2020 IT & security talent pipeline study

How successful organizations go beyond degrees and experience to fill open cybersecurity roles.

INFOSEC™

Summary

We've all heard it before — there are not enough cybersecurity professionals to fill open positions. Most agree the skills gap is a significant challenge for employers in nearly all industries and regions, but opinions over why it persists vary widely. Some say it's a lack of qualified candidates. Others believe employers are looking for elusive "unicorn" candidates that do not exist. Opinions aside, what's missing is actionable guidance to help hiring managers fill vacant cybersecurity roles.

In March 2020, Infosec surveyed over 250 IT and security hiring managers in the U.S. to learn what drives their hiring decisions. The study analyzed employer emphasis on candidates' skills, aptitude, experience, degrees and certifications across three candidate experience levels — and compared their responses to how they assessed their own ability to fill open cybersecurity roles.

Nearly all survey respondents (73%) reported challenges filling open cybersecurity positions, yet major differences emerged when the responses from successful hiring managers were compared to those who struggle. The study found hiring managers at organizations experiencing recruiting success:

- Are more likely to actively recruit and screen their own candidates
- Are more likely to hire inexperienced candidates
- Rely more on degrees and certifications as indicators of success
- Value cultural fit more than their counterparts
- Have established reskilling programs in place
- Are more likely to use projects in the evaluation process
- Place greater emphasis on in-person recruiting at industry events and conferences over traditional, passive methods like job boards and online networking sites

What are successful hiring managers doing differently?

113%
more likely to recruit their own candidates

58%
more likely to screen their own candidates

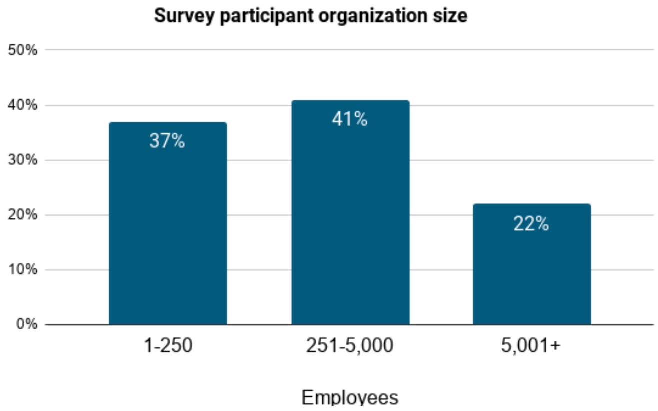
433%
more likely to use projects during the evaluation period

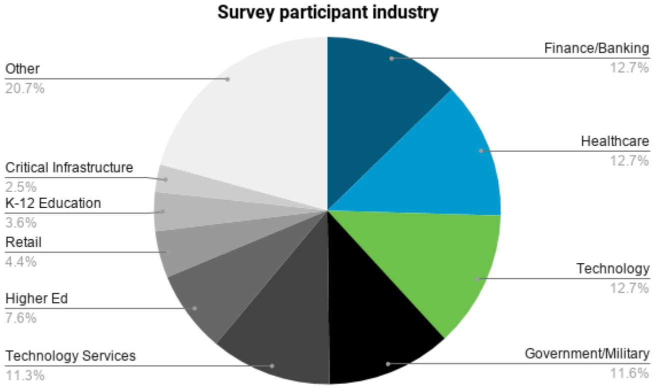
Survey methodology

The 2020 IT & Security Talent Pipeline Study surveyed over 250 IT and security hiring managers across the U.S. Infosec solicited responses from its own database, as well as the database of Osterman Research, a leading security market research firm, to diversify survey results. Respondents were sourced from a variety of industries and company sizes to ensure a representative and robust data set.

The 2020 IT & Security Talent Pipeline report primarily focuses on insights from the following cohorts:

- Respondents who strongly agree or agree their organization is doing a good job filling open cybersecurity positions
- Respondents who strongly disagree or disagree their organization is doing a good job filling open cybersecurity positions
- Respondents from small- to mid-sized organizations (<5,000 employees)
- Respondents from large organizations (>5,000 employees)



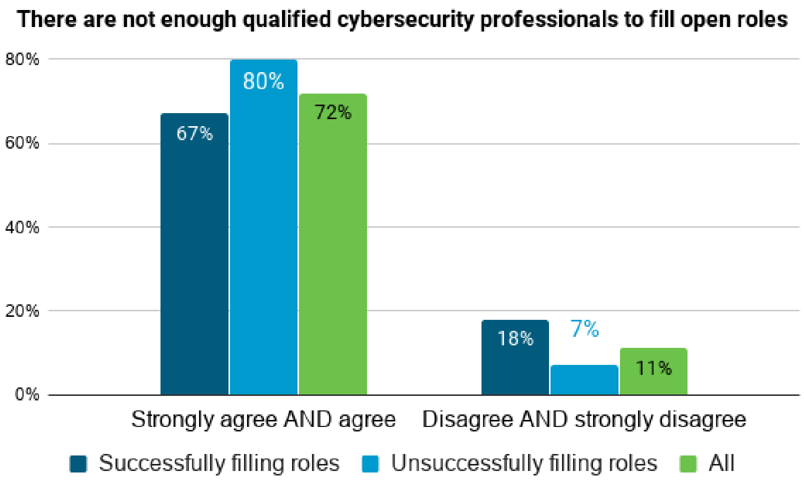


The report makes several references to entry-, mid- and advanced-level roles. The survey defined these as:

- Entry-level roles: 0-3 years of experience
- Mid-level roles: 4-6 years of experience (includes senior roles with specialized skills)
- Advanced-level roles: 7+ years of experience (includes managerial roles)

Cybersecurity skills gap: self fulfilling prophecy?

It's common to hear practitioners, pundits and media outlets rebuke the validity of the cybersecurity skills gap claim. An organization's location, reputation and staffing needs are just a few factors that impact how the cybersecurity talent shortage affects their ability to fill open roles. While most survey respondents in the 2020 IT & Security Talent Pipeline Study agreed there are not enough qualified cybersecurity professionals to fill open roles



(72%), hiring managers from organizations with successful recruiting strategies are much more likely to challenge the skills gap theory. Unsurprisingly, hiring managers unsatisfied with their organization's hiring efforts are more likely to point to the skills gap as a major hiring challenge — even more so than all survey respondents.

Top of funnel analysis: how HR and hiring manager responsibilities vary

Many conversations around cybersecurity hiring challenges focus on the candidates — their credentials, skills and experience — and how deficits in these three areas contribute to the growing skills gap. The 2020 IT & Security Talent Pipeline Study looks further up the talent pipeline to explore the strategies and tactics used by organizations and hiring managers recruiting for open roles.

Recruiting and hiring is not unlike a sales funnel. Individuals responsible for writing job descriptions, recruiting talent and screening candidates have a tremendous impact on an organization's ability to fill the top of their recruiting funnel with qualified candidates. The role of human resources in this process is significant, but findings from the 2020 Infosec study show more engaged hiring managers play a critical role in successfully filling open positions.

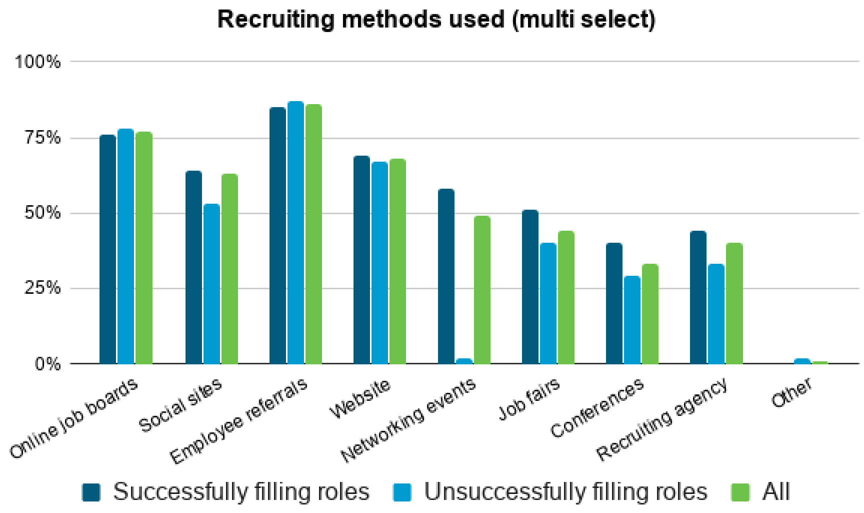
Recruiting and hiring responsibilities: Hiring managers vs. HR

	Successfully filling roles		**Unsuccessfully filling roles**		**All**	
N	106		45		267	
	Hiring manager	HR	Hiring manager	HR	Hiring manager	HR
Write job descriptions	75%	24%	71%	24%	76%	22%
List job openings	26%	72%	4%	91%	16%	82%
Recruit candidates	34%	61%	16%	73%	26%	66%
Screen candidates	49%	50%	31%	64%	43%	55%
Interview candidates	85%	13%	87%	11%	88%	10%
Conduct aptitude tests	62%	34%	42%	53%	54%	40%
Contact references	23%	74%	22%	71%	24%	72%

Hiring managers who agree or strongly agree their organization is doing a good job recruiting candidates are more likely to recruit and screen candidates and conduct their own aptitude and personality tests during the hiring process. Hiring managers who are unsatisfied with their organization's ability to fill open roles were less involved in these processes than both their counterparts and all survey respondents.

When it comes to recruiting, successful organizations do more

The cybersecurity community is small and tightly knit, which means how and where organizations recruit talent has a major impact on their ability to fill open roles. The 2020 IT & Security Talent Pipeline Study asked hiring managers to share their go-to recruiting methods, which included several traditional, passive recruiting



methods like online job boards, as well as active, in-person recruiting methods like attending industry conferences and professional networking events.

Unsurprisingly, hiring managers at organizations doing a good job filling open roles reported leveraging more tactics overall (4.9 vs. 3.9 on average) and were significantly more likely to actively recruit talent at industry events, conferences and job fairs. They were also more likely to use an external recruiting agency in the hiring process.

Even successful organizations struggle, but they struggle less

With 72% of all survey respondents confirming there are not enough qualified candidates to fill open cybersecurity positions, it's not surprising that organizations who are doing a good job filling open roles are still facing challenges along the way. 71% of hiring managers from these organizations report challenges finding qualified candidates, compared to 89% of those who are not satisfied with their organization's ability to fill open roles. So while they are challenged, they struggle less overall.

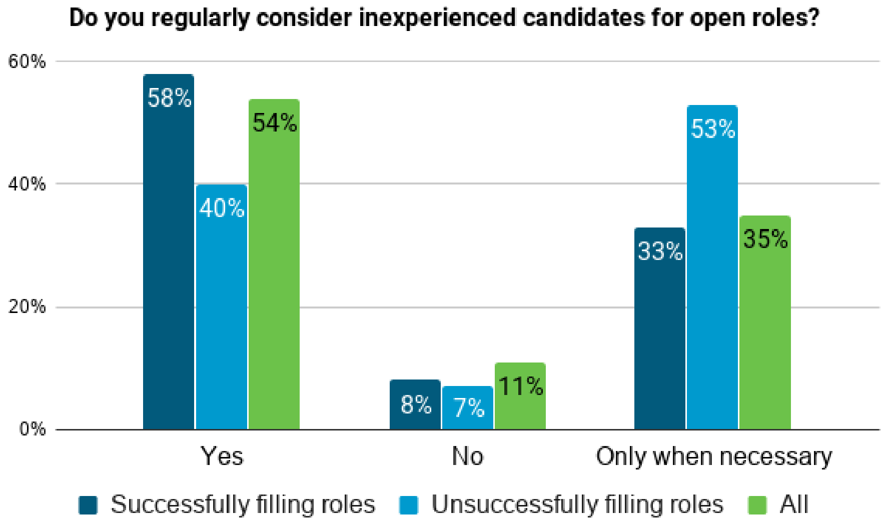
Hiring managers who experience more success filling open positions report fewer challenges on average (2.7 vs. 3.4). Most notably, they are significantly less likely to report a lack of candidate skills, education or certifications as challenges during the hiring process. They are also less likely to report an applicant shortage or salary requirements as a hiring concern.

Hiring challenges facing organizations

	Successfully filling roles	Unsuccessfully filling roles	All
N	106	45	260
Too few applicants	39%	51%	43%
Candidates do not meet technical skill requirements	66%	80%	70%
Candidates do not have required education and/or certifications	33%	40%	36%
Candidates do not have sufficient related job experience	64%	69%	63%
Our office is located in a competitive labor market (e.g., DC Metro)	20%	24%	25%
Candidates' salary requirements are too high	42%	64%	49%
Other	8%	11%	7%

Are hiring managers over emphasizing candidate experience?

Hiring managers at organizations doing a good job filling open roles are more engaged in early stages of the hiring process and leverage more recruiting tactics on average than those at organizations that struggle. The 2020 IT & Security Talent Pipeline Study also found they are more likely to consider hiring inexperienced candidates. The differences were telling: 58% of successful organizations

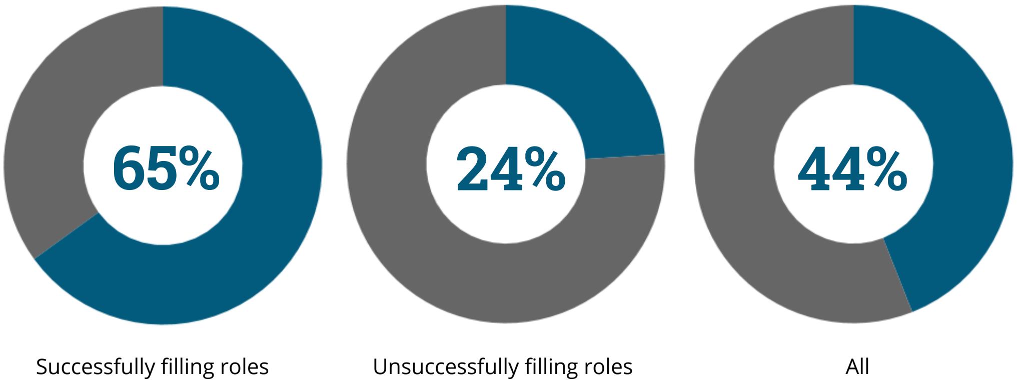


regularly consider inexperienced candidates for open roles compared to just 40% of organizations that struggle. Organizations challenged to fill positions were also less likely to consider inexperienced candidates than all other survey respondents (40% vs. 54%).

Reskilling programs give hiring managers confidence to take risks

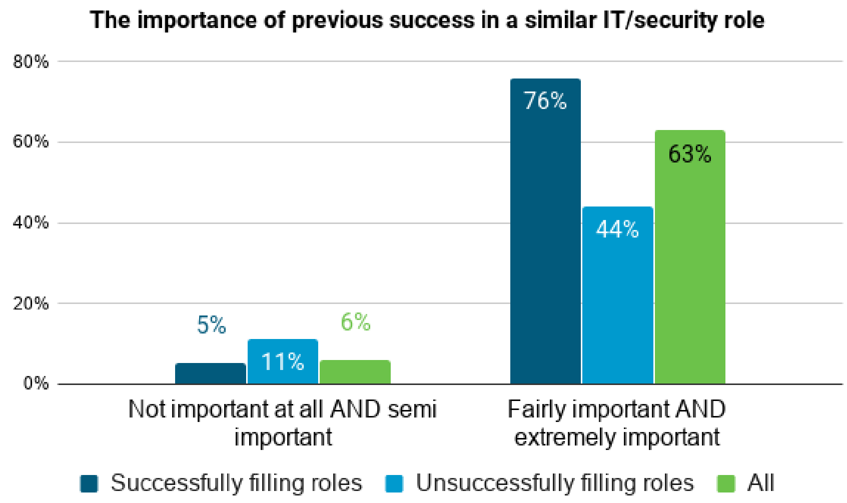
Interestingly, the same hiring managers who are more likely to consider inexperienced candidates are also more likely to work at organizations with established reskilling programs. This suggests that these organizations are more mature in their approach to employee development, which better equips hiring managers to take on inexperienced candidates and train them on the job. If properly resourced, hiring managers facing a lack of qualified candidates should consider removing onerous experience requirements from job descriptions to widen their talent pool and get more candidates into their hiring funnel.

Percentage of hiring managers at organizations with reskilling programs



Proven performers preferred

Data from the 2020 IT & Security Talent Pipeline Study shows hiring managers still place significant emphasis on prior experience, especially hiring managers who are doing better at filling open roles. It's easy to understand the value — candidates with hands-on experience are able to do more immediately upon hire. It's encouraging, however, to learn hiring managers are willing to compromise on this requirement, especially for entry-level positions or when internal employee development resources are available. Aspiring security professionals should not be discouraged by this finding: several training providers like Infosec offer low-cost resources to help build technical skills outside of paid positions and demonstrate proficiency through virtual labs, capture the flag exercises and skill assessments.



Degrees and certifications as indicators of success

The importance of college degrees and certifications in the cybersecurity field is hotly debated. Degrees and certifications are significant investments in terms of both time and resources, and their ability to predict candidate success in a cybersecurity role is not well established. At the same time, degree and certification requirements narrow the top of the recruiting funnel and reduce candidate pool size. Regardless, many organizations — including those excelling at filling open roles — use credentials like certifications to signal a candidate's overall potential. Completion of a degree or certification program suggests candidates can commit to — and complete — a project while also demonstrating their appreciation for professional development.

Hiring managers from organizations doing a good job filling open roles were more likely to emphasize both degrees and certifications in the hiring process. Emphasis on degrees was especially apparent for entry-level positions, where hiring managers had fewer signals to leverage in the candidate evaluation process. Across all respondents, emphasis placed on college degrees increased with role level. Hiring managers from organizations struggling to fill open roles were the least likely to emphasize college degrees in the hiring process.

Importance of four-year degrees

	Successfully filling roles	Unsuccessfully filling roles	All
N	106	45	246
Entry-level roles			
Not important at all AND semi important	29%	60%	42%
Fairly important AND extremely important	45%	18%	30%
Mid-level roles			
Not important at all AND semi important	19%	38%	28%
Fairly important AND extremely important	59%	36%	46%
Advanced-level roles			
Not important at all AND semi important	18%	22%	20%
Fairly important AND extremely important	72%	53%	61%

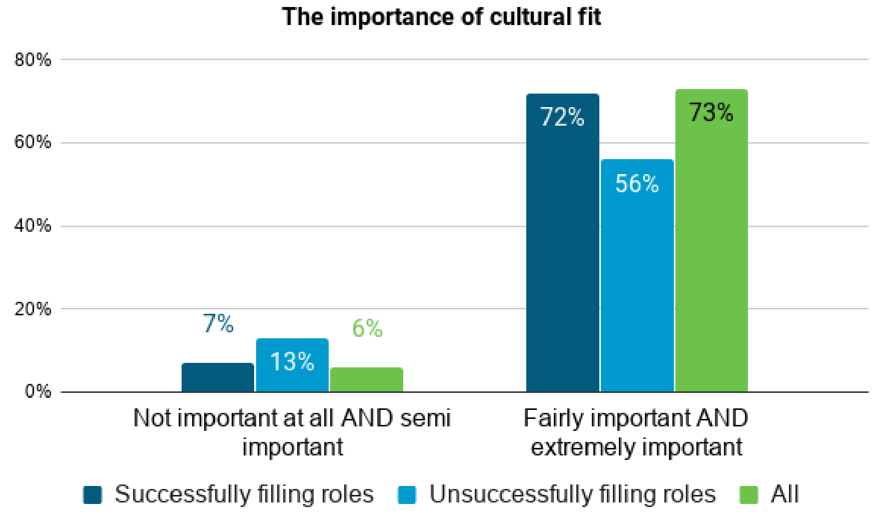
Overall, survey respondents were more likely to rate industry certifications as fairly important and extremely important when evaluating candidate fit. This was especially true for hiring managers at organizations doing a good job filling open roles. Hiring managers in this cohort placed more emphasis on certifications for entry-level positions than their counterparts (45% vs. 18%) and all survey respondents (30%). Like college degrees, emphasis placed on certifications increased with role level across all respondents.

Importance of industry certifications

	Successfully filling roles	Unsuccessfully filling roles	All
N	106	45	246
Entry-level roles			
Not important at all AND semi important	25%	33%	30%
Fairly important AND extremely important	49%	24%	37%
Mid-level roles			
Not important at all AND semi important	14%	13%	18%
Fairly important AND extremely important	63%	44%	52%
Advanced-level roles			
Not important at all AND semi important	16%	16%	17%
Fairly important AND extremely important	74%	62%	64%

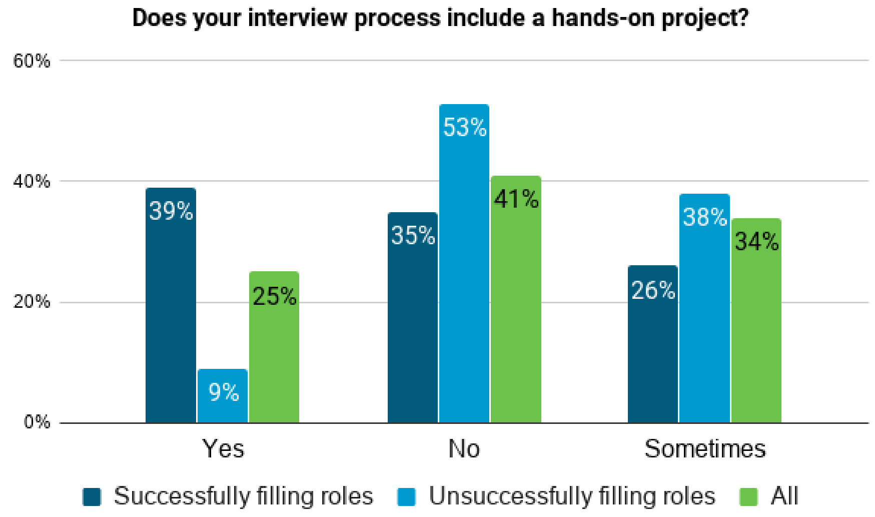
Cultural fit, project-based evaluations and NICE Cybersecurity Workforce Framework competencies — new signals for employers?

Candidates' lack of technical skills and previous experience in similar roles were the top two hiring challenges reported by all respondents in the 2020 IT & Security Talent Pipeline Study. It's unsurprising to learn that employers are looking outside of these traditional qualifications to evaluate candidate fit for open roles. Hiring managers who are more successful filling open positions are more likely to emphasize cultural fit in the hiring process than their counterparts (72% vs. 56%). Hiring managers from organizations struggling to fill open roles valued cultural fit less than all other survey respondents. This suggests that employers challenged to fill open roles should consider shifting focus from experience in the hiring process to overall candidate aptitude and cultural fit to improve recruiting effectiveness.



Projects help organizations identify technical aptitude

Hands-on projects during the candidate evaluation process offer a lower-risk way for employers to de-emphasize experience in favor of demonstrable technical knowledge and aptitude. Hiring managers at organizations who do a good job filling open roles are much more likely to leverage projects in the hiring process to evaluate candidate fit than their counterparts (39% vs. 9%), suggesting organizations who struggle would do well to loosen position requirements in favor of relying on candidate assessments and projects to determine fit.



Employers value softer skill competencies differently

As part of the 2020 IT & Security Talent Pipeline Study, we asked hiring managers to indicate which non-technical competencies from the NICE Cybersecurity Workforce Framework were critical to success in an IT or security role. Across all respondents, the top-five competencies deemed most critical to candidate success were:

- Problem solving
- Critical thinking
- Risk management and ethics
- Oral and written communication
- Interpersonal skills

Employee competencies critical to employee success (multi select)

	Successfully filling roles	Unsuccessfully filling roles	All
N	106	45	248
Problem solving	87%	91%	90%
Critical thinking	83%	91%	88%
Risk management and ethics	69%	62%	69%
Oral and written communication	61%	71%	66%
Interpersonal skills	58%	53%	62%
Knowledge management (information collection and sharing)	45%	58%	48%
Organizational awareness	42%	49%	47%
Data analysis	54%	31%	46%
Business continuity	42%	29%	39%
Policy management	30%	38%	35%
Strategic planning	37%	27%	34%
Project management	34%	29%	34%
Process control	40%	22%	33%
Teaching others	32%	24%	32%
Asset / inventory management	23%	29%	23%
Mathematical reasoning	25%	11%	17%
Workforce management	16%	11%	11%
Contracting and negotiation	8%	9%	8%

However, no actionable differences were identified between responses from hiring managers who think their organizations are doing a good job filling open roles and those who do not. It's unclear if this is because of a lack of universal interpretation of what the NICE competencies represent, or if hiring managers' experience with competency-based assessment and evaluation is limited. Regardless, evaluating candidates based on cultural fit and competency — either in addition to or instead of traditional experience and credential requirements — offer employers a new way to widen their talent pipeline and evaluate candidate fit.

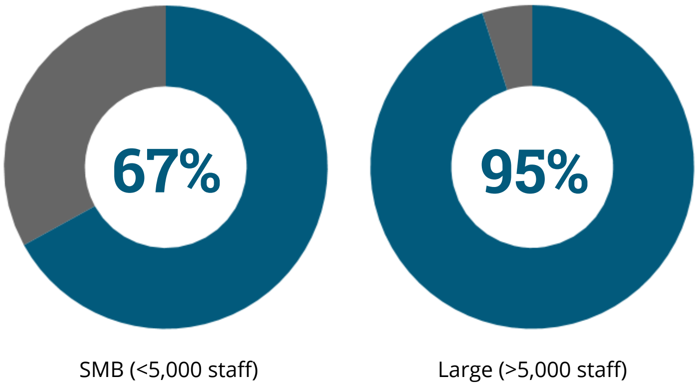
Smaller organizations less affected by hiring challenges

Survey responses among small- to mid-sized (<5,000 employees) and large organizations (>5,000 employees) varied in interesting ways. Smaller organizations were less likely to recognize the cybersecurity skills gap as a hiring challenge than larger organizations (68% vs. 84%) and were less likely to report hiring challenges overall (67% vs. 95%).

Analysis of reported hiring challenges suggest SMBs place less emphasis on technical skill requirements, education and certifications than larger organizations. Unsurprisingly, SMBs were more likely to report high salary requirements as a hiring challenge facing their organization.

Hiring managers at small- and mid-sized businesses also reported significantly smaller security team sizes: just 35% of SMBs reported security teams larger than 10 people compared to 86% of respondents from large organizations. This suggests SMBs may be less challenged to fill open roles simply because they require fewer candidates overall to staff their teams.

Percentage of organizations regularly challenged to find qualified candidates



Conclusion

Data from the 2020 IT & Security Talent Pipeline Study confirms no organization is immune from the cybersecurity skills gap and related hiring challenges. Even hiring managers who are satisfied with their organization's recruiting efforts still struggle to find candidates with the right combination of skills, credentials and experience to meet role requirements. How hiring managers at such organizations improve recruiting outcomes, however, is insightful:

- They rely less on HR for recruiting and screening candidates, and actively recruit talent at industry events and conferences
- They consider more indicators of success in the hiring process such as cultural fit and performance during a hands-on, technical project
- While they still value previous experience in a similar role, they are more likely to hire inexperienced candidates and invest in employee technical skill development

The cybersecurity skills gap and talent shortage is indisputable. To fill the growing skills gap, organizations must consider widening the top of their recruiting funnel. This means identifying new indicators of candidate success in addition to — or perhaps at times, in favor of — traditional hiring signals like college degrees and previous experience. Aptitude assessments and projects to evaluate skill proficiencies are just a few alternatives organizations can implement now to widen the top of their hiring funnel, diversify their candidate pool and improve recruiting outcomes.

About Infosec

At Infosec, we believe knowledge is power when fighting cybercrime. We help IT and security professionals advance their careers with certifications and skills training. We also empower all employees with security awareness training to stay cybersafe at work and home. Driven by smart people wanting to do good, Infosec educates entire organizations on how to defend themselves from cybercrime. It's what we do every day — equipping everyone with the latest security skills so the good guys win.

Learn more at infosecinstitute.com.