are Needed for Cybersecurity Roles?

Mary Sumner
University of Oklahoma

Keri Pearlson
University of Oklahoma

Dan Mazzola
University of Oklahoma

Chris Maurer
University of Oklahoma

What Technical and Professional Skills are Needed for Cybersecurity Roles?

Research-In-Progress

Mary Sumner
MIS Division, University of Oklahoma
Norman, OK, USA

Keri Pearlson
Sloan School of Management, Massachusetts Institute of Technology
Cambridge, MA, USA

Dan Mazzola
Information Systems, Arizona State University
Tempe, AZ, USA

Chris Maurer
McIntire School of Commerce, University of Virgina
Charlottesville, VA, USA

ABSTRACT

The Cybersecurity Skills Survey was designed to respond to the high-demand for cybersecurity professionals, noted by the findings of SIM (Society for Information Management) IT Trends and Issues Study (2017, 2018, 2019, 2020, 2021). The findings of the IT Trends and Issues Study are based upon input from over 1,000 IT leaders representing 37 SIM Chapters. The goals of the cybersecurity skills survey were to identify: (1) What technical skills are needed for entry-level professionals in cybersecurity jobs? (2) What professional skills are needed for entry level professionals in cybersecurity jobs? (3) What technical skills are needed for early-career professionals in cybersecurity jobs? and (4) What professional skills are needed for early-career professionals in cybersecurity jobs? The survey findings provide key insights into in-demand skills and "difficult-to-find" competencies. This paper reports on 99 responses captured from IT leaders representing the SIM Chapters in St. Louis, Austin, Milwaukee, and Phoenix.

Keywords: Cybersecurity Skills. Technical Skills. Professional Skills.

INTRODUCTION

SIM, the Society for Information Management, has 37 Chapters with over 5,000 IT Leaders and Chief Information Officers in the United States. The SIM IT Trends Study, which is planned and

organized by a team of SIM academic leaders surveys these IT leaders each year to determine their top challenges, their top "worries," their changing priorities, and their budgets for information services. The SIM IT Trends Study reports that Cybersecurity remains the #1 concern for CIO's and IT Leaders within organizations for the 4th year in a row. The overwhelming importance of the cybersecurity issue is combined with the high-demand for IT talent in cybersecurity roles. The projected job growth for information security analysts is 31% between 2019 and 2029 (Bureau of Labor Statistics 2021). A report by Cybersecurity Ventures predicts that there will be 3.5 million unfilled cybersecurity positions worldwide in 2025 (Morgan 2021).

In 2020 and 2021, the SIM Academic Council organized a research group to develop a survey to determine the skills needed by cybersecurity professionals. In developing a survey of cybersecurity skills, they decided to take technical skill sets and professional competencies into consideration. They sought to capture both entry level skills and early-career (3 to 5 years' experience) skills in the survey.

RELEVANT LITERATURE

A number of recent studies address the cybersecurity skills gap. In an assessment of education, professional experience, certification, security clearance, and programming skill requirements for 935 cybersecurity positions, Ramazan identified nine sub-fields, including architecture, auditing, education, governance, management, operations, penetration testing, software security, and threat intelligence (Ramezan 2023). Both higher education degrees and work experience were required across all sub-fields, and over 48% of the positions listed industry cybersecurity certifications, such as the CISSP, CISA, and Security + certifications. Notably, 19% of the positions required security clearance, and 25% listed knowledge of a programming language. These programming skills were prevalent in positions within the architecture, software security, and penetration testing fields.

Peslak and Hunsinger (2019) also posed the question, "What cybersecurity skills are employers seeking?" Based upon their analysis of job descriptions from 500 ads, they determined both higher education degrees, general technical skills, and professional experience related to cyber threats are needed by cybersecurity analysts and professionals (Peslak and Hunsinger 2019).

In a paper entitled, "Skills, Certifications, or Degrees: What Companies Demand for Entry-Level Cybersecurity Jobs," Marquardson and Elnoshokaty (2019) examine the trade-off's between education, experience and certifications. They analyzed 11,938 entry-level job postings for cybersecurity jobs on Dice.com, and discovered that 7,177 (60%) of the entry-level cybersecurity jobs require a college degree, while 3,406 (29%) of the jobs required a certification. SQL, Testing, Java, Excel, Oracle, and Database skills were listed in 16% of the cybersecurity jobs. The CISSP (Certified Information Systems Security Professional) certification was the most-frequently-mentioned certification, with 4.8% of the jobs listing the CISSP. By and large, college degrees are in highest demand for the field of Cybersecurity, and indicated by the fact that 60% of the jobs listed college degrees as required or desired. Parker and Brown's 2019 analysis of cybersecurity job descriptions (2019) found similar requirements to these studies.

In their content analysis of IS jobs, Niederman and Sumner analyzed positions in the Security Cluster, consisting of six IS job instances, including Security Administrator, Senior Security Engineer, Security Engineer, Senior Security Analyst, Security Analyst II, and Security Analyst. Their content analysis of IS Security jobs revealed that Security professionals need both professional skills and technical skills. Professional skills included communications skills,

problem-solving skills, the ability to balance business and technical solutions, and project management. Technical skill sets were security architecture and security risk management.

William Crumpler and James Lewis, who serve with the Technology Policy Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C., report that cybersecurity skills represent an urgent workforce need. Crumpler and Lewis (2019) cite significant gaps in the nation's capability to prepare professionals with cybersecurity skills. In a recent survey of IT decision-makers across 8 countries, 82% of the employers reported a shortage of cybersecurity skills, and 71% believed that this talent gap causes measurable harm to organizations (CSIS 2016). Job postings in this and other studies confirm that the number of unfilled cybersecurity jobs has grown significantly. Since organizations face challenges in recruiting the talent they need to secure their systems and infrastructure from cybersecurity threats, Crumpler and Lewis re-iterate that professionals with extensive technical expertise for roles in penetration testing, secure systems design, and tool design are greatly needed.

RESEARCH QUESTIONS AND DATA COLLECTION

The cybersecurity skills survey was designed to give SIM members and IT leaders an opportunity to identify cybersecurity skills, and to participate in dialogues between academic professionals and IT industry leaders in response to the findings of the on-line survey.

Research Questions

1. What technical skills are needed for entry-level professionals in cybersecurity jobs?
2. What professional skills are needed for entry level professionals in cybersecurity jobs?
3. What technical skills are needed for early-career professionals in cybersecurity jobs?
4. What professional skills are needed for early-career professionals in cybersecurity jobs?

Between August and October 2020, the cybersecurity research team rolled out the cybersecurity survey within four SIM Chapters, including SIM St. Louis, SIM Milwaukee, SIM Austin, SIM Phoenix. During that time, the team gathered 99 responses, and these findings are reported in this paper. Going forward, the plan is to extend the survey to SIM Chapters in Tampa, Los Angeles, Houston, Chicago, and Boston.

DATA ANALYSIS AND FINDINGS

In response to the technical skills needed for entry-level cybersecurity roles and early-career cybersecurity roles, these data show that knowledge of cybersecurity frameworks (COBIT, NIST) was high-in-priority for both groups. Risk assessment and knowledge of tools to detect and to identify cybersecurity issues came in next in level of importance. Several of the more technical competencies, such as operating systems and networking/telecom, were higher in importance for entry-level cybersecurity professionals as compared with early-career professionals. The vulnerability assessment competency was higher for early-career professionals, as compared with entry-level professionals. Incident response was similar in importance for both entry-level and early-career cybersecurity professionals. See Table 1.

Table 1. Technical Skills

Technical Skills	Entry-Level % selected*	Early Career % selected*
Cybersecurity Frameworks	68.8%	72.4%
Risk Assessment	41.9%	44.8%
Tools to Detect Issues (SIEM)	41.0%	37.9%
Cloud Technologies	36.2%	41.5%
Vulnerability Assessment	36.2%	42.5%
Operating Systems (Linux, Windows)	36.2%	20.7%
Incident Response	31.4%	35.2%
Regulatory/legal requirements (GDPR, CCPA)	27.6%	42.5%
Networking/telecom	24.8%	16.1%
Penetration testing	22.9%	29.9%

*The survey asked respondents to select the top 5 Technical Skills.

In response to the Professional Skills needed for entry-level and early-career cybersecurity roles, the top skill for both entry-level and early-career roles was Critical Thinking. This was followed by Attention to Detail and Problem-Solving Skills, Collaboration and Teamwork. See Table 2.

Table 2. Professional Skills

Professional Skills	Entry-Level % selected*	Early Career % selected*
Critical Thinking	73.3%	69.0%
Attention to Detail	61.9%	35.6%
Collaboration/Teamwork	58.1%	49.4%
Problem-solving	54.3%	49.4%
Written Communication	41.0%	42.5%
Oral Communication	39.0%	44.8%
Self-learner/ability to learn with limited direction	35.2%	26.4%
Innovative Thinking	24.8%	33.3%
Time Management/Project Management	15.2%	27.6%
Customer/Relationship Management	12.4%	21.8%

*The survey asked respondents to select the top 5 Professional Skills.

In the open dialogues between practitioners and academic professionals, there was a preference for individuals who are self-learners, or life-long learners. Communications skills, including oral and written communications, were considered important for both entry-level and early-career cybersecurity professionals.

Difficulty in Finding Cybersecurity Skills

In terms of the degree of difficulty in finding cybersecurity skills, including both technical skills and professional skills, the respondents indicated that both skill sets are difficult to find. See Table 3.

Table 3. Technical Skills (Difficult to Find)

	Entry-Level*	Early-Career*
Regulatory/Legal Requirements (GDPR, CCPA)	4.00	3.44
Cloud Technologies	3.77	3.33
Cybersecurity/Control Frameworks (COBIT, NIST)	3.73	3.20
Risk Assessment	3.59	3.32
Penetration Testing	3.58	3.38
Networking/telecom	3.50	3.07

*Higher is More Difficult to Find

Table 4 describes the difficulty in finding professional skills for entry-level and early-career candidates for cybersecurity roles. See Table 4.

Table 4. Professional Skills (Difficult to Find)

	Entry-Level*	Early-Career*
Critical Thinking	373	3.34
Oral Communication	3.53	3.18
Innovative Thinking	3.52	3.55
Self-Learner/Ability to Learn with Limited Direction	3.49	3.53
Written Communication	3.46	3.39
Customer/Relationship Management	3.45	3.59
Attention to Detail	3.40	3.20

*Higher is More Difficult to Find

Critical thinking and communications skills were “difficult-to-find” competencies for entry-level opportunities, and somewhat “difficult-to-find” for early-career roles. Self-learning skills were somewhat difficult-to-find for both entry-level and early-career roles. Written communication, innovative thinking, and attention to detail were all somewhat “difficult-to-find” for entry-level roles, and that held true for early-career roles as well.

The ideal qualification for entry-level cybersecurity candidates was a Bachelor’s Degree with an Internship. Bootcamps and Certifications were lesser in importance. We might surmise that the Bachelor’s programs go-beyond technical skilling and reinforce the professional skills needed for these positions.

PRIMARY TAKEAWAYS AND NEXT STEPS

1. Frameworks and regulatory requirements matter. The data on skills needed for cybersecurity roles (both entry-level and early-career) reinforce the importance of knowledge of cybersecurity/control frameworks, such as NIST and COBIT.
2. Entry-level positions rely more on operational skills/knowledge. At the entry-level, technical skills, security monitoring tools, and operating systems were viewed as important.
3. In-demand skills are difficult to find. Both technical skills and professional skills are difficult-to-find. These "difficult-to-find" skills included cloud technologies, cybersecurity frameworks, and vulnerability assessment at the entry-level, and both risk assessment and cloud technologies at the early-career level.
4. Professional skills (critical thinking, problem-solving) are difficult to find. Critical thinking, communications, and problem-solving skills were "difficult-to-find" for both entry-level and early-career roles.
5. Formal education is beneficial; and there was a preference for individuals with 4-year degrees.

REFERENCES

Crumpler, W. and Lewis, J. A. (2019). "The Cybersecurity Workforce Gap." Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-workforce-gap

Kappelman, L., McLean, E., Johnson, V., Torres, R., Maurer, C., Snyder, M., Kim, K., and Guerra, K. (2020). "The 2020 SIM IT Trends Study. The 2021 Comprehensive Report: Issues Investments, Concerns, and Practices of Organizations and their IT Executives." http://www.simnet.org/IT-Trends.

Marquardson, J. and Elnoshokaty, A. (2020). "Skills, Certifications, or Degrees: What Companies Demand for Entry-Level Cybersecurity Jobs." Information Systems Education Journal. 18(1), 22-28.

Morgan, S. (2021). "Cybersecurity Jobs Report: 3.5 Million Openings in 2025." Cybercrime Magazine. https://cybersecurityventures.com/jobs/

Parker, A. and Brown, I. (2019). "Skills Requirements for Cybersecurity Professionals: A Content Analysis of Job Descriptions in South Africa." In Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (Eds.), Information Security (pp. 176-192).

Peslak, A. and Hunsinger, D.S. (2019). "What is Cybersecurity and What Cybersecurity Skills are Employers Seeking?" Issues in Information Systems, 20(20, 62-72.

Ramezan, C. (2023). "Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field." Journal of Information Systems Education, 34 (1), 94-105.

Sumner, Mary and Niederman, F. (2019). "Resolving the IS Skills Paradox: A Content Analysis of a Jobs Database." Proceedings of the ACM SIG MIS 2019 Conference. ACM Digital Library.

U.S. Bureau of Labor Statistics. (2021). Information Security Analysts: Occupational Outlook Handbook. U.S. Department of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/home.htm