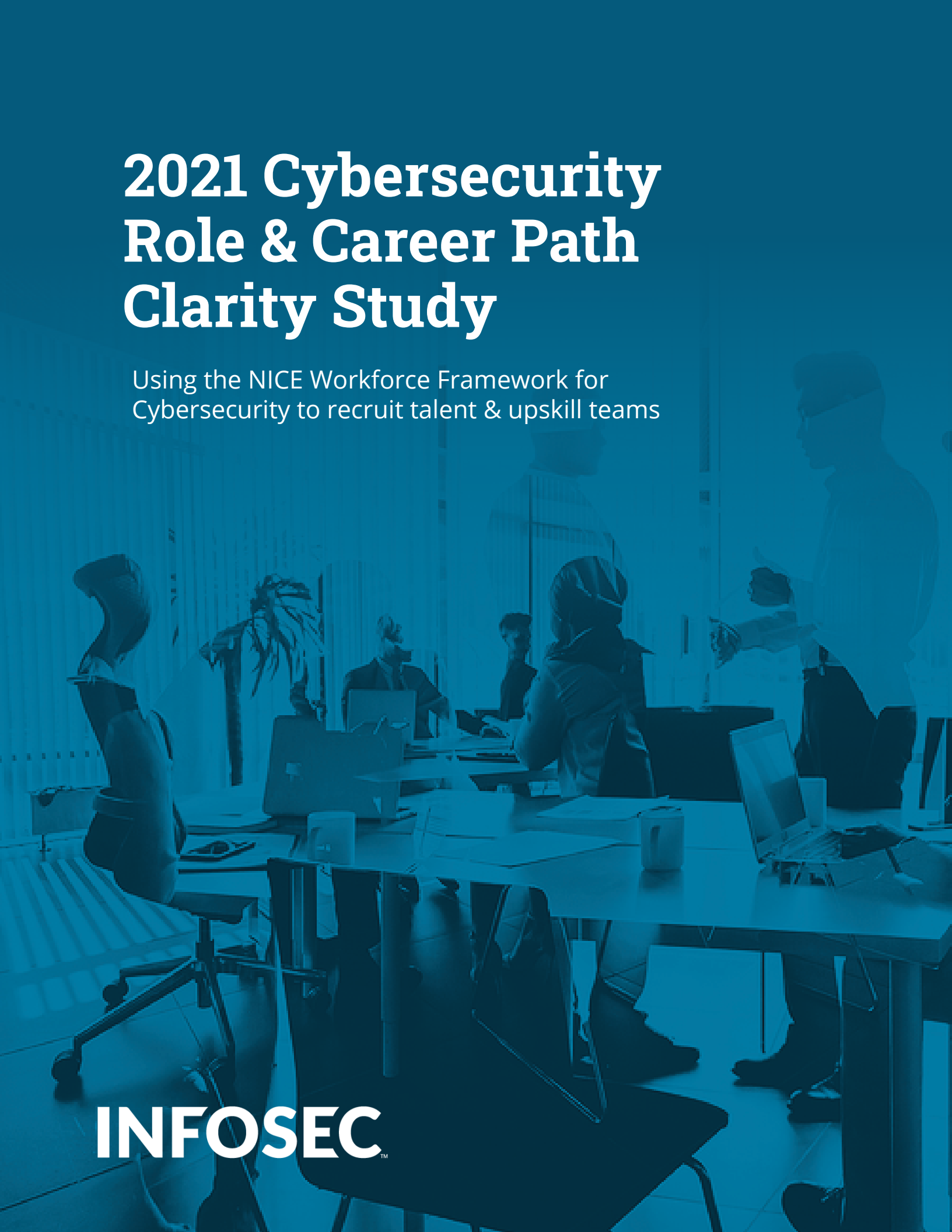
2021 Cybersecurity Role & Career Path Clarity Study

Using the NICE Workforce Framework for Cybersecurity to recruit talent & upskill teams



INFOSEC™

Summary

Identifying, recruiting and retaining cybersecurity talent is one of the biggest challenges facing our industry. While advances in cybersecurity tools and tech are important, the majority of security incidents are attributed to understaffed, undereducated and under-resourced cybersecurity teams. This is not a small challenge. Last year, Infosec's 2020 IT & Security Talent Pipeline Study revealed 73% of U.S.-based cybersecurity hiring managers face challenges filling open cybersecurity positions. Reported challenges included too few applicants overall, and of course, a lack of adequately skilled and seasoned cybersecurity pros.

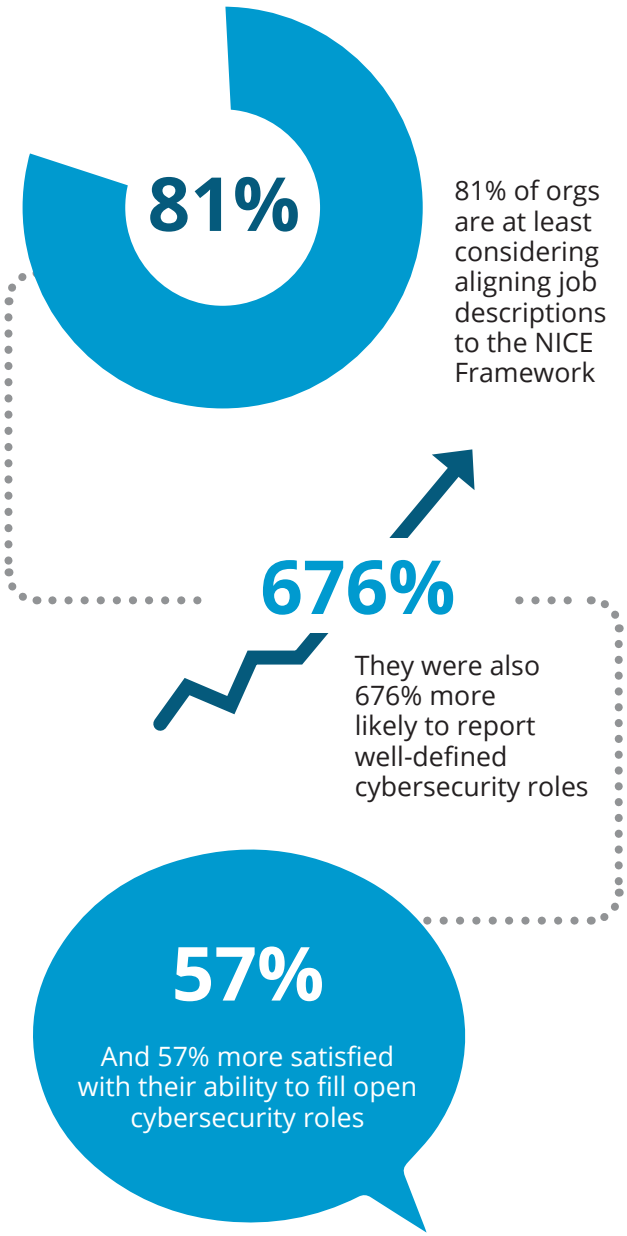
To better understand the steps enterprises are taking to address these challenges, Infosec surveyed over 370 cybersecurity leaders in the U.S. and Canada about resources used to structure job descriptions and development plans. Responses were then compared to employee training program investments, organizations' ability to fill open cybersecurity roles and sentiments toward resources like the NICE Workforce Framework for Cybersecurity (NICE Framework). The study specifically analyzed the following data points by team size, organization size and industry:

- Job description and career path clarity
- Employee development program maturity
- Resources used to create job descriptions and employee development plans
- Adoption rates of frameworks like the NICE Framework
- Satisfaction with organization's ability to recruit and hire cybersecurity candidates

While resources used to guide job descriptions and employee development plans varied widely across all organization sizes and industries, adoption of tools like the NICE Framework had the largest influence on organizations' abilities to fill open cybersecurity roles. Overall:

- 81% of organizations reported they were at least considering aligning cybersecurity job descriptions to the NICE Framework
- That same cohort was 676% more likely to report very to extremely well-defined cybersecurity job roles and responsibilities
- And 57% more likely to report satisfaction with their ability to fill open cybersecurity roles than respondents at organizations with no intent to map job descriptions to NICE

NICE Framework benefits

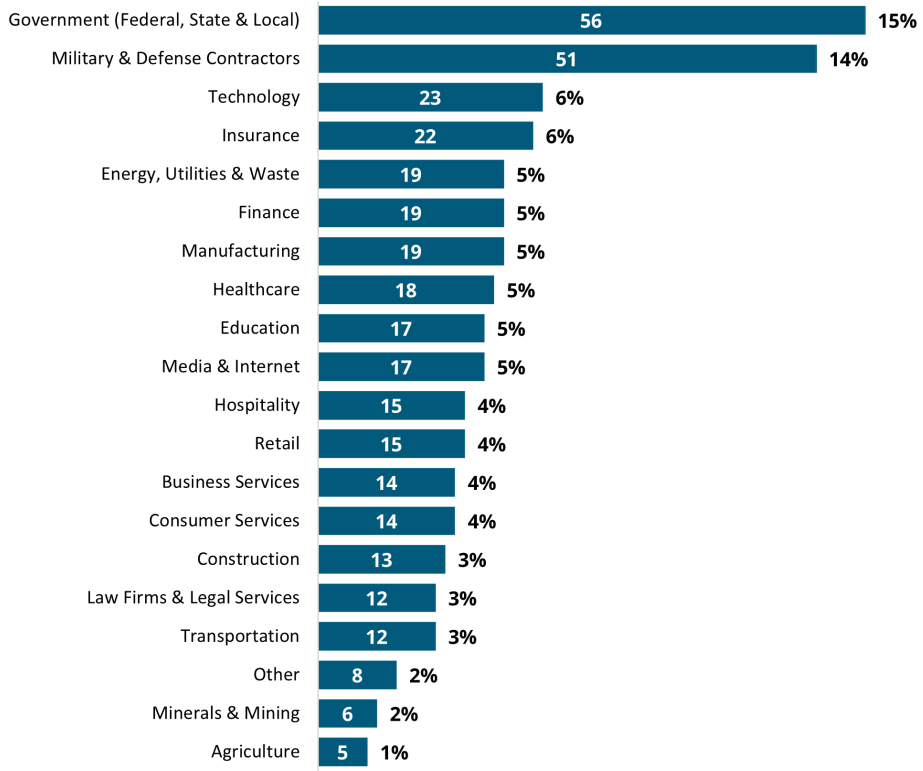


Survey methodology

The 2021 Cybersecurity Role & Career Path Clarity Study surveyed over 370 IT and security team managers from U.S. and Canada-based organizations with at least 1,000 employees. Data was collected in late 2020 and analyzed in early 2021. 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, and received a nominal incentive for their participation.

The project was directed and authored by Megan Sawle, VP Marketing at Infosec, with data analysis conducted in collaboration with University of Wisconsin Research Program Manager and MolMoi Biosciences CEO Margaret Phillips, Ph.D, PMP.

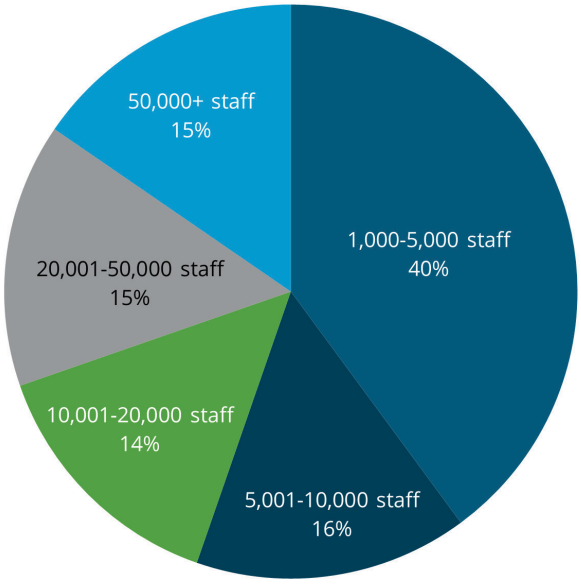
Industry participation



IT & cybersecurity teams scale with enterprise size

Mystery and ambiguity around cybersecurity team sizes, titles and responsibilities has long plagued tech industry analysts in the security space. Even the largest and most sophisticated data enrichment vendors fail to segment cybersecurity roles outside of the IT function, aggregating them alongside a wide variety of IT roles from software engineer to help desk technician. To better understand how IT and security team sizes scale with organization size — and presumingly, IT and security needs — the 2021 Cybersecurity Role & Career Path Clarity Study asked participants to share their IT team size, as well as

Organization size



the number of staff in dedicated cybersecurity roles.

Overwhelming, study participants from larger organizations reported the biggest IT teams. This was especially evident as employee counts exceeded 10,000.

As IT team sizes grew, so did the likelihood and amount of dedicated cybersecurity expertise to support the enterprise. This trend was especially notable at organizations with more than 20,000 employees.

The study also analyzed team sizes by industry to better understand how IT and security talent pipeline needs vary among verticals. Industry segments in the study were not large enough to generate statistically significant findings and should be viewed with caution; however, results warrant further research to validate results and confirm trends shared here and throughout the study.

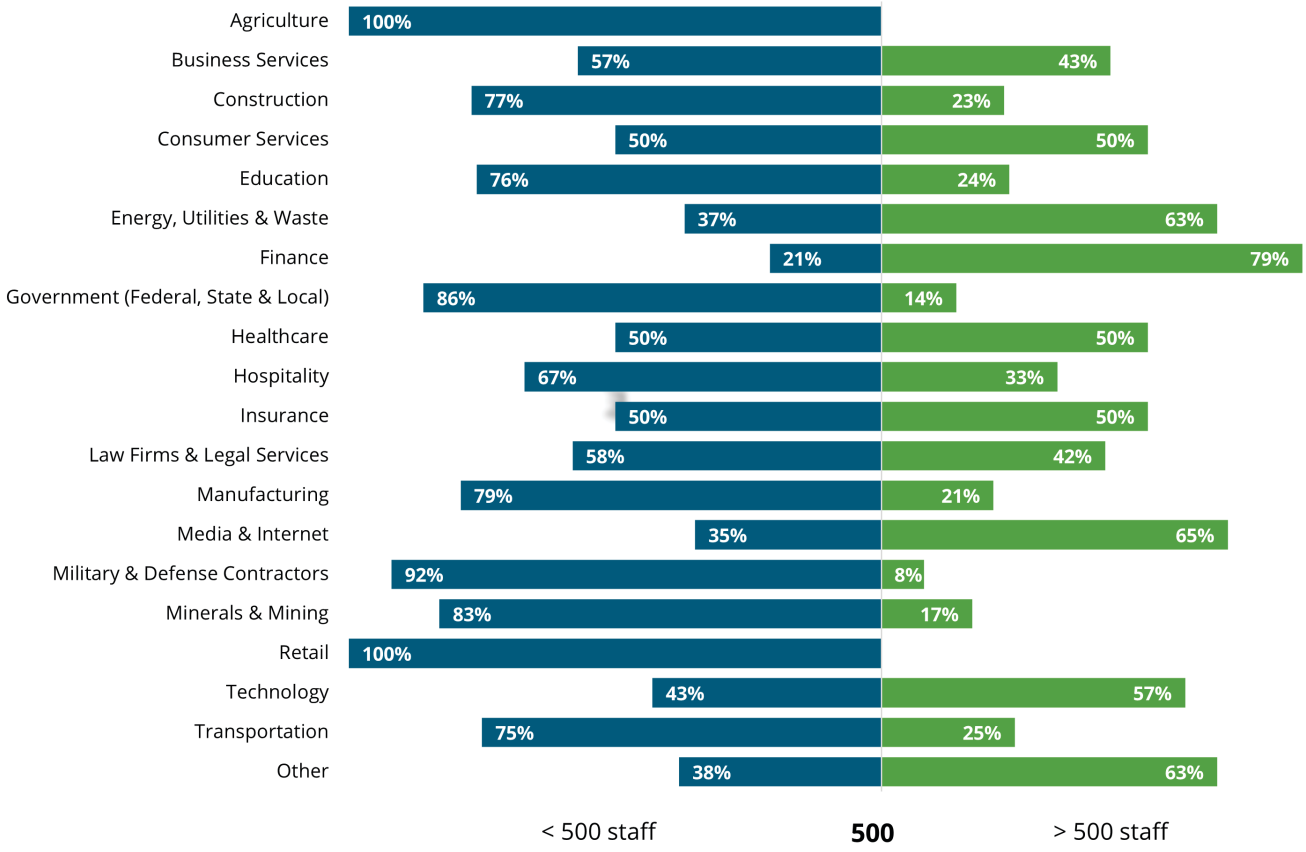
IT team size by org size

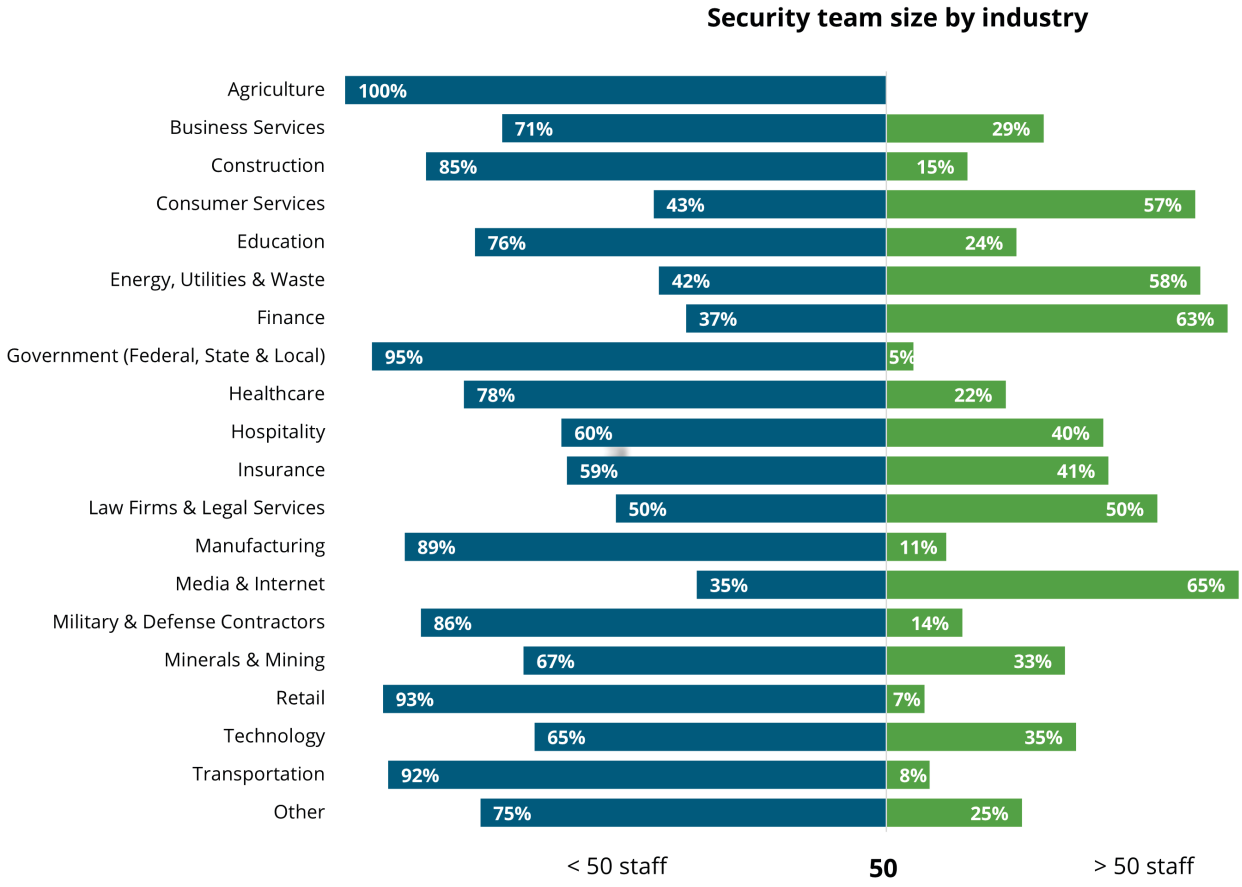
	1k-5k emp.	5k-10k emp.	10k-20k emp.	20k-50k emp.	50k+ emp.
1-50 IT	89%	8%	3%	0%	0%
51-500 IT	32%	29%	20%	16%	3%
501-2k IT	12%	2%	21%	33%	33%
2k-5k IT	17%	0%	6%	17%	61%
5k+ IT	0%	3%	14%	21%	62%

Security team size by org size

	1k-5k emp.	5k-10k emp.	10k-20k emp.	20k-50k emp.	50k+ emp.
0-9 security	77%	12%	6%	3%	2%
10-50 security	34%	27%	16%	17%	6%
51-250 security	3%	4%	31%	35%	27%
251-500 security	0%	0%	6%	13%	81%
500+ security	6%	0%	0%	0%	94%

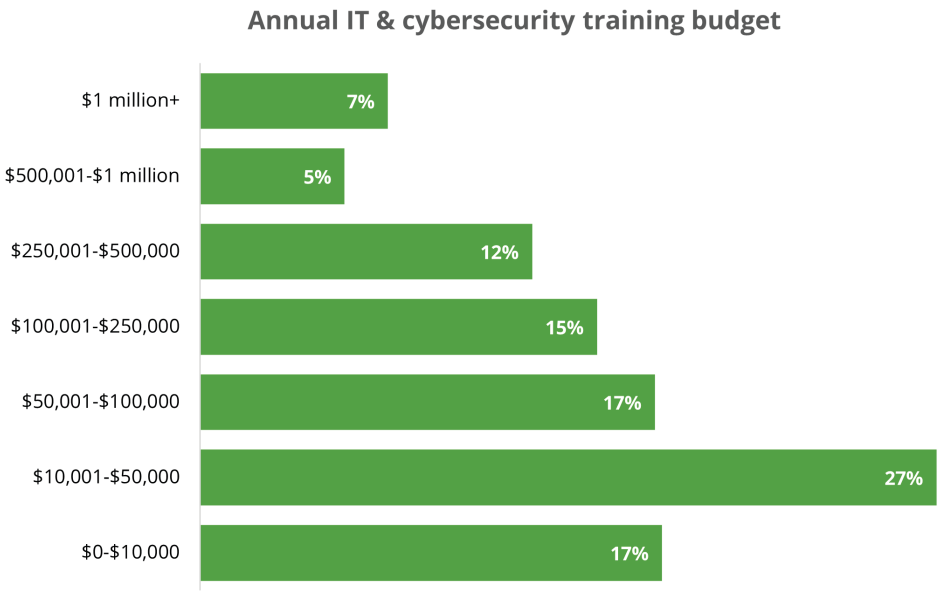
IT team size by industry





Combating the half-life of tech skills with training

Practitioners in the cybersecurity space often reference the half-life of technical skills — or how skills lose value overtime — when making the case for continuous employee skill development. Recent research from IBM suggests most professional skills lose 50% of their value every 5 years; for technical roles, it's even shorter. Why, how and how much an organization allocates to IT and cybersecurity training offers insights into their employee development program maturity and the steps being taken to combat the shrinking half-life of technical skills.



The 2021 Cybersecurity Role & Career Path Clarity Study found IT and security training budgets typically scale alongside organization and IT team size. This was especially true in relation to IT team size, where teams of 500 staff or more were more likely to spend at least $100,000 upskilling their staff each year.

Finance, energy/utilities & media/internet report largest IT teams, budgets

Of the 20 industry segments analyzed in the study, finance, media/internet, energy/utilities and consumer services emerged as leaders in terms of IT and security team sizes and training budgets by industry. Agriculture, retail and government reported the smallest IT and security team sizes and training budgets, while finance, media/internet, energy/utilities and insurance reported the largest.

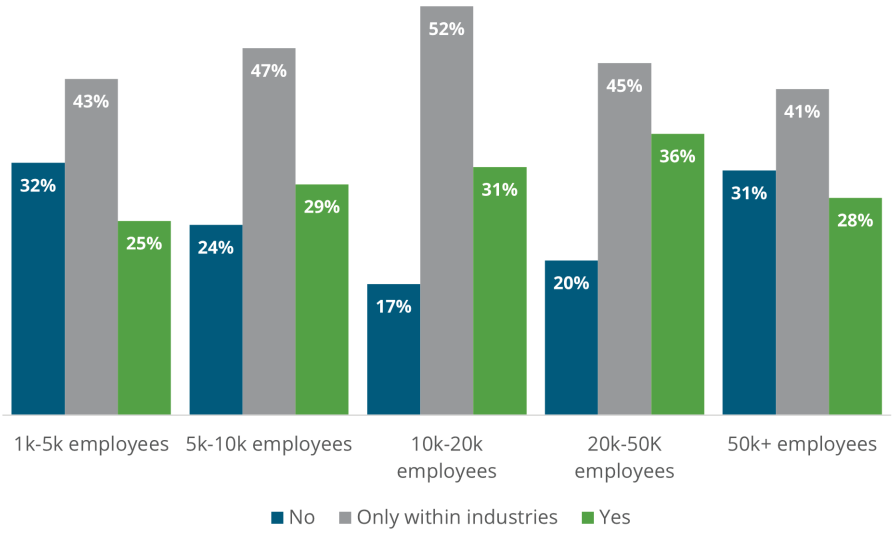
IT team size		Security team size		IT & security training budget	
Smallest	**Largest**	**Smallest**	**Highest**	**Smallest**	**Highest**
Agriculture	Finance	Agriculture	Media / internet	Agriculture	Finance
Retail	Media / internet	Government	Finance	Retail	Media / internet
Military / defense	Energy / utilities	Retail	Energy / utilities	Government	Insurance
Government	Technology	Transportation	Consumer services	Education	Consumer services
Minerals / mining	Consumer services, healthcare, insurance	Manufacturing	Law / legal	Construction	Energy / utilities

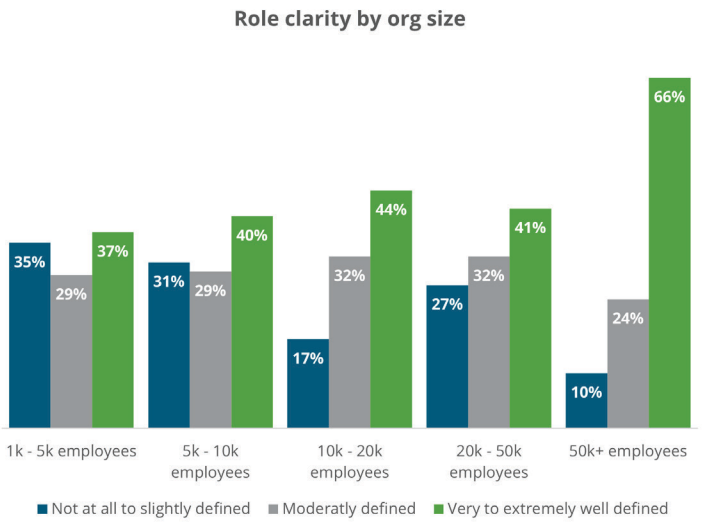
Cybersecurity roles & career paths remain murky for many

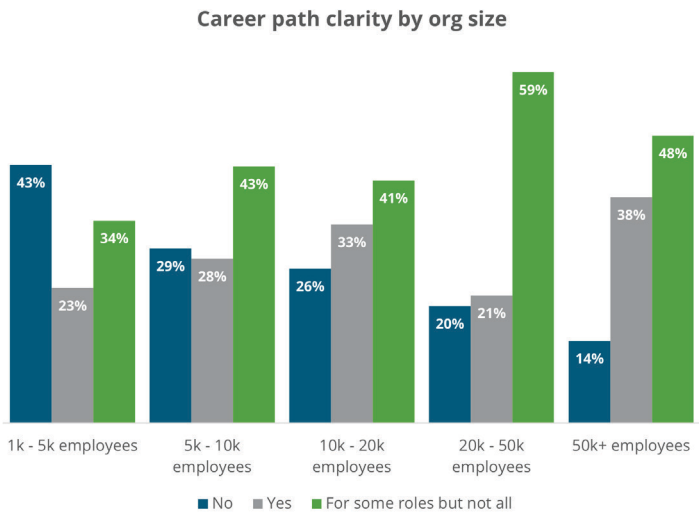
Resources like the NICE Framework establish a common lexicon to more clearly describe cybersecurity roles, responsibilities and career paths, while also making it easier to understand the knowledge, skills and competencies needed to support specific cybersecurity functions within an organization. Initiatives like the NICE Framework are essential to breaking down barriers to entry for aspiring cybersecurity professionals — but only if the industry believes cybersecurity role and responsibility standardization is possible. Overwhelming, participants in the 2021 Cybersecurity Role & Career Path Clarity Study reported job role standardization was possible — either generally or within specific industries.

In addition to confirming its feasibility, respondents confirmed cybersecurity role standardization has several benefits, including improving employee retention, recruiting efforts and career path clarity.

Is standardizing cybersecurity titles and roles realistic?



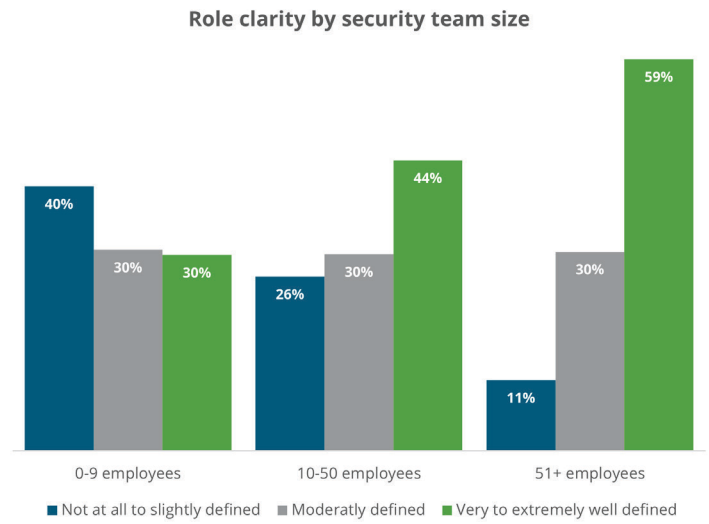


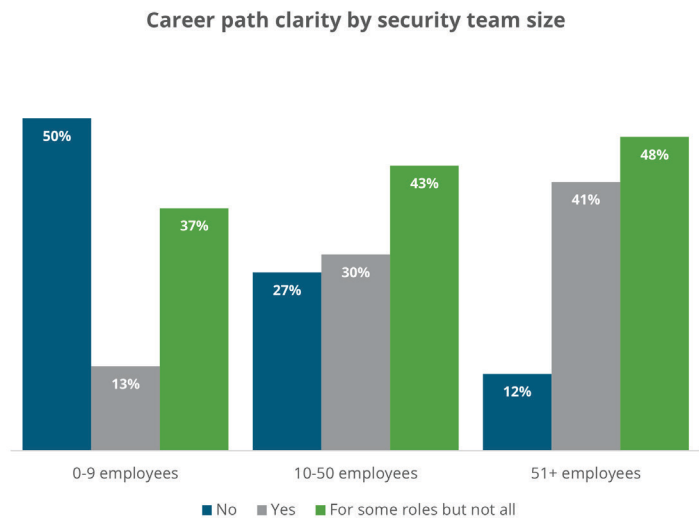


When analyzing reported cybersecurity job role and career path clarity, it's obvious no organization is safe from the cybersecurity role and responsibility ambiguity plaguing the profession. However, as organization size increases, role clarity improves — likely due to larger team sizes and fewer overlapping responsibilities. The study found organizations with more than 10,000 employees were:

- 35% more likely to report well-defined job descriptions
- 55% more likely to report having at least some clearly defined cybersecurity career paths
- 46% more likely to have mature employee development programs with required training

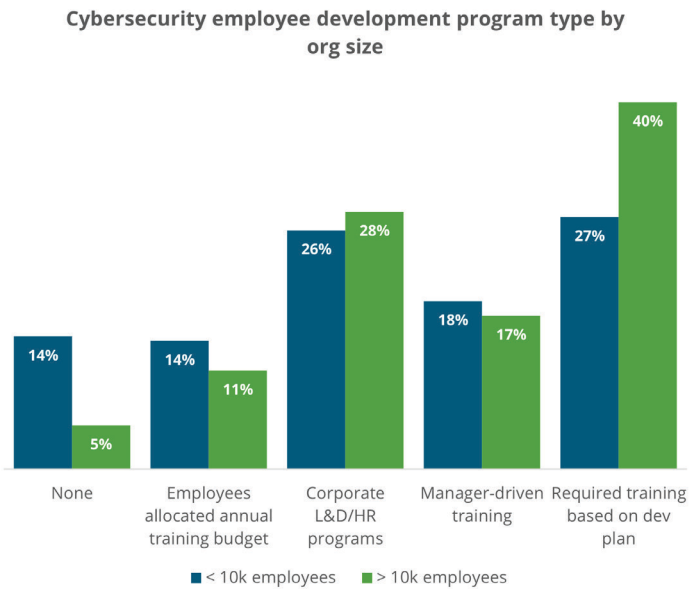
Put another way: cybersecurity job role and career path clarity remains a serious challenge at organizations of all sizes. While larger organizations generally do better, much room for improvement exists to help practitioners better understand their job responsibilities and career potential. Similar differences were observed at the security team size level.

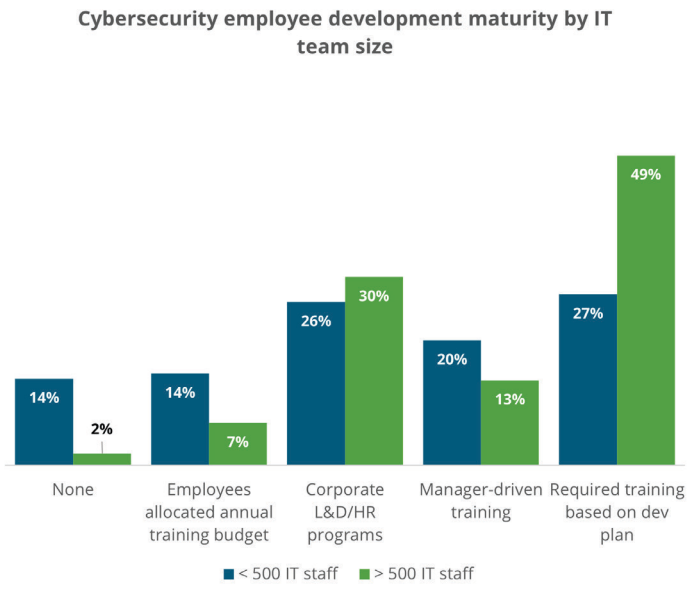




Employee count drives development program maturity

Similar to the job role and career path clarity challenges discussed earlier, organizations with less than 10,000 employees and 500 IT staff underperformed their larger-organization counterparts in terms of



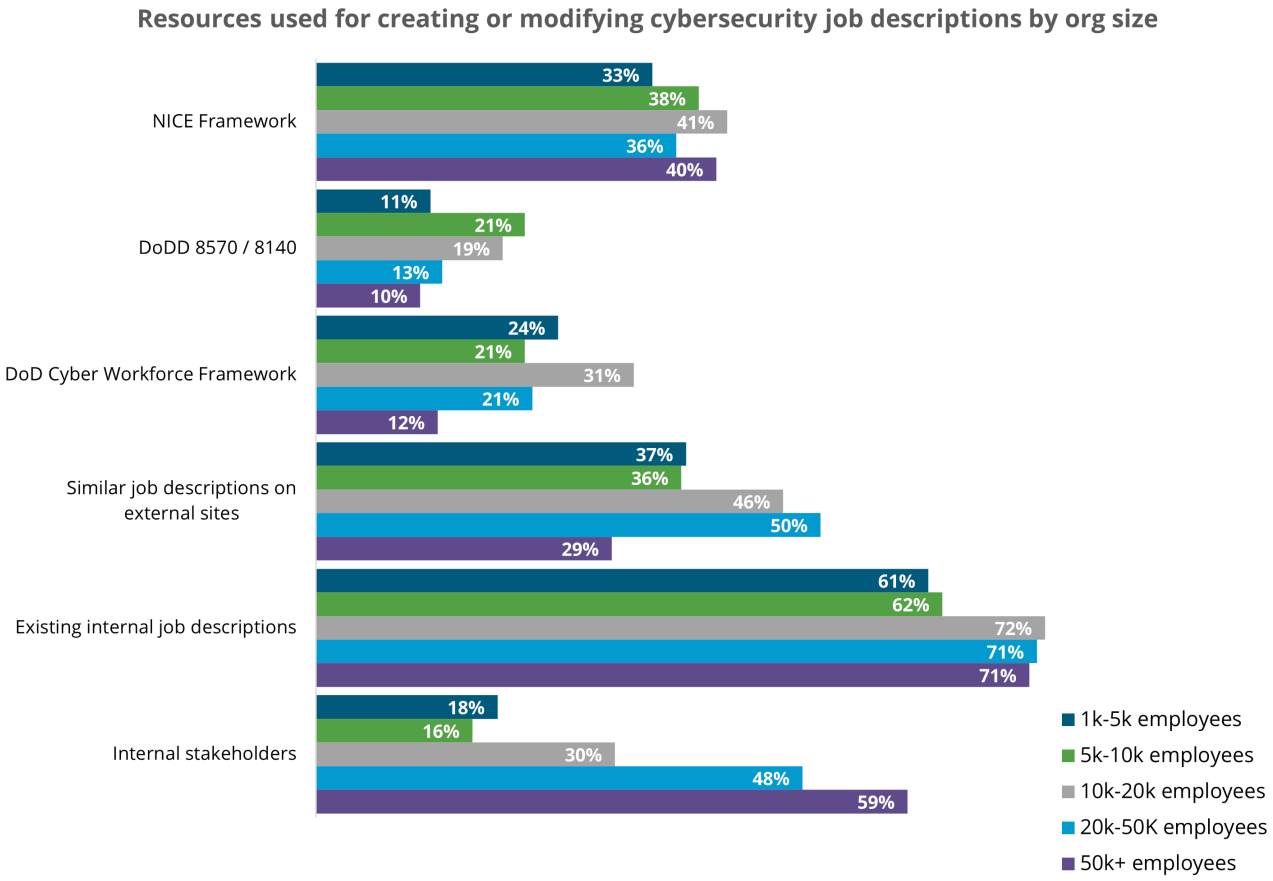


employee development program maturity. It's not surprising when considering they also invested less in IT and cybersecurity education and reported the most ambiguity among cybersecurity job roles and career paths. Why this trend exists between small and large organizations is unknown, but could be attributed to more resourced cybersecurity teams, more dedicated cybersecurity employees and, as a result, less overlap in responsibilities and career growth opportunities.

Finance, energy/utilities & business services lead the way

In terms of cybersecurity role and career path clarity and employee development program maturity, some industries appear to do better. Additional data is needed to confirm the findings below. However, results are interesting: across the 20 industry segments included in the study, finance, energy/utilities, media/internet, business services and military/defense lead with strongest reported role and career path clarity, as well as employee development program maturity.

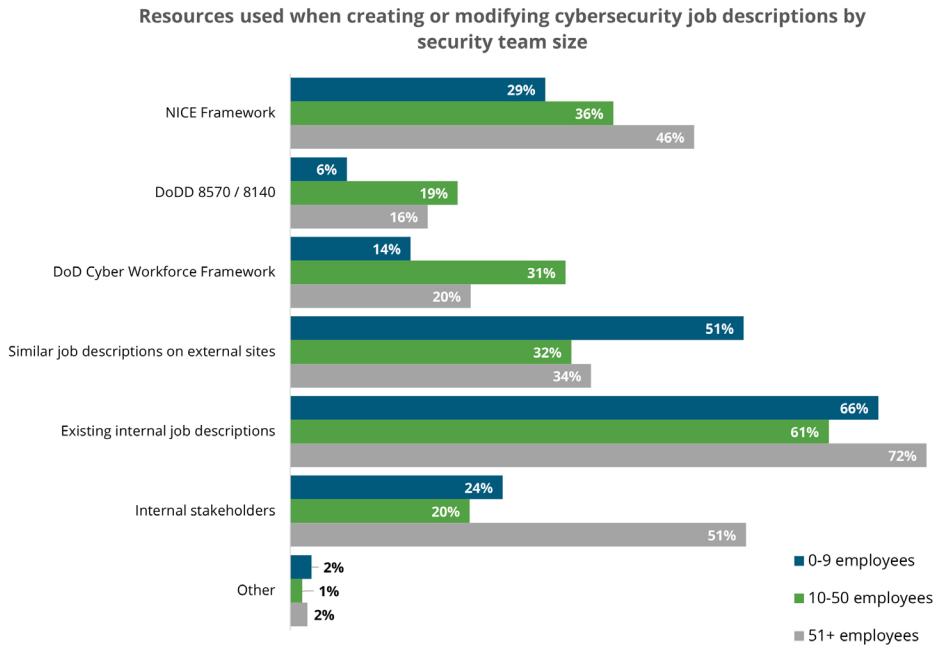
Role clarity		Career path clarity		Emp. dev. program maturity	
Weakest	**Strongest**	**Weakest**	**Strongest**	**Weakest**	**Strongest**
Minerals / mining	Finance	Agriculture	Finance	Agriculture	Insurance
Agriculture	Energy / utilities	Construction	Business services	Hospitality	Business services
Transportation	Media / internet	Healthcare	Energy / utilities	Retail	Finance
Construction	Military / defense	Retail	Military / defense	Education	Media / internet
Hospitality	Technology	Education	Government	Healthcare	Military / defense



Talent pipeline management: familiarity over effectiveness?

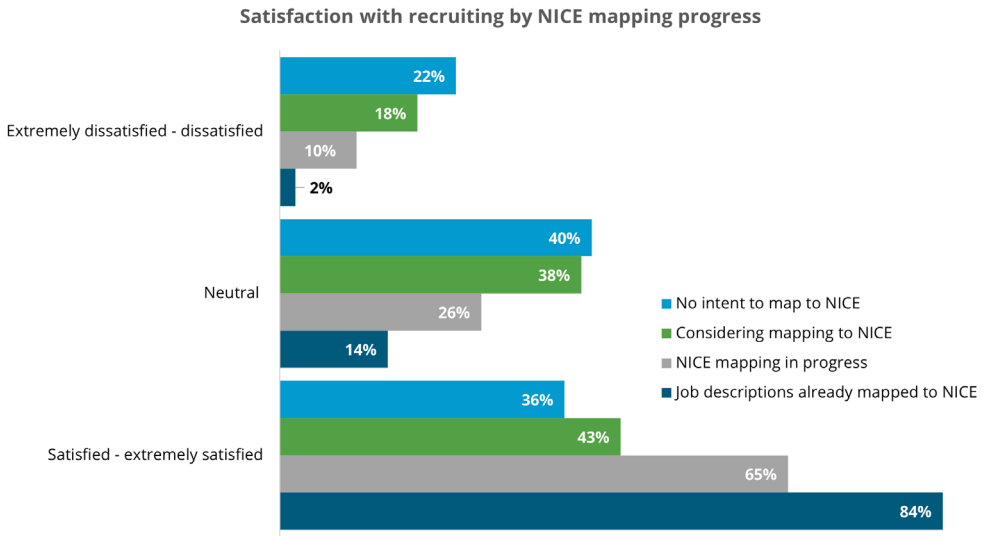
Interestingly, most study participants look to the status quo when building or modifying cybersecurity job descriptions. While organizations with more than 10,000 employees were more likely to consult resources like the NICE Framework, most respondents reported referencing existing or external job descriptions and internal stakeholders when creating cybersecurity job descriptions. This pattern suggests enterprises may be inadvertently entering a "self-fulfilling prophecy" where existing, unclear cybersecurity job descriptions are affirmed by defunct external job postings.

As security team sizes increase, managers are more likely to consult alternative resources like the NICE Framework and work with internal resources when creating or existing cybersecurity job descriptions. IT managers leading large teams are also less likely to consult external job boards for comparative job descriptions.



NICE Framework adopters improve recruiting, role clarity

As organizations increase in size and their talent pipeline needs change, intent to align cybersecurity job descriptions to the NICE Framework increases. Respondents at organizations with more than 5,000 employees were much more likely to consider or pursue aligning their cybersecurity job descriptions to NICE.

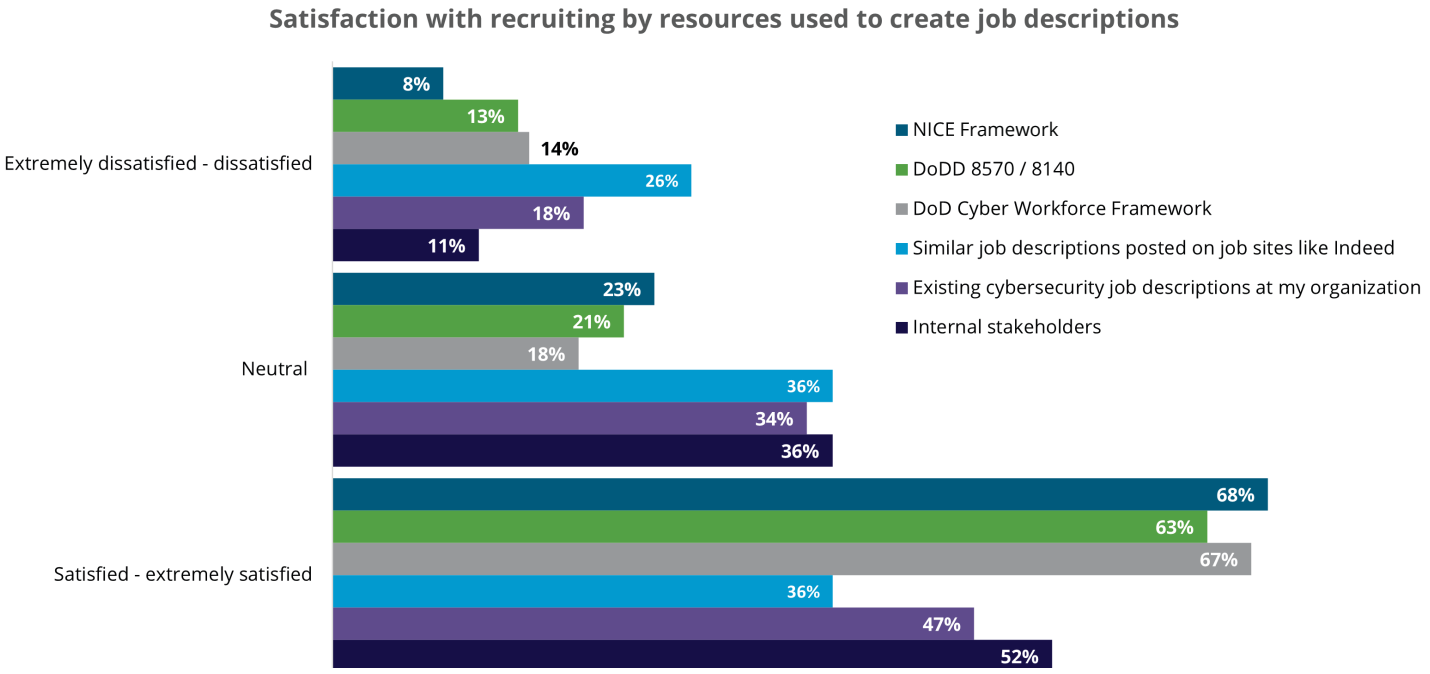


Overall, 81% of all survey participants reported they were at least considering mapping existing cybersecurity roles to the NICE Framework.

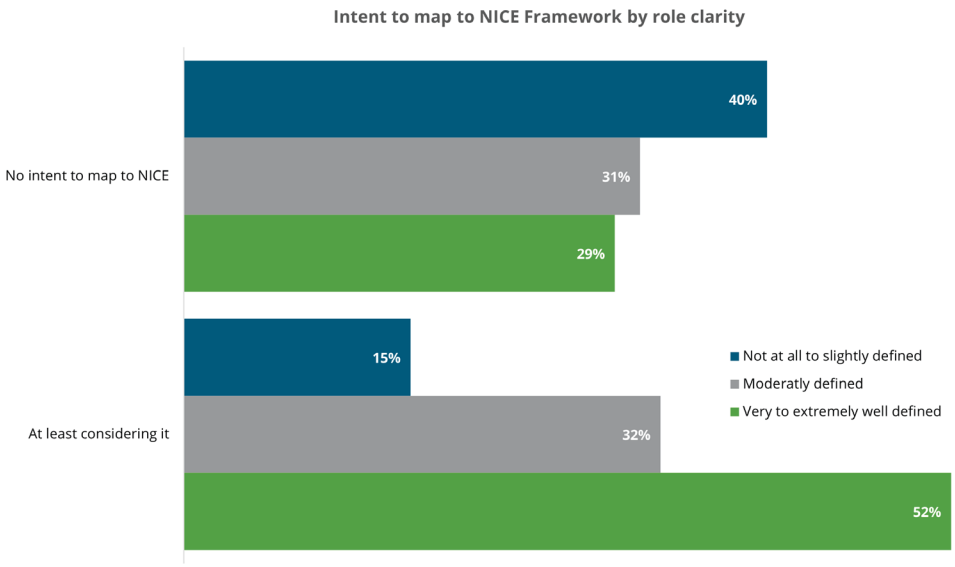
Workforce frameworks work

While resources used to guide job descriptions and employee development plans varied widely across all organization sizes and industries, adoption of tools like the NICE Framework had the largest influence on an organization's ability to fill open cybersecurity roles. Respondents from organizations with cybersecurity job descriptions previously mapped to NICE were 57% more likely to report satisfaction with their ability to fill open cybersecurity roles than respondents at organizations with no intent to map job descriptions to the NICE Framework.

The same advantage was observed when any workforce framework was used, including the DoD Cyber Workforce Framework and the DoDD 8570 / 8140.



Analyzing respondent satisfaction with recruiting efforts against NICE Framework adoption and reported role clarity is telling: organizations that are at least considering mapping cybersecurity job descriptions to NICE were also 676% more likely to report well-defined cybersecurity job roles and responsibilities. Bottom line: workforce frameworks work.



Conclusion

Study after study shows cybersecurity job descriptions lack clarity across most roles and industries — stifling talent recruitment, development and retention efforts. Data from the 2021 Cybersecurity Role & Career Path Clarity Study strongly indicates organizations struggling to recruit and fill open cybersecurity roles should look to workforce frameworks like the NICE Workforce Framework for Cybersecurity to increase hiring success and guide employee development programs.

Respondents from organizations with cybersecurity job descriptions previously mapped to NICE were 57% more likely to report satisfaction with their ability to fill open cybersecurity roles than respondents at organizations with no intent to map job descriptions to the NICE Framework. They also reported the strongest cybersecurity role clarity — very likely a result of their efforts to align with the NICE Framework.

While nearly all survey participants reported challenges in cybersecurity job role clarity and career pathing, it's clear those who look towards innovative and flexible solutions like the NICE Framework — and not to the status quo — benefit from a richer talent pipeline and clearer cybersecurity employee roles and expectations.

About Infosec

Infosec believes knowledge is power when fighting cybercrime. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and privacy training to stay cyber-safe at work and home. It's our mission to equip all organizations and individuals with the know-how and confidence to outsmart cybercrime.

Learn more at infosecinstitute.com.