U.S. Chamber of Commerce

CollegeBoard



Cybersecurity Readiness Report 2026

Insights from Decision-Makers on Entry-Level Cyber Workforce Preparedness

November 2026

Table of Contents

4
Executive Summary

7
Candidate Quality

12
Skills and Experiences

18
Cyber Literacy

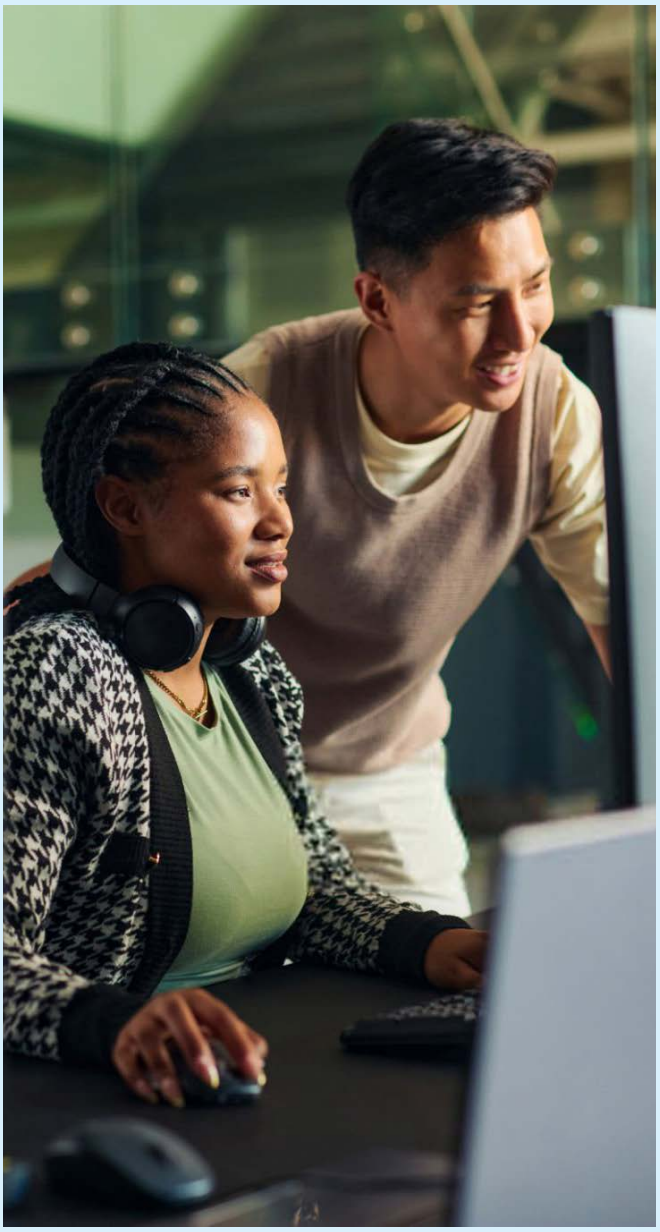
21
Conclusion

22
Methodology

Executive Summary

Cybersecurity readiness is a workforce challenge

As cyber threats become more complex, employers need a stronger pipeline of talent with technical credentials and real-world skills.



While employers generally view today's entry-level cybersecurity hires positively, they report difficulty finding candidates with the right combination of technical knowledge, real-world experience, communication skills, and AI expertise needed to succeed in a rapidly evolving environment.

85%

of cybersecurity decision-makers say most students are not prepared to enter cybersecurity roles straight out of high school.

Overall, decision-makers say they are looking for fundamental things in early career cybersecurity professionals: Industry-recognized credentials, durable skills (e.g., critical thinking, communication), and real-world experience. Another fundamental is new: Almost all decision-makers say AI cybersecurity skills are valuable.

These are findings of the Cybersecurity Readiness Report, a poll of cybersecurity decision-makers from companies of all sizes taken between August 11–25, 2026. The U.S. Chamber of Commerce and College Board conducted the survey to study the perceived preparedness of entry-level employees entering the cybersecurity sector.

As cyber threats evolve and AI continues to reshape the cybersecurity landscape, employers are looking for more than technical proficiency alone. The findings suggest that success in today's cybersecurity workforce depends on a combination of foundational cybersecurity knowledge, professional skills, AI literacy, and opportunities to apply learning in real-world settings.

The results also point to the value of multiple pathways that help students build these capabilities before entering the workforce. Employers consistently emphasized the importance of hands-on experience, problem-solving, collaboration, and communication alongside technical training.

Programs such as College Board's new AP Cybersecurity course can help expose students to cybersecurity concepts and demonstrate achievement in the field, while also serving as a foundation for further learning, credentials, internships, and work-based experiences. The course helps students build durable skills through real-world cybersecurity exercises. Collaboration is a core course skill, alongside cybersecurity skills like analyzing and mitigating risk. Students also have opportunities to collaborate with AI—learning how adversaries use it to augment attacks and how defenders use it to detect and respond to threats faster.

90%

of cybersecurity decision-makers believe AP Cybersecurity will have a positive impact on preparing high schoolers to enter cybersecurity careers.

In fact, the AP Cybersecurity credential validates the recognized professional skills outlined in the National Initiative for Cybersecurity Education (NICE) Workforce Framework. After learning of the new AP Cybersecurity course, 90% of the cybersecurity experts surveyed believe that it will have a positive impact on preparing high schoolers to enter cybersecurity.

Ultimately, strengthening the cybersecurity talent pipeline will require continued collaboration among educators, employers, workforce leaders, and policymakers. As organizations face increasingly complex digital threats, ensuring that the next generation is prepared with both technical and human skills will be critical to building a more resilient workforce and economy.



Survey Highlights



It's hard to find the right cyber candidates. Four in five (81%) respondents report they have difficulty finding the right cybersecurity candidates. They largely indicate that they are satisfied with the candidates they've hired, but the process of finding them is hard.

High school is the starting line, not the finish. More than four in five (85%) surveyed respondents agree that most students are not prepared to enter cybersecurity out of high school.

Durable skills are highly valued. Nearly all respondents believe that it is important that their employees learn communication (96%), decision making (97%), and collaboration (97%) before entering cybersecurity.

Internships are key. Decision-makers believe students gain the skills needed to be successful early in their careers at: Internships (51%), 4-year colleges (45%), trade schools/technical colleges (32%), and career and technical education courses (25%). In fact, trade school grads with internship experience are viewed about as favorably as 4-year grads with internships (88% and 92%).

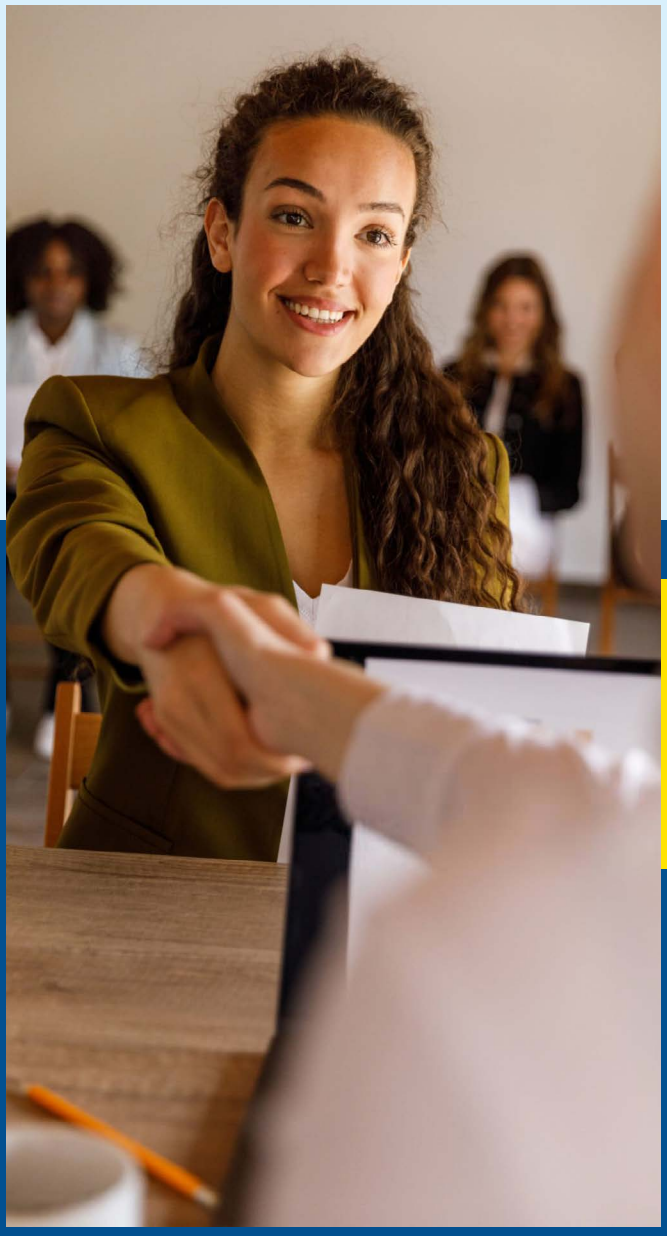
Credentials boost high school grads' chances. High school graduates with industry-recognized credentials are seen as much more prepared than those without them (61% vs. 36%).

Cyber pros with AI cybersecurity skills are highly sought after. Nearly all (97%) surveyed decision-makers view artificial intelligence skills as valuable for employees who are just starting their career in cybersecurity, including 62% who find them very valuable.

Candidate Quality

New cyber hires are good overall, but there is room for improvement

83% say recruits are good, but only 27% say they are “very” good.



Overall, those surveyed feel that early-career cyber recruits are good and prepared to begin work, but most do not find them very good or very prepared.

Among those who have recruited cybersecurity talent this year, four in five (83%) rate the quality of potential recruits that are applying for positions at their company as good or very good. About one in six decision-makers rate these recruits as fair (16%), while just 1% rate them as poor. However, while most believe that the current pool of cyber recruits is good, just 27% rate them as very good.

▶ Decision-Maker Viewpoints

In-depth interview participants point out that professionalism and technical know-how are where entry-level candidates often fall short.

“The biggest gap that we have right now is professionalism. They’re not prepared for interviews and knowing how to work in a professional environment.”

—Female, Interview Participant, Technical Recruiter, Cybersecurity

"If you ask somebody that just graduated, have you ever logged into a router? Have you ever logged into a firewall? Have you ever built a server? That's the technical side that universities are lacking– they don't start out with the basics of building systems or configuring networks."

—Male, Interview Participant, Hiring Manager



Likewise, among all surveyed decision-makers, 83% say that the entry-level employees hired in recent months are prepared to enter the workforce, though just 30% say they are very prepared.

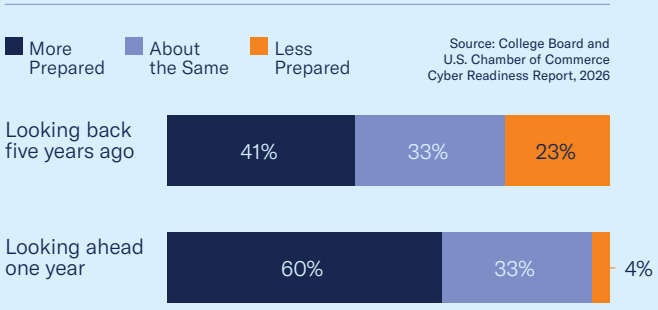
By generation, Gen Z/Millennial decision-makers are more likely than Gen Xers[1] to rate the quality of potential recruits as good (88% vs. 76%) and view their recent entry-level hires as prepared (89% vs 80%). Additionally, those companies with fewer than 20 employees are less likely to view recent entry-level hires as prepared compared to those with 20-499 and 500 or more employees (76% vs. 91% each).

When asked to compare recent hires to candidates that were hired five years ago, two in five (41%) say the past candidates they hired were more prepared than their recent hires. About one in four say the past candidates were less prepared (23%), while one in three say they were about the same level of preparedness (33%).[2]

Looking ahead, three in five expect the entry-level employees they hire a year from now to be more prepared than the candidates they recently hired. One in three expect future candidates to be as prepared as recently hired candidates, while few expect them to be less prepared (4%).

Views of employee preparedness when...

% Very/Somewhat Easy



Three percent of respondents answered, "does not apply."

1 The sample size for Baby Boomers and older is too low to report on (N < 100). Any references to age will focus on Gen Z/Millennial and Gen X respondents.

2 Three percent of respondents answered, "does not apply."

The decision-makers in this cyber workforce readiness study are more likely to believe that candidates a year from now will be more prepared than the decision-makers surveyed in the 2025 New Hire Readiness Report, a general workforce readiness study with a similar methodology (60% vs. 26%).[3]

Few say it's easy to find candidates with experience, skills they need

While general sentiments toward entry-level employees are positive, there are signs of struggle under the surface, particularly when it comes to finding candidates with the right combination of skills and experience.

Fewer than two in five say it is easy to find candidates with the skills (37%) or experience they need (35%). For each of these, more feel it is somewhat easy rather than very easy to find candidates with these criteria.

When it comes to keeping the workers they already have, a slim majority (53%) say that it is easy to retain their employees. Just under half say the same of finding enough candidates to fill open positions (46%), candidates in their area (45%), and candidates open to working in an office/onsite (45%).

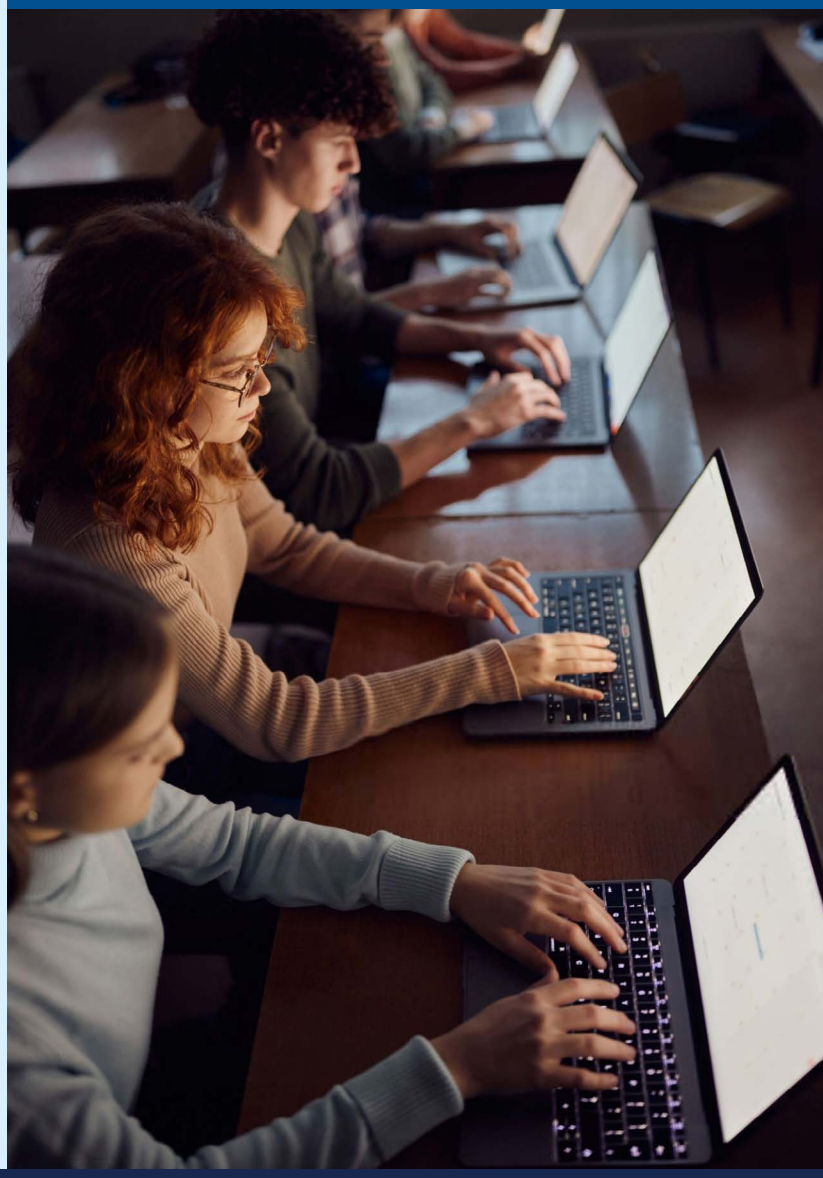
Across all attributes, Gen Z/Millennial decision-makers are significantly more likely than their Gen X counterparts to say that finding candidates is easy. By company size, those who work at businesses with 500+ employees are more likely than those at companies with fewer than 20 employees to find it easy to retain their employees (61% vs. 47%) and find enough candidates to fill open positions (53% vs. 41%).

▶ Decision-Maker Viewpoints

When asked whether they expect candidates a year from now to be less or better prepared, in-depth interview participants had a variety of different views.

"We have better training programs and better AI models than in the past."

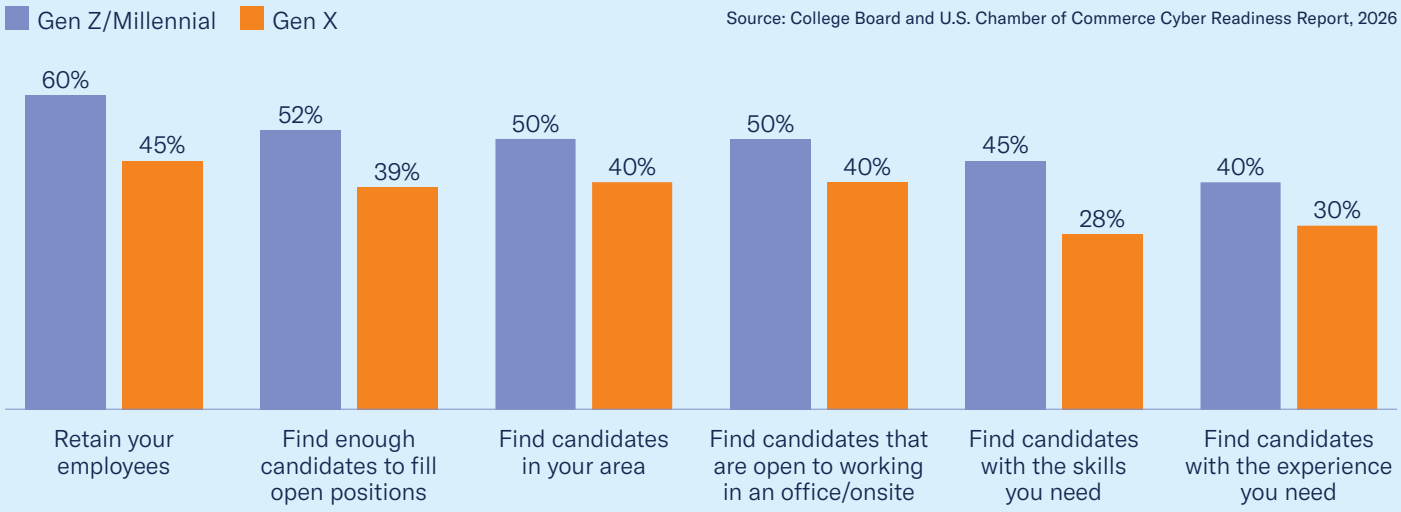
—Male, Age 37, Chief Executive Officer, 10 years of hiring experience, believes candidates will be more prepared



3 *New Hire Readiness Report* (U.S. Chamber of Commerce and College Board, 2025), https://www.uschamber.com/workforce/new-hire-readiness-report-2025

How easy or hard is it to do the following?

% Very/Somewhat Easy



"Improved training programs, hands-on learning, and greater familiarity with AI tools should make new hires better prepared for the role."

—Female, Age 43, Chief Executive Officer, 5 years of hiring experience, believes candidates will be more prepared

"Regardless of the level of technical expertise learned in academia, entry-level candidates typically lack real-world experiences that enhance problem-solving skills and critical thinking 'outside-the-box' to apply their technical expertise for practical solutions."

—Male, Age 65, President, 30 years of hiring experience, believes candidates will be about the same level of preparedness



More broadly, four in five (81%) surveyed respondents report they have difficulty finding the right candidates.

When asked about potential consequences due to difficulty finding candidates, more than a third said they have spent more time/money training for current staff (37%) or asked staff to work longer hours (36%).

Other actions taken include outsourcing work (30%), hiring temporary staff (26%), having difficulty scheduling work due to lack of staff (20%), and passing on new work due to lack of staff (15%).

Overall, cyber decision-makers largely indicate that they are satisfied with the candidates they've hired, but the process of finding these candidates is difficult.

"AI has rapidly changed the cybersecurity landscape, and entry-level employees will have more to learn just to make a minimal impact. I expect that they will either know the fundamentals and not the new techniques, or the other way around, but not both."

—Male, Age 45, Chief Information Security Officer, 15 years of hiring experience, believes candidates will be less prepared



Skills and Experiences

Durable skills and experience highly valued for entry-level talent

Internships viewed as most important path to right skills.

▶ Decision-Maker Viewpoints

Interview participants often expressed how durable skills and willingness to learn are just as important as technical know-how.

"The most important soft skills that are a determinant of success for people we bring into the programs in early careers are critical thinking and problem-solving."

—Simone Bachmann, Managing Director within Cybersecurity & Technology Controls, JPMorganChase*

*This comment reflects the individual speaker's perspective and does not imply endorsement by JPMorganChase.

"As a leader, I'm looking for a baseline technical competency... layered then with ability to explain a technical solution, the ability to communicate, the confidence to share your opinion and influence others that may not have the same level of expertise as you in your particular domain. Soft skills are almost equally as important as those technical skills."

—Female, Interview Participant, Head of Governance, Risk and Compliance, Cybersecurity

Employers are looking for early-career cybersecurity professionals with a mix of cybersecurity experience and durable skills mastery. Although most do not feel that those straight out of high school are ready for the workforce, cybersecurity recruiters feel there are many pathways to the requisite experience and cite internships as a top way to get it.



First, the employers surveyed expect entry-level employees to have a baseline grasp of critically important durable skills. Nearly all of these respondents believe that it is important that their employees learn communication (96%), decision making (97%) and collaboration (97%) before entering cybersecurity, including a majority across each that say it is very important.

Second, employers are looking for work experience. The most cited places these decision-makers believe students gain the skills needed to be successful early in their careers are internships (51%) and 4-year colleges (45%), followed by trade schools/ technical colleges (32%) and career and technical education courses (25%).

Notably, survey respondents across manufacturing, retail, and professional services report similar shares (25%-28%) who believe skills are primarily learned in career and technical education high school courses. By contrast, those in professional services (49%) and retail (48%) are more likely than those in manufacturing (38%) to say skills are learned in 4-year colleges.

In-depth interview participants offered additional context about why internships topped the list of experiences necessary for success. Being in an office environment and learning how to communicate and interact with others is a skill that was seen as critical, but sometimes lacking, for entry-level employees. One manager noted the importance of a “real-life practicum” and learning from business practitioners, not just professors or teachers in a classroom.

However, cybersecurity skills are also vital. The poll finds that nearly three in five agree hat they don’t consider candidates for open positions that don’t have all the skills they are looking for (59%) and that their company spends too much time on training and upskilling new employees (58%). Notably, Gen Z/Millennial decision-makers are more likely than Gen X to say that their company spends too much time on training or upskilling new employees.



▶ Decision-Maker Viewpoints

In-depth interview participants who said that high school courses play a minor or no role in their company's hiring process were asked what would increase their importance.

"If they held credentials or could display projects they worked on."

—Male, Age 31, Chief Technology Officer, 5 years of hiring experience

"If these high school courses helped students develop portfolios of skills obtained and projects completed, they would be a much better demonstration of the students' abilities and play a bigger role in the hiring process."

—Male, Age 36, Department Head, 4 years of hiring experience

"More practical IT skills, cybersecurity basics, and hands-on projects would increase their value."

—Female, Age 41, Chief Executive Officer, 5 years of hiring experience

"I look for actual knowledge of candidates. The tests themselves do not matter to me. It is about the actual knowledge they have."

—Female, Age 41, Department Head, 15 years of hiring experience

Today's high school grads less prepared

More than four in five surveyed respondents agree that most students are not prepared to enter cybersecurity roles straight out of high school (85%), and 65% agree that current high school graduates are less prepared to enter the workforce when compared to previous cohorts. A majority across all demographic groups share these sentiments.

When asked about what should be taught in high schools, nearly all survey respondents agree that there should be more courses teaching communication, collaboration, and critical thinking (94%)—those highly-desired durable skills that employers find so important.



AI skills and industry credentials are both highly sought after

College/trade school grads with credentials, experience seen as most prepared.

Overall, decision-makers view candidates with an industry-recognized credential as more prepared than those without one. However, credentials alone only go so far. Decision-makers view trade school graduates with credentials as equally prepared as those with internship experience.

More education, more experience, and more industry-recognized credentials tend to make cybersecurity candidates more attractive to decision-makers. When it comes to high school graduates, those with industry-recognized credentials are seen as much more prepared than those without (61% vs. 36%). Those viewed as most prepared (92%) were 4-year college grads with internship experience, followed closely by 4-year college grads with a credential (91%), trade school grads with internship experience and trade school grads with a credential (both 88%). Among those without a credential, 4-year college grads (66%) were viewed as the most prepared and even more prepared than high school grads with an industry-recognized credential (61%).

Three in four respondents also say that young adults with internship experience are prepared to enter the cybersecurity sector (74%). A majority across all demographics hold this sentiment. In the same vein, 91% of surveyed decision-makers say they would be more likely to hire an entry-level employee if they have credentials in a relevant field, including 46% who say they would be much more likely. Credentials are highly valued, but similar weight is placed on durable skills such as critical thinking/problem-solving (89%) and communication (88%), as well as internship experience (89%) and leadership experience (83%).

▶ Decision-Maker Viewpoints

Many in-depth interview participants highlighted the value of industry-recognized credentials and what they say about a candidate.

"Most of the time, somebody with a certification is going to show that initiative because they wanted to do it. And it is going to hold a little bit higher value for me... Even if someone's here for three, five years, we encourage them to continue to learn and to pursue those ancillary certifications."

—Lou Modano, Executive Vice President, Chief Information Security Officer, and Global Head of Corporate Information Technology, Nasdaq

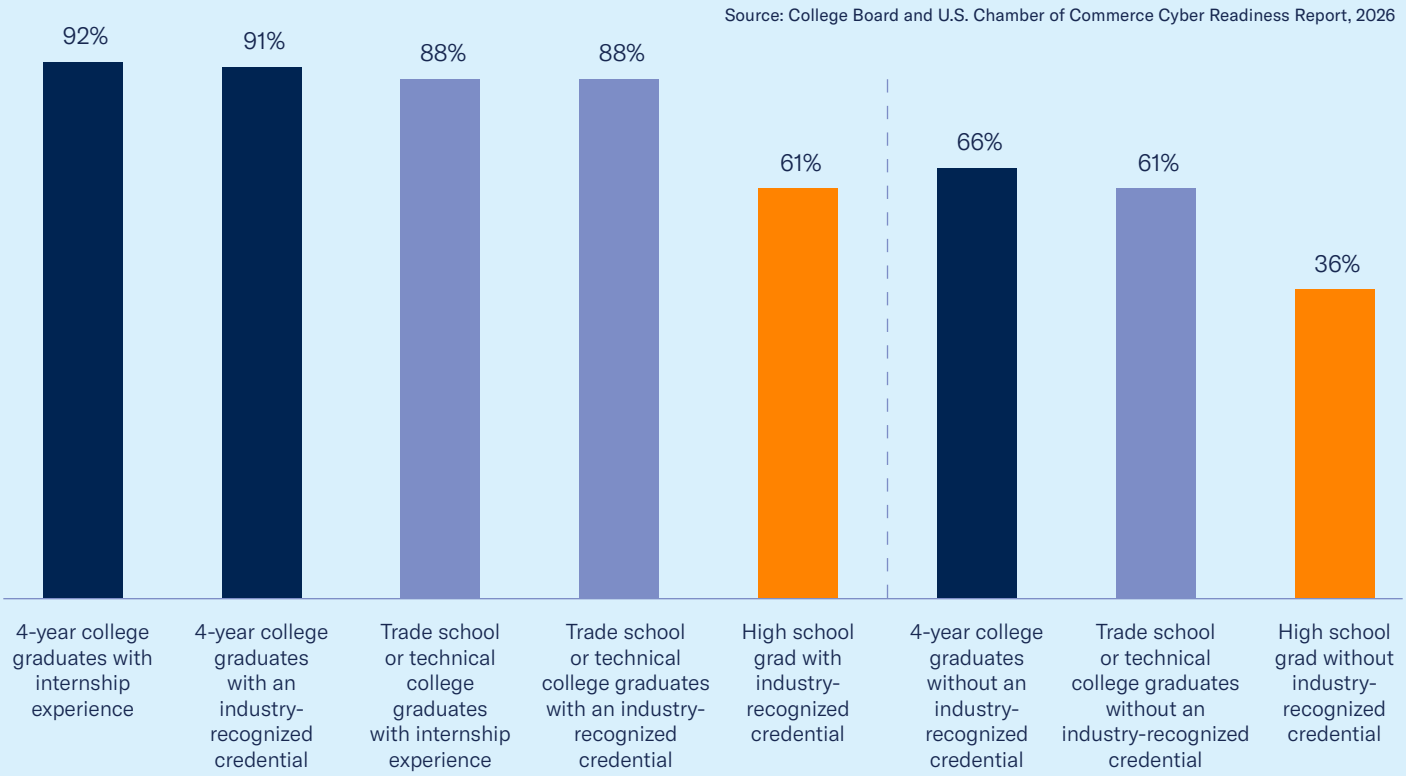
"Credentials can demonstrate a strong foundation and understanding of key concepts, but they're only one part of the equation. What matters most is the ability to apply that knowledge, solve real-world problems and continue building skills as the environment evolves."

—Deneen DeFiore, Vice President & Chief Information Security Officer, United Airlines

"If you don't have that passion to continuously learn the industry, then it can tend to leave you behind. So that really sets you apart when you have those certifications, even though it's not a hard requirement."

—Female, Interview Participant, Senior Manager Cybersecurity Recruitment

In general, how prepared, if at all, do you feel each of the following are to enter the cybersecurity sector?



▶ Decision-Maker Viewpoints

When asked about their own role in developing entry-level talent, in-depth interview participants consistently described hiring for potential and building technical skills on the job.

"We have to mentor properly and provide that on-the-job training. People typically think about that in a technical capacity, but on-the-job training is also learning how to interface with people."

—Michael Priest, SVP and Chief Information Security Officer, financial services industry

"As I transform my workforce, it's great to give traditional AI training, online courses, go to school, get a certificate. But it's the application of it. So, what we started doing is, every week I have a big general manager call. One person shows how they're using AI. It can be at home, it can be at work, and then we create a video library."

—Senior Vice President and Chief Information Security Officer

Decision-makers very highly value AI skills

In addition to credentials, experience, and durable skills—there is a new, standout fundamental skill that decision-makers in cybersecurity are almost all looking for: AI.

Along these lines, nearly all (97%) surveyed decision-makers view artificial intelligence skills as valuable for employees who are just starting their career in cybersecurity, including 62% who find them very valuable. More than four in five also indicate that they would be more likely to hire an entry-level employee who has training or certification on how to use artificial intelligence (84%).

When asked what the biggest challenges are facing the cybersecurity sector, nearly half of respondents surveyed selected artificial intelligence (47%) or rapid technology changes (45%). Three in ten say the biggest challenge is a lack of qualified professionals, while about one in five say ransomware attacks (19%) and employee retention (17%).

▶ Decision-Maker Viewpoints

When asked why they believe artificial intelligence skills are valuable for employees who are just starting their cybersecurity careers, in-depth interview participants said:

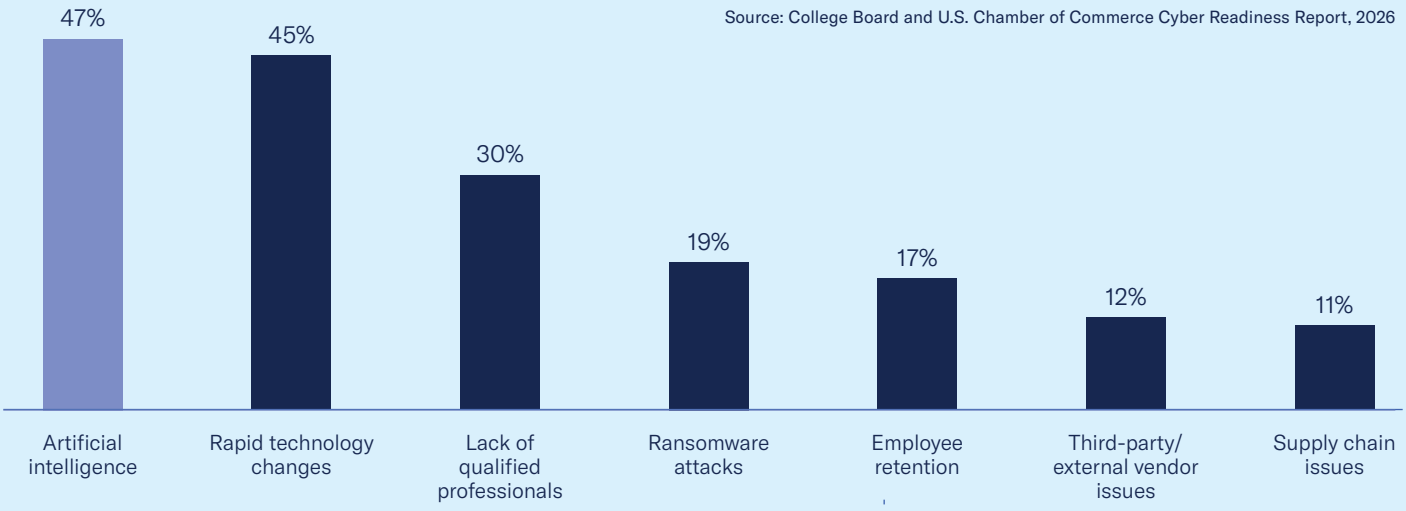
"AI helps entry-level analysts detect threats faster, automate repetitive tasks, and stay ahead of evolving cyberattacks."

—Male, Age 39, Chief Information Security Officer, 15 years of hiring experience

"Even if they don't have a deep understanding of the underpinnings of AI, they do need to have a basic knowledge of its capabilities, applications, strengths, weaknesses, and limitations as AI is becoming a part of EVERYTHING."

—Male, Age 58, Chief Operating Officer, 16 years of hiring experience

Which of the following are the biggest challenges facing the cybersecurity sector?



Source: College Board and U.S. Chamber of Commerce Cyber Readiness Report, 2026

Cyber Literacy

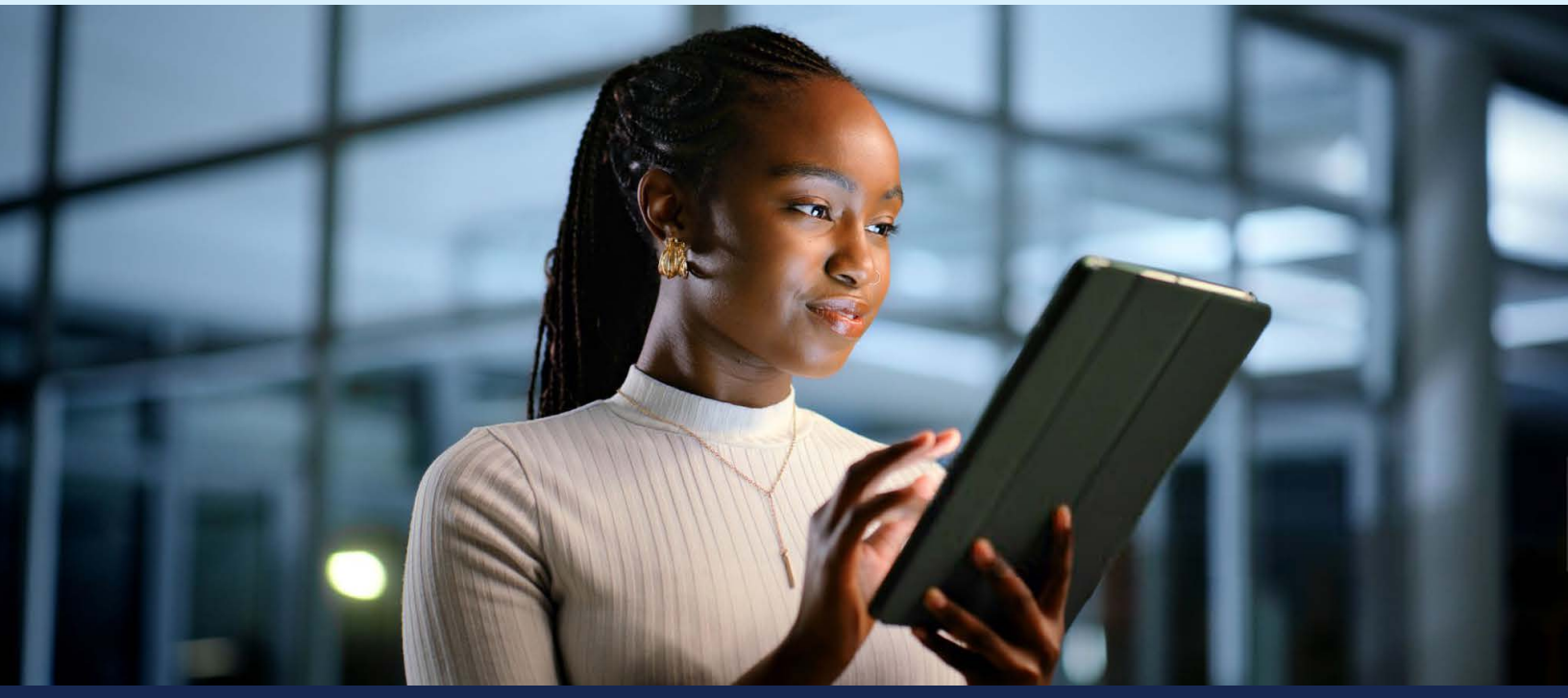
Majority believe AP Cybersecurity course will have positive impact

Durable skills remain essential alongside technical training.

A majority of the cybersecurity decision-makers surveyed said that the AP Cybersecurity course (that will be taught in high schools starting in the 2026-2027 school year) will have a positive impact on preparing high schoolers to enter cybersecurity field and would give them a leg up on similar candidates who had not taken the course. However, it's important not to skimp on learning those ever-valuable durable skills, even at this early stage, because decision-makers will be looking for evidence that candidates have them.

Overall, two in three (65%) report seeing, hearing, or reading anything about the AP Cybersecurity course. However, just 18% say they have heard a great deal.

The AP Cybersecurity credential validates the recognized professional skills outlined in the National Initiative for Cybersecurity Education (NICE) Workforce Framework. After learning about the course and its goals, 90% believe that it will have a positive impact on prepping high school students for a career in cybersecurity. Additionally, for entry-level roles outside of cybersecurity, 81% said they would be more likely to hire a candidate who had taken the AP Cybersecurity course over a similar candidate who had not.



▶ Decision-Maker Viewpoints

In-depth interview participants find value in the AP Cybersecurity course simply because of the exposure it gives to different topics.

"Exposure to the scenarios and the techniques in a learning environment...is super helpful because you can translate that into the context of whatever role you're in."

—Female, Interview Participant, Chief Information Security Officer

"Lab work or something of this sort where they could touch the tools, that would be great, because then you would know that they come in with that baseline and that they have some hands-on experience."

—Female, Interview Participant, Senior Manager Cybersecurity Recruitment

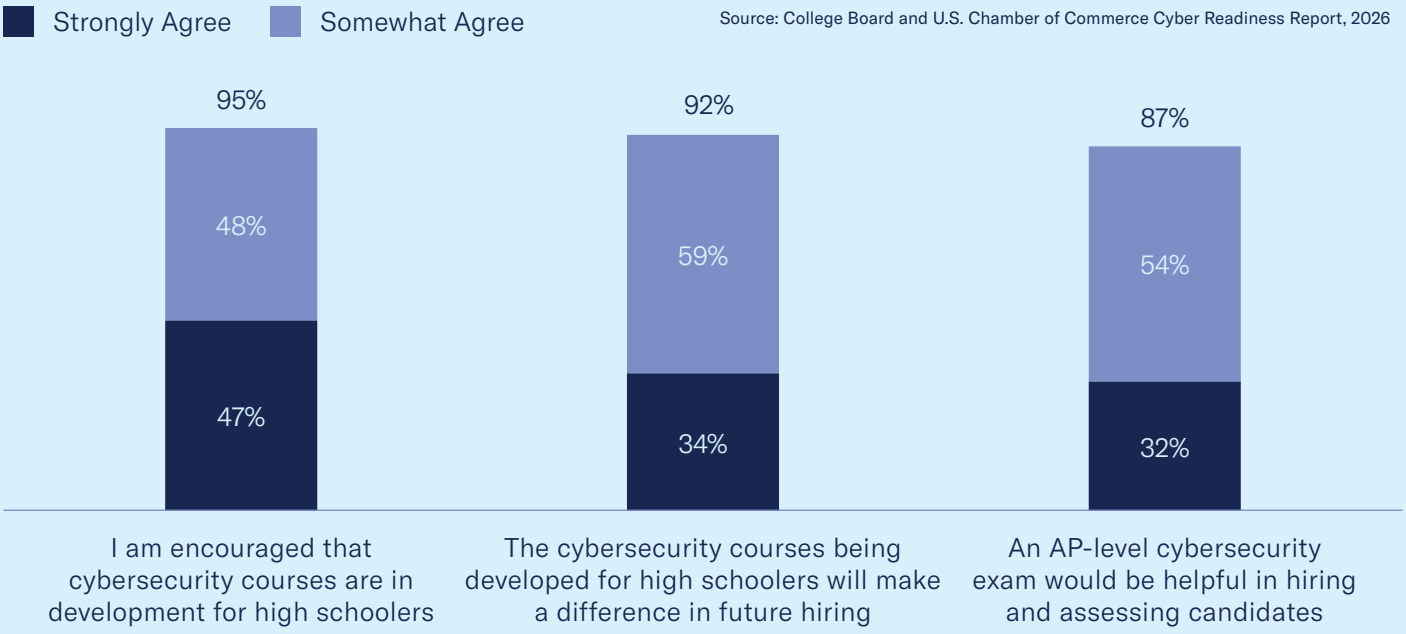




"Covering general risk and mitigations and how to deploy countermeasures prior to those vulnerabilities being identified would be valuable. If it's just a, hey, there's a website vulnerability, okay, patch it, then that's completely different."

—Male, Interview Participant, Head of Security Operations

To what extent do you agree or disagree with the following statements?



Among surveyed decision-makers, overwhelming majorities agree that they are encouraged by the development of cybersecurity courses for high schoolers (95%) and that these cybersecurity courses will make a difference in future hiring (92%). Additionally, 93% believe that there should be more cybersecurity courses taught in high school. Nearly nine in ten also agree that an AP-level cybersecurity exam would be helpful in hiring and assessing candidates.

At the same time, decision-makers are clear that real-world experiences matter, too. About nine in ten agree that work experience is more valuable than formal education (89%). This helps underscore that these durable skills are as important and desirable as the more technical skills.

When survey respondents were asked how much of a role high school courses play in their company's hiring process, four in five say that they play at least some role, including nearly three in ten who say they play a major role (28%). Gen Z/Millennial decision-makers are more likely than their Gen X counterparts to say that high school courses play a role in the hiring process (84% vs. 75%).

Conclusion

Building the cyber workforce of tomorrow

Preparing the next generation requires earlier access to cyber education, durable skills, and hands-on experience.

In summary, this survey finds that there are some key elements that make early-career cybersecurity candidates compelling to decision-makers: Industry-recognized credentials, experience (including internships), durable skills (like communication and collaboration), and AI skills. Candidates who combine all four attributes are likely to stand out from the competition. Of course, having a degree is also valued with 4-year college degrees most valued, trade school degrees a close second, followed by high school diplomas.

Overall, decision-makers see good candidates come their way, but fewer that are a good match. Most (83%) decision-makers say the quality of potential recruits that are applying for cybersecurity positions at their company are very good or good. However, most (81%) respondents report having difficulty finding the right cybersecurity candidates.

While most (85%) decision-makers agree that most students are not prepared to enter cybersecurity straight out of high school, they view high school graduates with industry-recognized credentials as much more prepared than those without them (61% vs. 36%). And after learning of the course, 90% of cybersecurity experts surveyed believe that the AP Cybersecurity course will have a positive impact on preparing high schoolers to enter the cybersecurity field.

The findings point to a clear opportunity: creating more pathways that help students with both cybersecurity knowledge and real-world experience. As organizations face increasingly complex digital threats, the workforce of tomorrow will need both the technical skills to understand cybersecurity challenges and the professional skills to solve them.

Policymakers can help close this gap. States and school districts should leverage existing federal funding streams, including Title IV-A, to reduce or eliminate AP Cybersecurity exam fees for students, while Congress should expand should increase career and technical education (CTE) funding and confirm that those dollars can cover AP Cybersecurity exam fees, course costs, and work-based learning. States should open flexible licensure pathways so cybersecurity practitioners can teach these courses, and federal agencies and employers should partner with high schools to turn this course into a pipeline for military and national security careers. The threats are not waiting.

Methodology

These are the findings of an Ipsos poll conducted between August 11-25, 2026. For this survey, a sample of 450 cybersecurity decision-makers from small, mid-sized, and large companies (age 18 and older) from the continental U.S., Alaska, and Hawaii, was interviewed online in English.

To qualify for the survey, respondents had to be employed, director level or above and have input on the hiring process for entry-level employees in cybersecurity. No post-hoc weights were applied to the data and the findings reflect the opinion of these respondents.





U.S. Chamber of Commerce

CollegeBoard

U.S. Chamber of Commerce
1615 H Street, NW
Washington, DC 20062
uschamber.com