CYBRARY

2020 Research Survey Report

Cybersecurity skills gap threatens job effectiveness amidst global talent shortage

Survey reveals negative organizational impacts in a world of increasing attacks.

CONTENT

EXECUTIVE **SUMMARY**

65% of IT and Security Managers agree/strongly agree that skill gaps are negatively impacting their team's effectiveness.

In June 2020, Cybrary conducted a survey to assess the current challenges and perceptions of the oft-mentioned cybersecurity skills gap problem faced by IT and security teams worldwide. More than 800 individuals of varying experience, ranging from system admins to CISOs responded. Key takeaways from the survey are reported here.

KEY **TAKEWAY #1**

Growing skill gaps among IT and security professionals are negatively impacting security team effectiveness. As organizations worldwide face a lack of qualified candidates for key positions, improving the job skills of existing staff becomes critical to preventing breaches and protecting IT infrastructure.

Results from Cybrary's research survey shows that nearly 3 out of 4 respondents (72 %) agree/strongly agree that skill gaps exist on their teams. Even more alarming, 65% of IT and Security managers agree/strongly agree these skills gaps have a negative impact on their team's effectiveness. This skills gap is clearly eroding the performance and productivity of IT and security teams. Yet 23% of respondents say their organizations do not enable them to develop the skills needed to be successful in their current role, and another 30% appear unsure.

KEY **TAKEWAY #2**

IT and security professionals are avidly working to improve their skills on their own personal time, even while reporting cost and lack of time as significant barriers. Respondents overwhelmingly preferred online learning for job-related skills (62%) including online courses, virtual labs, and web-based media to help them gain new skills for improving current job performance and advancing their careers.

According to survey respondents, IT and security professionals want to improve their job skills with 40% spending time every day, while another 38% at least once a week. Nearly half (48%) invest their own time before and after work, or on weekends (20%) to improve their skills.

However, cost (33%) and lack of time (28%) are the main barriers preventing IT and security professionals from getting the skills development training they need to do their jobs to the best of their abilities. Even more disturbing, 40% say these barriers have a major/severe impact on developing their skills.

Respondents clearly indicated a preference for learning through online, self-paced courses(38%) along with online virtual labs (17%). Their motivation appears to focus on improving their current job performance (25%) or advancing their careers (29%), rather than pursuing a new career path (13%).

KEY **TAKEWAY #3**

Many organizations are not sufficiently investing in nor actively supporting skills development for their teams. Many respondents feel their organizations do not understand what skills are required of their team members, and a surprising portion of organizations do not track skill development for their IT and security teams at all.

IT and security team members are not getting the full support they need to improve skills since about half of organizations have either decreased their training budgets (22%) or kept them the same (25%) this past year. Even more disturbing, 16% of respondents report their organizations do not have any training budget at all.

Most organizations continue to rely on performance reviews by managers (46%) or job-related assessments (37%) to assess skill proficiencies, as opposed to more objective skill-based assessment (20%) or certification practice tests (17%). Nearly one out of four (23%) of organizations do not track skill development for their IT and security teams at all. And, nearly half (46%) do not confirm new hire skills for specific roles, nor assess the skills of newly onboarded team members (40% rarely or never).

It's clear many organizations do not use skills assessment technologies for newly onboarded team members or new hires joining a team. They are likely missing the opportunities and insights that assessment and tracking tools offer to baseline, measure, and monitor skills development effectively. At the same time, many respondents feel their organizations do not understand what skills are required of their team members (46%), and 38% do not communicate what skills are needed to be successful in a job/role.

RECOMMENDATIONS

The survey results identify obstacles and demonstrate compelling insights into how organizations can make efforts to close skill gaps towards maximizing team effectiveness and keep information assets secure. The data suggests several recommendations that will improve skills development:

1. Acknowledge the implications and challenges associated with the cybersecurity skills gap among security and IT professionals.

While cybersecurity is often considered a top priority, the industry lacks urgency when it comes to skills development practices for individual team members. Organizations need to establish continuous cybersecurity education and professional development not only for security teams, but across multiple disciplines, including HR, IT and management.

The "cybersecurity skills gap" must be bridged by cultivating the talents of existing employees to ultimately protect and maintain critical company data and digital assets.

2. Empower team members to learn on the job.

IT and security teams are already struggling with time constraints and doing their best to improve their skills, even outside of work hours. But it's not enough. Organizations must also provide compelling training solutions so that team members don't have to pay out of their own pockets to acquire the critical skills they need to perform at the highest levels in their roles. Internal development of teams will not only drive an increase in overall efficiency, productivity, and performance, it will improve retention of key staff since they will recognize they have opportunity to grow within their current organization.

3. Organizations need to reevaluate their training solution investments to ensure the resources they provide are effective and can measure and track team skills growth.

The data shows learners are using a variety of learning modalities, but overall skills gaps are not being solved to maximize team performance. The survey strongly indicates that team members heavily prefer (62%) to learning online and at their own pace. Organizations need to employ intelligent and measurable training systems that empower team members to learn needed skills, faster, while providing organizations a better understanding of their training programs ROI.

4. A skills growth mindset must be adopted as a key business priority, and ingrained into each organization's culture.

Simply offering "training" is not sufficient. Organizations must be intentional in assessing their workforce's skills and continually monitoring skill development. By adopting a targeted approach to understanding and solving skill gaps, organizations can establish clear development goals, better communicate to teams, and ensure mutual accountability in achieving their objectives.

INTRODUCTION

Why addressing the cybersecurity skills gap is so critical now?

"It's a full-on war for cybertalent. CEOs know that, so they play hardball. Everyone's throwing money at this."

- Matt Comyns, *Managing Partner at executive search firm Caldwell Partners specializing in information security*

Facing a severe shortage of talent for cybersecurity positions, organizations throughout the world are competing as never before for expertise to bolster their security efforts. While competing to recruit experienced professionals, far too many organizations may be overlooking an issue that is just as important: improving the professional skills of their existing team members --- keeping them happier and more productive.

This "Cybersecurity Skills Gap" report from Cybrary reveals the willingness of IT and security team members to devote their personal time and effort---frequently on nights and weekends---to improve their job skills. Yet they face serious obstacles in terms of the cost and time demands during work which prevent them from increasing their skills. The consequences are dire in a world of constantly escalating cyber threats. Team effectiveness is being significantly reduced due to this skills gap and more investment will be required to remedy the situation.

As the LA Times noted, "The threat of digital breaches — and the fines, lawsuits and executive resignations that sometimes follow — has left companies scrambling to scoop up scarce security experts. The growing compensation packages and broadened responsibilities are a dramatic shift for a group of workers once confined to obscure IT departments, little more than an afterthought to senior management." (1)

Reading this report is a first step in understanding the scope and importance of the cybersecurity skills gap, along with reviewing recommendations that will address the issue with a measurable return on your skills training investment. For more information, contact Cybrary at [email/URL]

KEY **TAKEWAY #1**

Growing cybersecurity skill gaps among IT and security professionals are negatively impacting security team effectiveness. As organizations worldwide face a lack of qualified candidates for key positions, improving the job skills of existing staff becomes critical to preventing breaches and protecting IT infrastructure.

Some of the most alarming results from Cybrary's research survey show that nearly 3 out of 4 respondents (72%) agree/strongly agree that skill gaps exist on their teams. (Figure 1). When looking at those on the front line of cybersecurity efforts, non-manager responses reveal that nearly 70% agree or strongly agree that skill gaps are real.

Figure 1 – Skill gaps exist on your team?

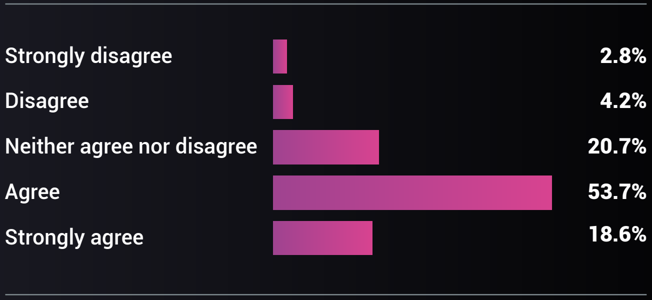
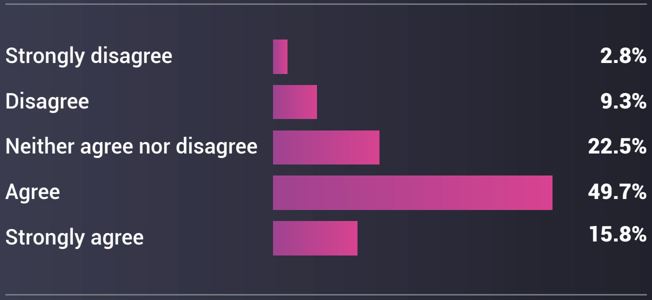


Figure 2 – Skill gaps are negatively impacting your team's effectiveness.



Even more alarming, 65% of IT and security managers agree/strongly agree these skills gaps have a negative impact on their team's effectiveness. (Figure 2)

72%
admit skills gaps exist

65%
of IT Managers say
skill gaps hurt effectiveness

23%
feel their organization does not
enable skill development;
30% unsure

Thus, existing skill gaps are clearly eroding the performance and productivity of IT and security teams. Yet, a significant proportion of respondents do not feel their organizations enable their skill development for their current role (Figure 3) or career advancement (Figure 4). Among the rank and file (non-managers) one in four (approx. 25%) do not feel they are enabled to develop skills for their current role or future advancement, with another 30% unsure, neither agreeing or disagreeing.

Figure 3 – *My organization enables me to develop the skills I need to be successful in my current role.*

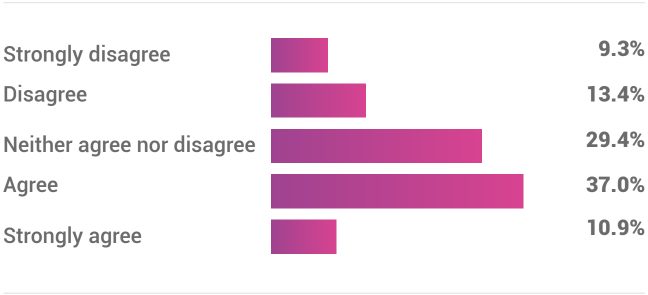
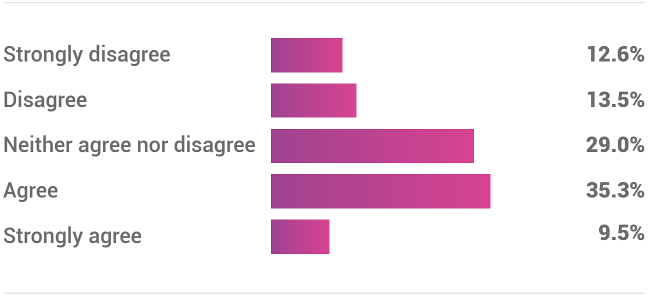


Figure 4 – *My organization enables me to develop the skills I need to advance my career and be successful in future roles.*



RECOMMENDATION

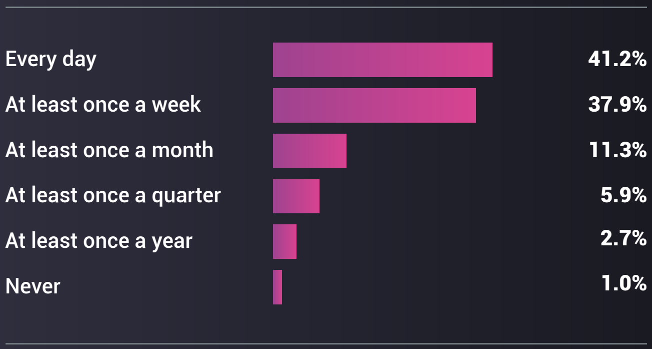
Acknowledge the implications and challenges associated with the cybersecurity skills gap among security and IT professionals.

While cybersecurity is often considered a top priority, the industry lacks urgency when it comes to skills development practices for individual team members. Organizations need to establish continuous cybersecurity education and professional development not only for security teams, but across multiple disciplines, including HR, IT and management. The “cybersecurity skills gap” must be bridged by cultivating the talents of existing employees to ultimately protect and maintain critical company data and digital assets.

KEY **TAKEWAY #2**

IT and security professionals are avidly working to improve their skills on their own personal time, even while reporting cost and lack of time as significant barriers. Respondents overwhelmingly preferred online learning for job-related skills (62%) including online courses, virtual labs, and web-based media to help them gain new skills for improving current job performance and advancing their careers.

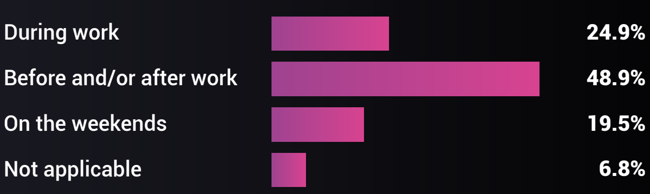
Figure 5 – How often do you spend time developing new job-related skills?



According to survey respondents, IT and security professionals want to improve their job skills as evidenced by more than 40% spending time every day developing job-related skills and another 38% investing in improving their skills at least once a week. (Figure 5)

While a quarter of respondents (25%) do spend time during work to learn new skills, their interest and commitment extend well beyond typical work hours, with nearly half (49%) of the respondents saying they invest their own time before and after work, and on weekends (20%) to improve their skills.

Figure 6 *– When do you typically spend time learning new job-related skills?ж*



40%
spend time every day to improve skills

49%
learn before/after work; 20% on weekends

Costs and lack of time biggest barriers to learning

But learning and improving on job-related skills comes at a price. Cost (33%) and lack of time (28%) are the main barriers preventing IT and security professionals from getting the skills development training they want and need to do their jobs.

Figure 7 – What is your biggest barrier to developing new skills?

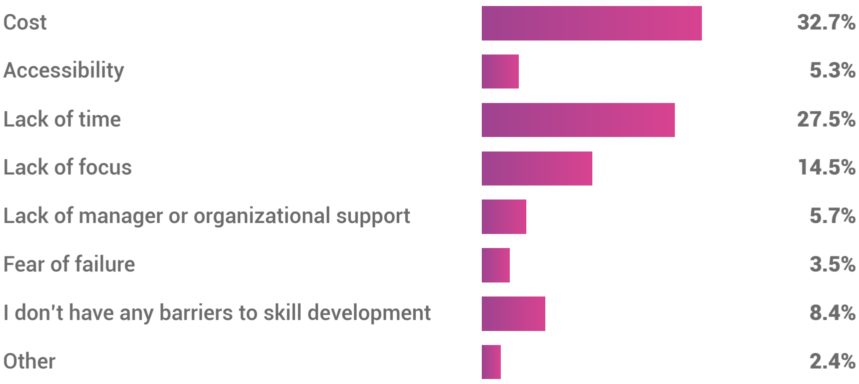
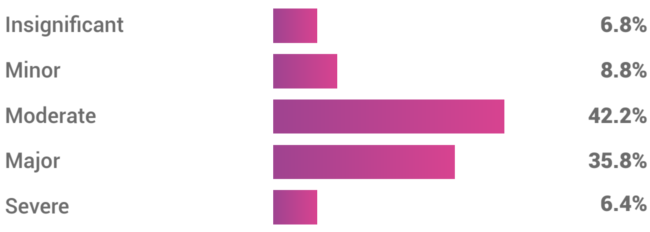


Figure 8 – How significant of an impact do these barriers have on your ability to make skill development a priority?



Even more disturbing, 40% say these barriers have a major/severe negative impact on developing their skills. So even when willing to spend extra time outside of work on learning new skills, the additional costs and time requirements are keeping many team members from doing so.

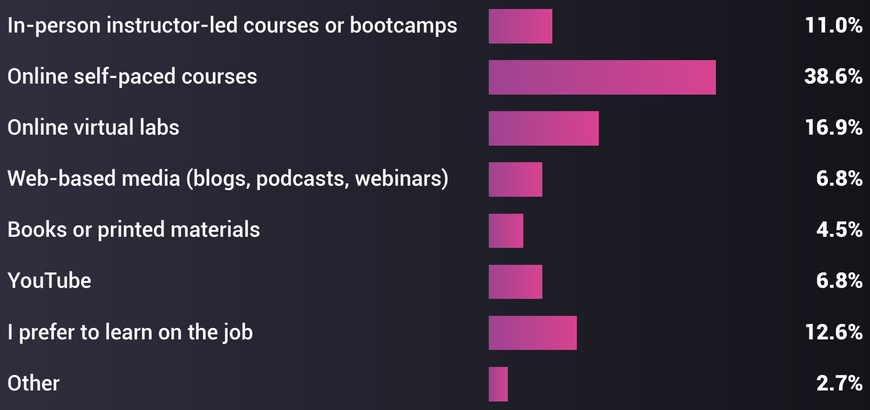
62%
prefer online learning
to improve skills

38%
favored online
self-paced courses

30%
learn to improve skills
to advance their careers

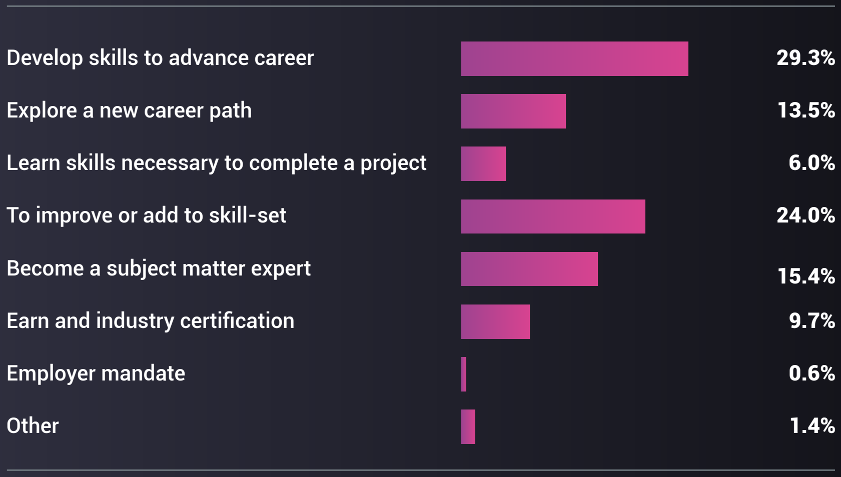
Respondents overwhelmingly preferred online learning for job-related skills (62%) including online courses, virtual labs, and web-based media. The top learning method was through online, self-paced learning (38%) along with online virtual labs (17%). This may be related to the convenience and flexibility that online learning offers individuals who are time-constrained with work tasks and duties.

Figure 9 – What is your preffered method for learning new job-related skills?



Team member's motivations appear to focus on improving their current job performance (25%) or advancing their careers (29%), rather than pursuing a new career path (13%). This would suggest that investing in training for current employees would help form a career path and seek advancement by improving their skills.

Figure 10 – What is your primary motivation for learning new job-related skills?



RECOMMENDATION

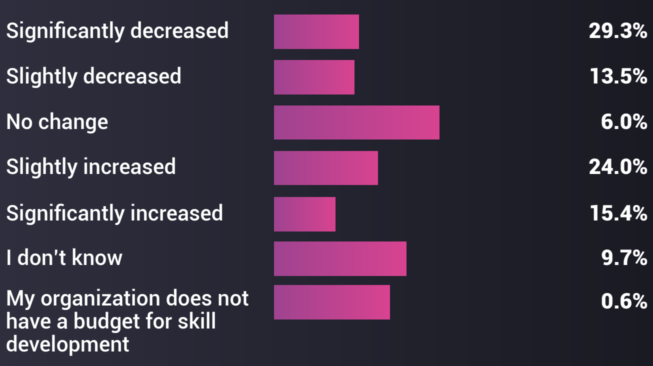
Empower team members to learn on the job.

IT and security teams are already struggling with time constraints and doing their best to improve their skills, even outside of work hours. But it's not enough. Organizations must also provide compelling training solutions so that team members don't have to pay out of their own pockets to acquire the critical skills they need to perform at the highest levels in their roles. Internal development of teams will not only drive an increase in overall efficiency, productivity, and performance, it will improve retention of key staff since they will recognize they have opportunity to grow within their current organization.

KEY **TAKEWAY #3**

Many organizations are not sufficiently investing in nor actively supporting skills development for their teams, and many respondents feel their organizations do not understand what skills are required of their team members. It is clear organizations are not effectively leveraging skills training and tracking technologies for developing their teams, while a sizable portion do not track skill development for their IT and security teams at all.

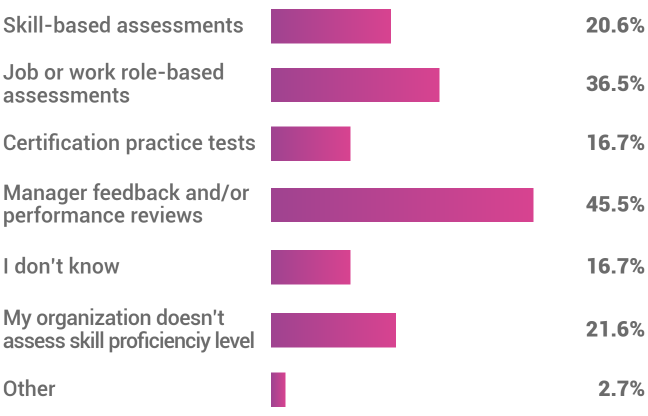
Figure 11 – How has your organization's budget for skill development changed over the past year?



IT and security team members are not getting the full support they need to improve skills since about half of organizations have either decreased their training budgets (22%) or kept them the same (25%) this past year. *Even more disturbing, 16% of respondents report their organizations do not have any training budget at all.*

Most organizations continue to rely on performance reviews by managers (46%) or job-related assessments (37%) to assess skill proficiencies, as opposed to more objective skill-based assessment (20%) or certification practice tests (17%).

Figure 12 – How does your organization currently assess skill proficiencies?



22%
had training budget cut
16% have no training budget

22%
do not assess any skill proficiency levels

40%
rarely or never assess new hire skills

Perhaps most shocking, more than one out of five (23%) organizations rarely or never track skill development for their IT and security teams. Without an objective method for tracking skill development organizations can only guess whether training/learning investments are paying off with improved skill levels.

Figure 13 – Does your organization use any of the following track and/or measure skill development?

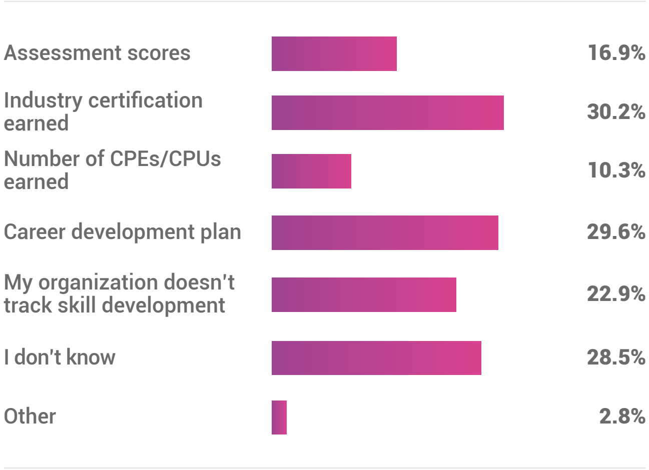
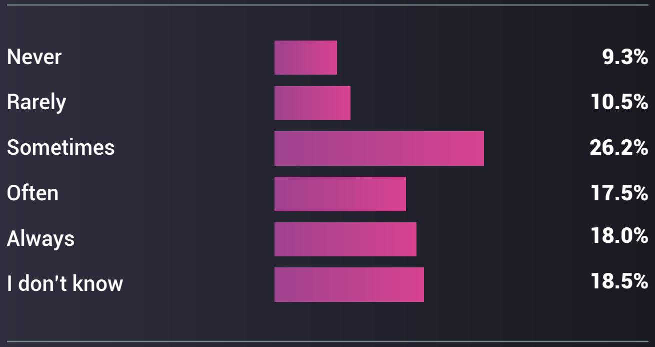


Figure 14 – Does your organization confirm that new hires possess the skill required to execute their specific roles?

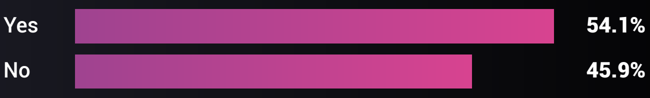


The situation for skills assessment is even worse for new hires, possibly reflecting the desire to hire talent as quickly as possible. Nearly half (46%) do not confirm new hire skills for specific roles, nor do they assess the skills of newly onboarded team members (40% rarely or never).

It's clear far too many organizations do not use skills assessment technologies for newly onboarded team members or new hires joining a team. They are likely missing the opportunities and insights that assessment and skill tracking tools offer to establish measure, baseline, and monitor skills development effectively.

At the same time, many respondents feel their organizations do not understand what skills are required of their team members (46%).

***Figure 14.1** – Do you feel your organization understands the skills required for your team to be the most effective in their roles?*



46%
say their organization doesn't know skills required to be effective in their roles

38%
say skills required to be successful in current role not communicated

30%
rarely or never communicate what skills are needed to advance their career

In addition, 38% of organizations do not clearly communicate what skills are needed by team members in order to be successful in their job/role (Figure 15) and 44% feel their organizations do not communicate the necessary skills required to advance in their careers (Figure 16).

***Figure 15** – Does your organization communicate what skills each team member needs in order to be successful in their role?*

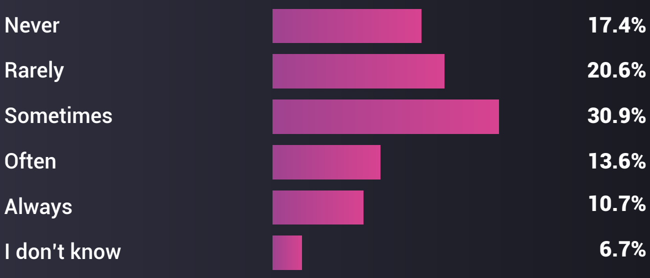
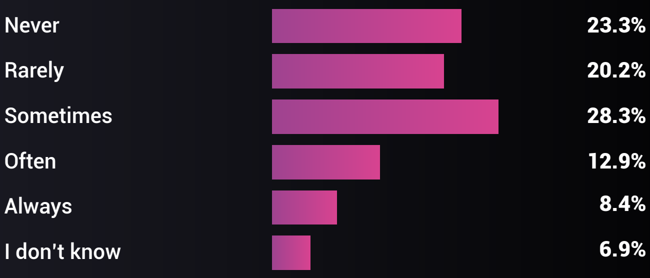


***Figure 16** – Does your organization communicate what skills each team member needs in order to advance their careers and be successfull in the future roles?*



RECOMMENDATION

Organizations need to reevaluate their training solution investments to ensure the resources they provide are effective and can measure and track team skills growth.

The data shows learners are using a variety of learning modalities, but overall, the skill gaps are not being closed/bridged to maximize team performance. The survey indicates that team members are most receptive to learning online and at their own pace. Employing intelligent and deliberate, measurable training systems can enable team members to learn needed skills, and give organizations a better understanding of their training programs ROI.

CONCLUSION

Building a skills growth culture

Acknowledging the widespread cybersecurity skills gap, organizations today must strive to cultivate a skills growth mindset that will influence the priorities and culture of the business; simply providing "training" is not sufficient.

Organizations must be intentional in assessing their workforce's skills and continually monitoring skill development. By adopting a targeted approach to understanding and solving skill gaps, organizations can establish clear development goals, better communicate to teams, and ensure mutual accountability in achieving their objectives.

This cybersecurity skills gap survey and report serve as a wake up call for organizations and IT professionals to re-examine their current training and skills development investments (or lack thereof). The dissatisfaction with current modes of training and skills development is a sign that organizations need to consider new training modes and platforms which can leverage self-paced learning along with expanded training budgets to reduce cost barriers.

Too often, cybersecurity skills development is an afterthought, leaving team members on their own to find solutions. In an environment where highly skilled professionals are scarce and expensive, organizations must nourish talent inhouse in order to improve cybersecurity effectiveness and minimize risks.

To learn more about options for improving your team member training and skills development, visit Cybrary.it

About the Survey

Conducted in June 2020, the Cybrary cybersecurity skills gap survey received more than 800 responses from IT and security professionals located around the globe with the majority from North America.

Nearly 42% of survey respondents manage teams that include IT (33%), security (25%) along with Engineering (6%), support/help desk (7%) operations (6%) and several others.

Figure 17 – *Do you manage a team?*

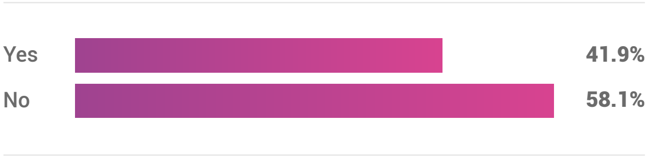
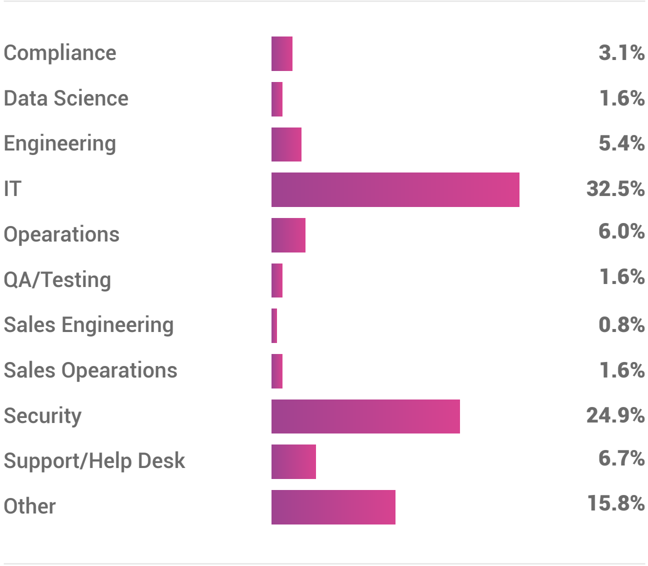


Figure 18 – *What team are you on?*



Overall, respondents represented teams with fewer than 10 members. More than 43% of respondents belonged to teams of 5 people or less, with another 29% serving on teams of 10 or fewer.

Respondents represented a wide range of experience (Figure 20), ages (Figure 21) and education levels (Figure 22).

Figure 19 – *How many people are on your team?*

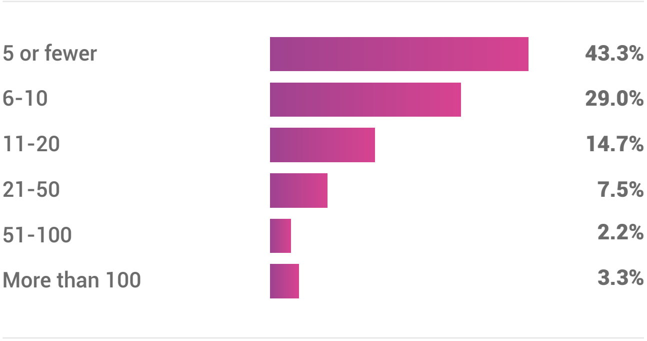


Figure 20 – *How many years of professional experience do you have in a technology role?*

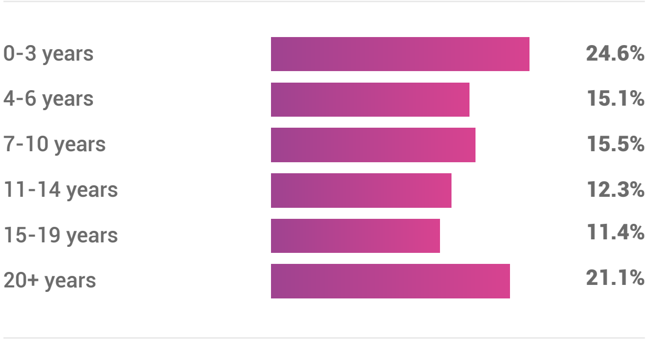


Figure 21 *– What is your age group?*

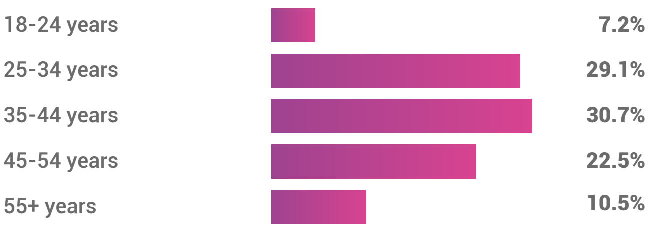
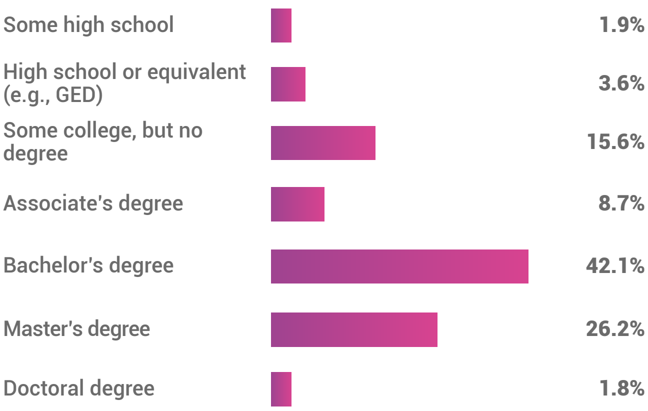


Figure 22 *– What is the highest level of education you have completed?*



References

https://www.latimes.com/business/story/2019-08-07/cybersecurity-pros-name-their-price-as-hacker-attacks-swell