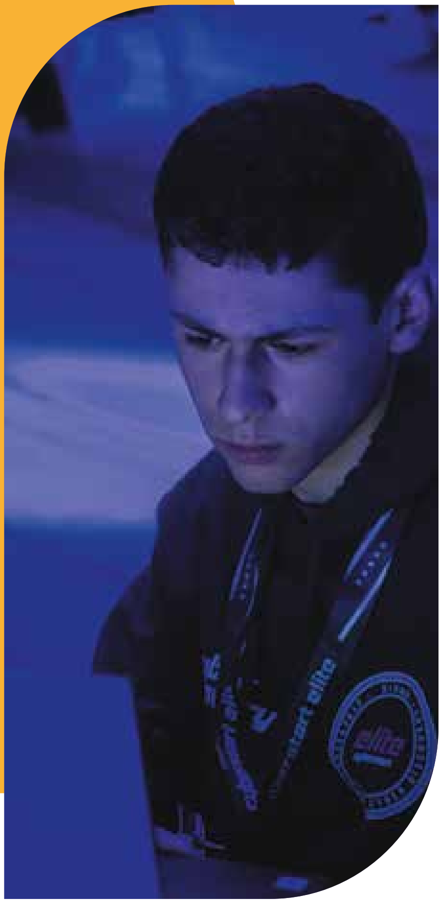
Using Certifications to Rank Cybersecurity Job Candidates



A Report of the CIO Institute

CIO INSTITUTE

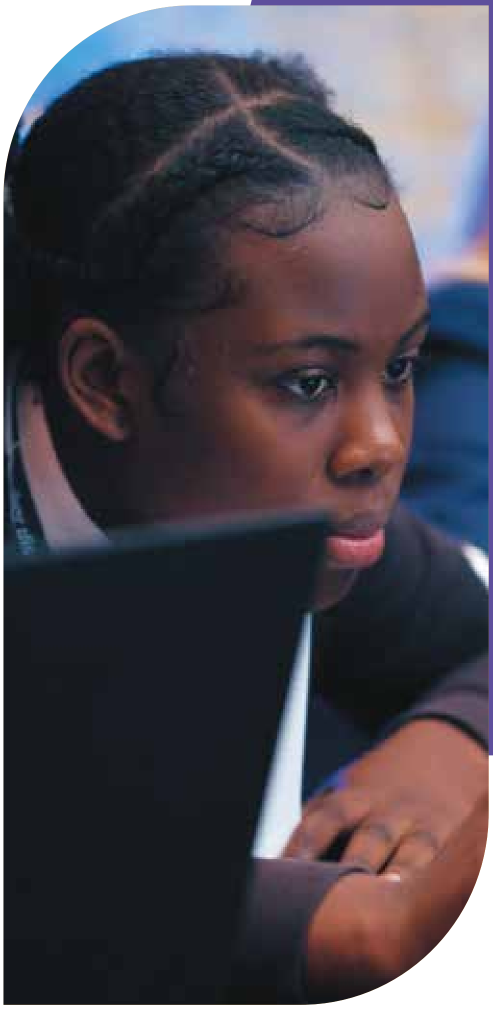
CIO.org

Authors: Franklin Reeder, Alan Paller

ISBN 978-0-578-83950-9
US$25.00
52500>
9 780578 839509

Copyright 2021. All Rights Reserved

Contents



Introduction

Cybersecurity professionals earn certifications because they see them as an effective way to learn new skills and demonstrate mastery of those skills to employers. Unfortunately, the Chief Information Officers and Human Resources personnel looking to hire those professionals often have limited knowledge about the certifications. To some, they are little more than acronyms on a page.

So how can those doing the hiring accurately and reliably determine which certifications are important and relevant when they select whom to interview for available positions?

To find out, we first searched for the number of job postings that requested that applicants have a given certification, using data published by Cyber Seek, Indeed, Acclaim, and LinkedIn. Those counts were used to identify the six cybersecurity certifications that are most often included in cybersecurity job postings: CISSP® from ISC^2, Security Essentials (GSEC) and Certified Incident Handler (GCIH) from GIAC, Certified Information Systems Auditor (CISA) from ISACA, Security+ from CompTIA, and Certified Ethical Hacker (CEH) from EC-Council.

CISSP: The CISSP® exam is convers eight domains: security and risk management, asset security, security architecture and engineering, communication and network security, identity and access management, security assessment and testing, and security operations.

GSEC: The Global Information Assurance Certification (GIAC) Security Essentials GSEC) certification validates a practitioner's knowledge of information security beyond simple terminology and concepts.

GCIH: The Global Information Assurance Certification (GIAC) Certified Incident Handler (GCIH) certification validates a practitioner's ability to detect and resolve computer security incidents by understanding common attack techniques and mastering the tools neededto respond effectively.

CEH: The Certified Ethical Hacker (CEH) certification knowledge needed to look for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker.

CISA: The Certified Information Systems Auditor (CISA) is a certification for those who audit, control, monitor, and assess an organization's information technology and business systems.

Security+: CompTIA's Security+ certification covers baseline knowledge required of many cybersecurity roles.

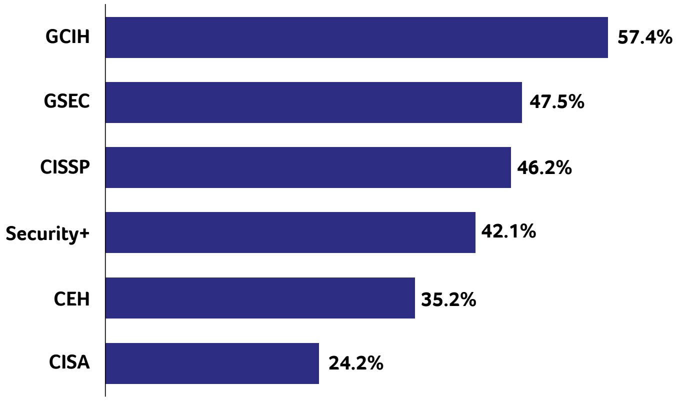
The Survey

We then conducted an online survey of 31,000 holders of the listed GIAC certifications asking them to respond only if they also held one or more of the non-GIAC certifications commonly included in job postings. A total of 2,500 people responded saying that they have another certification besides their GIAC certification, and they then assigned a value to each of those certifications. The survey required that respondents provide their names and employers so that responses could be attributed and certification holdings confirmed. To help persons entering the cybersecurity profession who might see the survey, respondents were also asked for additional comments about how their certification had benefited them.

While the ultimate test of the value of a professional certification is job performance, we would assert that the value that those in the field place on each certification is a meaningful and more readily measured proxy. So we asked respondents whether they would be more likely to recommend a job applicant who holds a given certification for an interview for a hands-on, entry-level cybersecurity role. Of course, determining who is to be interviewed is only the start of the hiring process and more rigorous screening is also recommended.

The percentages of respondents who hold each of these six certifications are shown in Figure 1.

Figure 1: Percentage of Respondents Who Hold Each of the Six Most Popular Cybersecurity Certifications

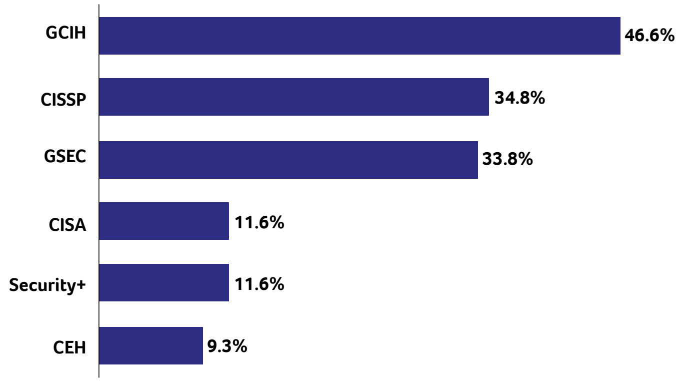


Note: Percentages total more than 100% because all of those surveyed hold more than one certification and many hold more than two.

Results

Holders of the three most popular cybersecurity certifications are at least three times more likely to be interviewed for jobs in cybersecurity than holders of the next three certifications. Figure 2 shows the percentage of survey respondents who would be "very likely" to recommend interviews of job candidates who hold each of the six most popular cybersecurity certifications mentioned above (Security+, CISSP®, CISA, GSEC, GCIH, and CEH).

Figure 2: Percentage of Respondents "Very Likely" to Recommend that a Candidate Holding One of the Six Most Popular Certifications Be Interviewed

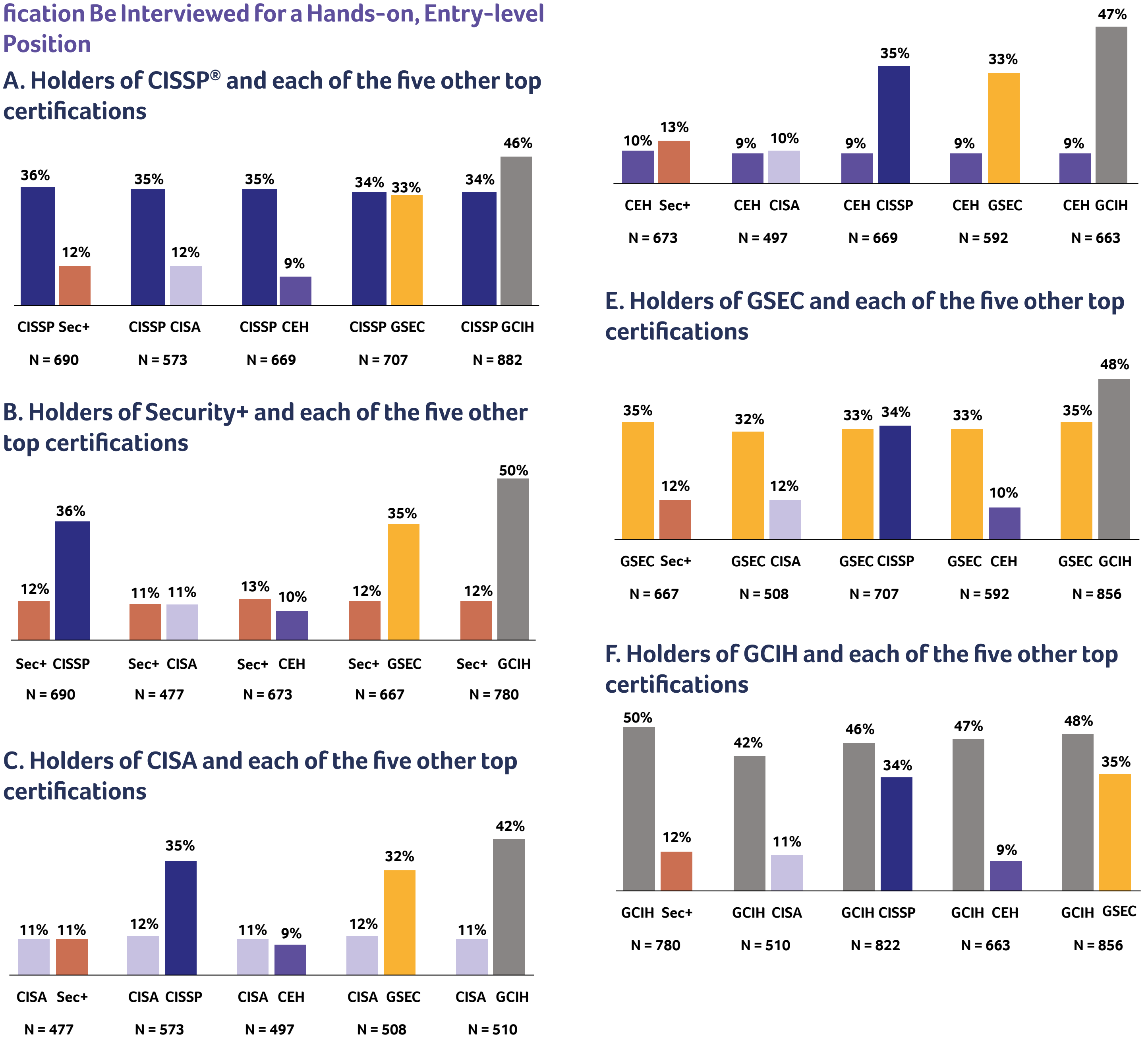


How Holders of Each Certification Value the Other Certifications They Have Earned

Since one might expect that most individuals who hold a certification would value that certification, we analyzed the responses to compare how each respondent valued all of the certifications he or she holds. Each panel in Figure 3 presents data from respondents who reported they hold both of the certifications being compared. Each pair of bars shows only the responses of individuals who hold those two certifications. The number of respondents who hold both is shown in the bar pairings in each panel. Consistent colors are used for each certification according to the following legend:

Security+	🟧
CISA	🟪
CISSP	🟦
CEH	🟪
GSEC	🟨
GCIH	⬜

Figure 3: Percentage of Respondents Who Highly Recommend that Applicants Who Hold Each Certification Be Interviewed for a Hands-on, Entry-level Position



A. Holders of CISSP® and each of the five other top certifications

B. Holders of Security+ and each of the five other top certifications

C. Holders of CISA and each of the five other top certifications

D. Holders of CEH and each of the five other top certifications

E. Holders of GSEC and each of the five other top certifications

F. Holders of GCIH and each of the five other top certifications

Why Are Some Certifications More Highly Valued Than Others?

We asked survey respondents why they thought the top-rated certifications were so valuable to their employers. Among the more than 500 comments we received, several themes came up repeatedly, including that the certification:

- "Enabled me to implement new techniques that improve security at my organization."
- "Gave me respect, credibility, and prestige with my bosses and peers to persuade management to make important security improvements."
- "Helps me sell our products/services to customers concerned about security because my certification is widely respected."
- "Helped make audits less burdensome because the auditors trusted me."

Examples of Comments from Survey Respondents about the Six Most Popular Certifications

CISSP® (ISC²)

"The knowledge I got studying for the exam is not just about security; it is also about IT leadership, so it helped me become a better manager."

"Studying for the CISSP® exam was intense. It took me five months, but it gave me an understanding of how processes operate, and I used that knowledge to improve my work, including performing security functions myself, so we didn't have to hire consultants or additional employees."

”It gave me more credibility, and that helps in conversations and presentations with leaders of my firm.”

“Our clients want to be confident we are protecting their data. My CISSP® helps me talk to our clients’ security teams and explain how information is kept securely.”

“Earning my CISSP® gave me visibility into the broad security market to help me eliminate flaws that are not critical today but might become a problem tomorrow.”

GSEC and GCIH (GIAC)

“Great hands-on learning that helped reinforce all the skills taught. Rather than just being informational, I really feel that these certifications helped build and reinforce my skillset.”

“After obtaining each of the certs I was able to perform significantly better in the area that was my weakness before, and I can measure and show the improvements based on my performance in NetWars exercises.”

“The GIAC Certs prove I learned best practices from national experts. They shared practical, real-world examples that have helped me make difficult decisions after I left the classroom. In other words, it’s the training that matters; the certification is evidence I mastered the material in the training.”

“When engaging with external auditors who discover you have GIAC certifications, the whole audit process takes on a more positive outcome.”

“The GCIH specifically has allowed me to talk in a common language with my other Incident Response peers. This is greatly beneficial in breaking down communication barriers that can exist. Things like using PICERL to identify the phase you are in are very beneficial.”

“Better understanding of attack techniques has allowed me to have better conversations with prospective customers of our security solutions and how they can mitigate those risks.”

“GIAC certs are able to be used as a replacement for years of required experience or degree in hiring and promotion.”

"The classes leading to my certs allowed me to meet like-minded people, and even today we have an open communication channel where we discuss solutions to common problems."

Security+ (CompTIA)

"My employer said I had to get a Sec+ cert because we work on DoD contracts, so it helped me keep my job."

"It covers a lot of the basics like networking and operating systems that are really useful."

"In studying for it, I learned about analyzing firewall rules and logs, which I've been able to use in my job."

CISA (ISACA)

"It opened the door to my current job. The audit manager who interviewed me told me he has a CISA."

"I feel it gives my resumé strength, because CISA is recognized all over the world."

"Studying for the CISA showed me the value of focusing on business objectives during an audit."

CEH (EC-Council)

"I learned how to use tools and techniques hackers use."

"CEH lifted me to Level II on the DoD scale and that earned me a good raise."

"It got me into the minds of hackers and that's helped me in understanding what kinds of threats we face."

About the Authors

Franklin Reeder

Frank Reeder served two stints at the U.S. Office of Management and Budget totaling more than 20 years where he was chief of Information Policy (the first "federal CIO"), Deputy Associate Director for Veterans Affairs and Personnel, and Assistant Director for General Management. He subsequently served as Director of the Office of Administration of the Executive Office of the President under President Bill Clinton. Frank helped conceive and build several programs recognizing singular contributions to technology in Government, including the Federal 100 Awards.

Frank represented the Administration in negotiating and securing enactment of the Computer Privacy Act and the Computer Security Act of 1987 and wrote the guidelines on implementing the Privacy Act. He also chaired the Public Management Committee of the OECD. After retiring from government service, Frank co-founded and became the chairman of the Center for Internet Security, a not-for-profit established "to help organizations around the world effectively manage the organizational risks related to information security," and chaired the Information Security and Privacy Advisory Board of the National Institute of Standards and Technology, a federal advisory committee. Earlier in his career he was deputy director of House Information Systems, the technology support organization of the U.S. House of Representatives.

Alan Paller

Alan Paller founded STI, a regionally accredited college and graduate school, and SANS, a global provider of cybersecurity training whose 185,000 alumni are technical cybersecurity professionals protecting 17,000 government agencies, non-profit organizations, and business enterprises. Alan created the CyberStart America program with 26 state governors, which enabled tens of thousands of young women and men to discover their talent and ability to excel in cybersecurity. CyberStart inspired students to pursue a cyber career, while also allowing them to compete for $2 million in college scholarships to help them attain their potential and ultimately start a career in cybersecurity. Alan oversees a global program celebrating people responsible for remarkable improvements in cybersecurity and chairs the annual RSA keynote, "The Five Most Dangerous New Attack Vectors." He has testified multiple times before the US Senate and House and was an initial member of President Clinton's National Infrastructure Assurance Council and winner of the 2005 Azimuth Award, a lifetime achievement award recognizing outstanding service of a single, non-government person responsible for improving federal information technology. In 2010, the Washington Post named him one of seven people "worth knowing in cybersecurity." Alan co-chaired the DHS Task Force on Cyber Skills and headed the FCC Task Force on Best Practices in Cybersecurity. Earlier in his career Alan helped build one of the first large public software companies.

ISBN 978-0-578-83950-9
US$25.00
52500>
9 780578 839509

CIO
INSTITUTE
CIO.org