BUILD RESILIENT CYBERSECURITY TEAMS

Stop Chasing 'All Stars' for Short-Term Gain and Develop Your Team for Years of Success

INTRODUCTION

Building a strong cybersecurity team is a big challenge for any organization. Talent is scarce. The current workforce gap is estimated at 3.1 million worldwide.[i] But many organizations continue to repeat the mistakes of focusing their time and energy on hunting down and competing for a select few cybersecurity "All Stars" instead of strategically developing their teams at all skill levels to create a sustainable, long-term investment in their security personnel.

It's an often-discussed frustration among current and aspiring cybersecurity professionals: too many organizations have unrealistic expectations for the positions they are trying to fill.[ii] They either overload job descriptions with too many responsibilities or set unrealistic experience requirements for entry-level and even mid-career jobs. Often, it goes beyond that to include a lack of support once cybersecurity professionals join an organization without clear plans for training, mentorship or advancement.[iii] That leads to talent drain, dissatisfied team members, continuous hiring cycles, and, ultimately, weaker security postures and degraded incident response capabilities.

To provide organizations advice on how to develop more effective recruitment and professional development strategies for their teams, the (ISC)^2 Cybersecurity Career Pursuers Study surveyed 2,034 cybersecurity professionals (professionals) and cybersecurity jobseekers (pursuers) throughout the U.S. and Canada (1,024 cybersecurity professionals and 1,010 jobseekers pursuing their first cybersecurity role).

Findings reveal the experiences, education, skills and attributes cybersecurity professionals say made them successful. We also gained insights into the opportunities and challenges today's pursuers anticipate upon entering the workforce, as well as which skills and technical security concepts interest them, and the attributes they feel are important for success in the field. This

assessment creates a roadmap for organizations to follow when recruiting new hires, especially when it comes to the entry-level and junior team members necessary to build teams from the ground up for long-term success and viability.

Data suggests many entrants into the field – especially those not working in an IT position – are unsure what to expect from their first cybersecurity job and may be wary of technical obstacles. Organizations must strategically plan when assigning initial responsibilities and offering on-the-job training to invest in pursuers' development. While that may sound like a burden for organizations, input from professionals strongly implies that having a mentor, access to training, education and professional achievements, such as earning certifications, and being exposed to the right mix of tasks in their first few years is critical to their growth, confidence and longevity in the profession.

The survey results also provide guidance on how recruiters and hiring managers may need to adjust the tactics they use to proactively identify internal and external candidates. Findings point to strong agreement about what makes a cybersecurity professional successful, at what point in their careers professionals seem likely to pursue a cybersecurity path, what attracts people to the job and what qualities rank as strong indicators of future successful team members.

WHO ARE THE PROFESSIONALS?

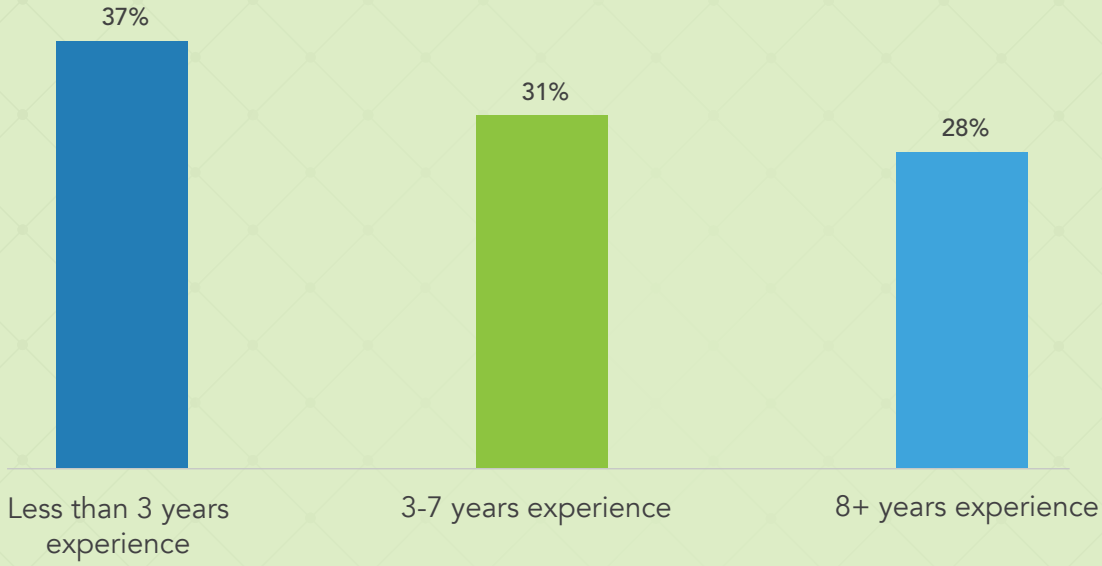
To help capture broad perspectives, opinions and views about what makes a cybersecurity professional successful, our methodology ensured a strong mix of responses across tenure in the field. Of the 1,024 cybersecurity professionals who participated in our study, 42% have less than 3 years of experience; 29% have 3-7 years of experience; and 29% have more than 8 years of experience.

About half (49%) of participating professionals are aged 35 to 44, while 26% of professionals are under the age of 35. Another 10% are aged 45 to 49, and those aged 50 or older make up the remainder of participants.

The gender breakdown among study participants was 67% men and 33% women.*

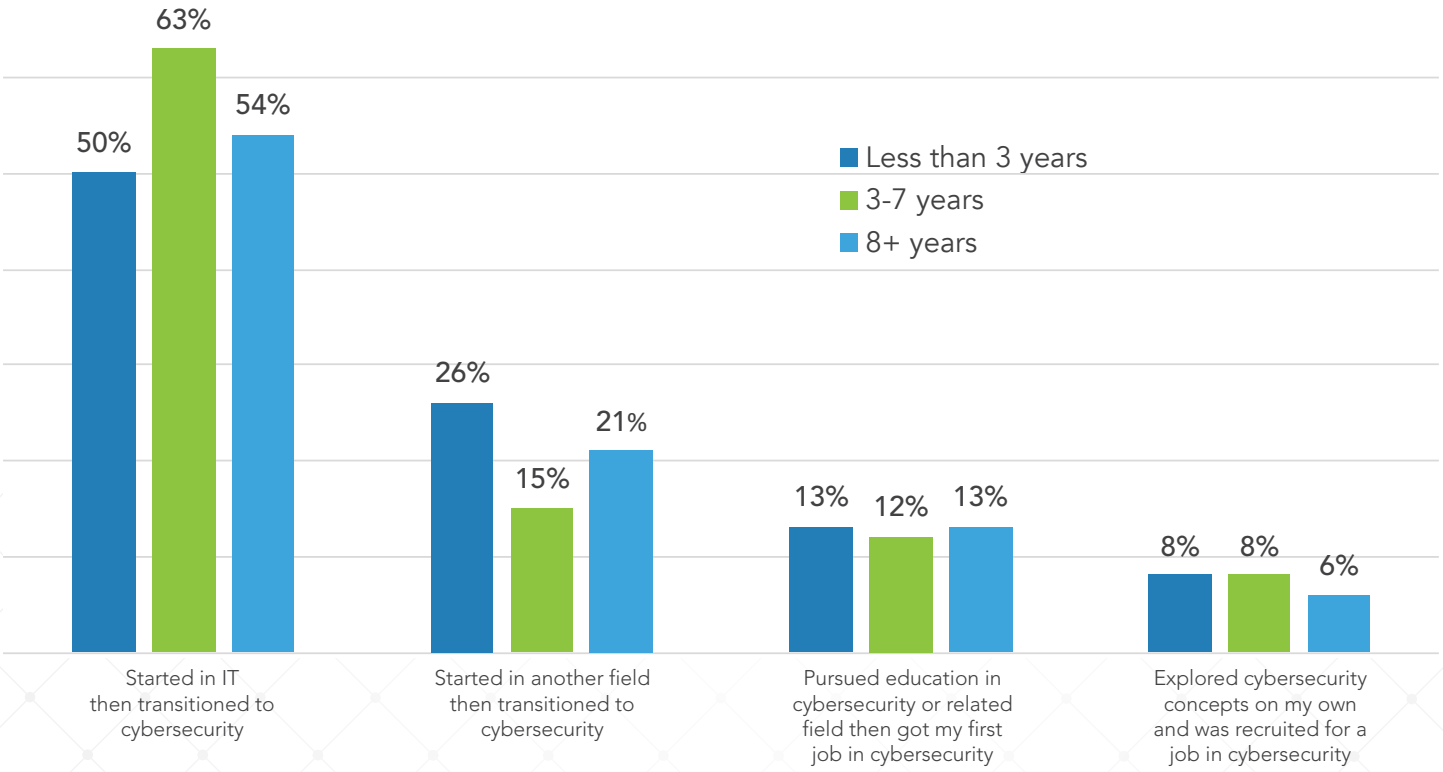
The study reaffirms previous research that prior IT roles provide the most common pathway to cybersecurity jobs. 55% of cybersecurity professionals have transitioned from IT. The number is higher for men (59%) than women (46%). Among those who didn't get into cybersecurity via IT, 21% started their careers in another field. Only 13% got into cybersecurity after receiving a cybersecurity education, and 8% explored cybersecurity on their own before being recruited to the field.

Professionals: Younger Women Entering Cybersecurity at Higher Rates



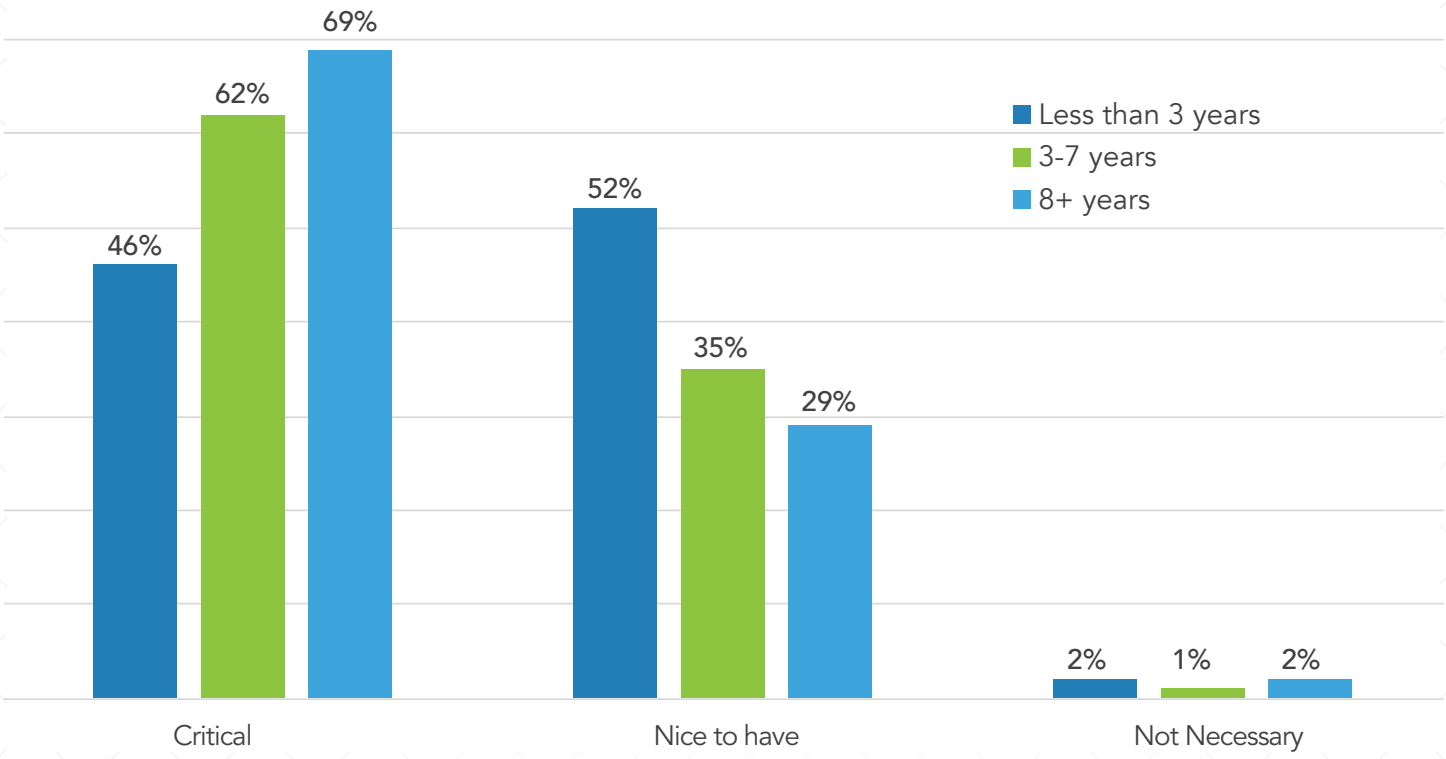
The percentage of women working in cybersecurity roles decreases as tenure increases. This may indicate that more women are joining the profession, but it may also suggest that women may not find enough advancement opportunities as they progress in the field.

Professionals: Pathway to Cybersecurity



There appears to be a shift in entry pathways for those newer to the profession. 26% of professionals with less than 3 years of experience started in a field other than IT. Meanwhile, only about 1 in 5 professionals with 8 or more years of experience started in a field other than IT.

Professionals: How Important is IT Experience?

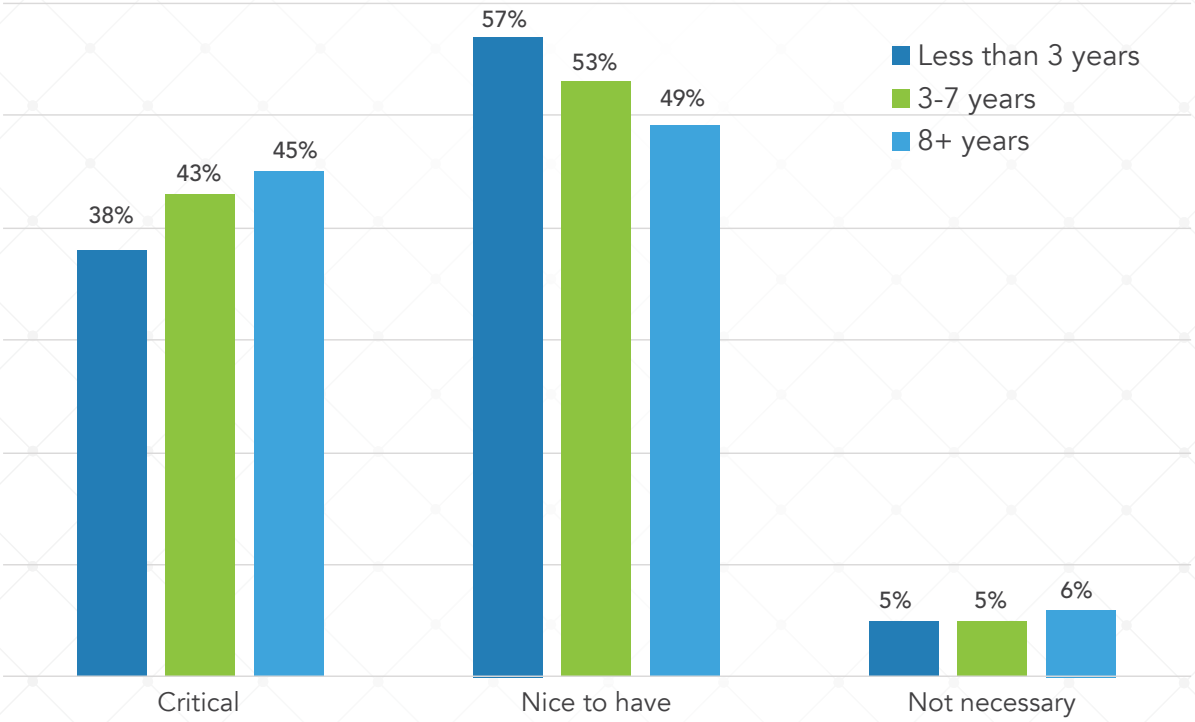


Opinions differ by years of experience when asked how important IT experience is for a successful cybersecurity career. Those relatively new to the field say IT experience is less critical than their more senior colleagues, but more than half still say it's a "Nice to have."

Cybersecurity professionals tend to be highly educated. The largest group among participants (73%) comprises people with a bachelor's (40%) or master's degree (33%). Another 8% have a doctorate. Slightly more than half (51%) pursued an education in computer and information sciences, while another 13% studied engineering. Those newer to the field (less than 3 years of experience) have higher rates of associates (11%) or technical (10%) degrees than those with longer tenure in the industry.

The majority of professionals holding post-graduate degrees tend to hold management positions (39%) or work in security administration (21%). Meanwhile, professionals with bachelor's degrees are found more evenly distributed across management (26%), security administration (23%) and security operations (21%).

Professionals: How Important is a Security Education?



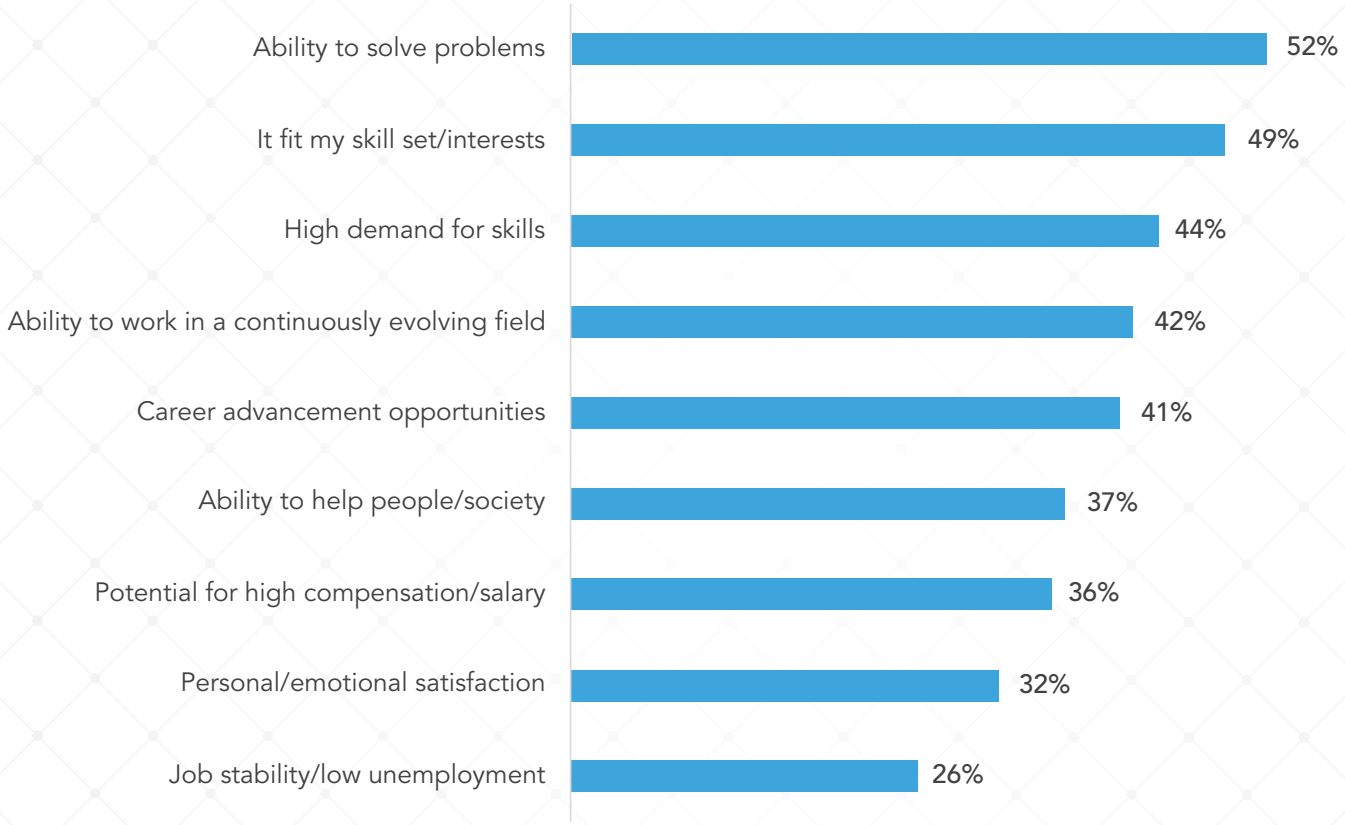
When asked how important an education background in security or a related field was for success in cybersecurity, only 5-6% of respondents say it's "Not necessary," while more than half say it's a "Nice to have" with some variations across years of experience

Military veterans and law enforcement are often cited as prime areas for recruiting cybersecurity professionals, and this group combined represents nearly a third of professionals in our study. 16% of participating cybersecurity professionals have military affiliation (6% are currently in the military; 10% are retired military), and 15% have law enforcement experience (11% are currently working in law enforcement; 4% are retired law enforcement). Military and law enforcement affiliations were much higher for those newer to the profession (less than 3 years of experience) with 12% currently in the military, another 12% retired military, and 18% are currently employed in law enforcement.

When asked what motivated them to pursue a cybersecurity career, professionals listed *ability to solve problems* (52%) as the top reason. That was followed by *it fit my skill set/interests* (49%), *high demand for skills* (44%), *working in a continuously evolving field* (42%) and *career advancement opportunities* (41%).

Other motivations, such as potential for high compensation (36%) and job stability (26%), ranked substantially lower. The compensation finding reflects past research by (ISC)² showing that earning a high salary isn't a primary goal.[iv] It's possible cybersecurity professionals don't place too high a priority on compensation because high salaries are expected in the industry.[v] This could also explain why job stability ranks low – since opportunities consistently outnumber skilled candidates, stability is not a concern.[vi]

Professionals: What Motivates Cybersecurity Pros?



Professionals cited a range of motivating factors for choosing a cybersecurity career. Not only does this underscore how broadly rewarding the field is for many people, but it also enables hiring managers to look for similar motivations among new team members to identify those who will find the work fulfilling for the long-term.

KEYS TO SUCCESS: SKILL AND MOTIVATION

We asked professionals to rate a broad range of attributes, including technical and soft skills to produce their weighted *Top Lists* of advice for pursuers.

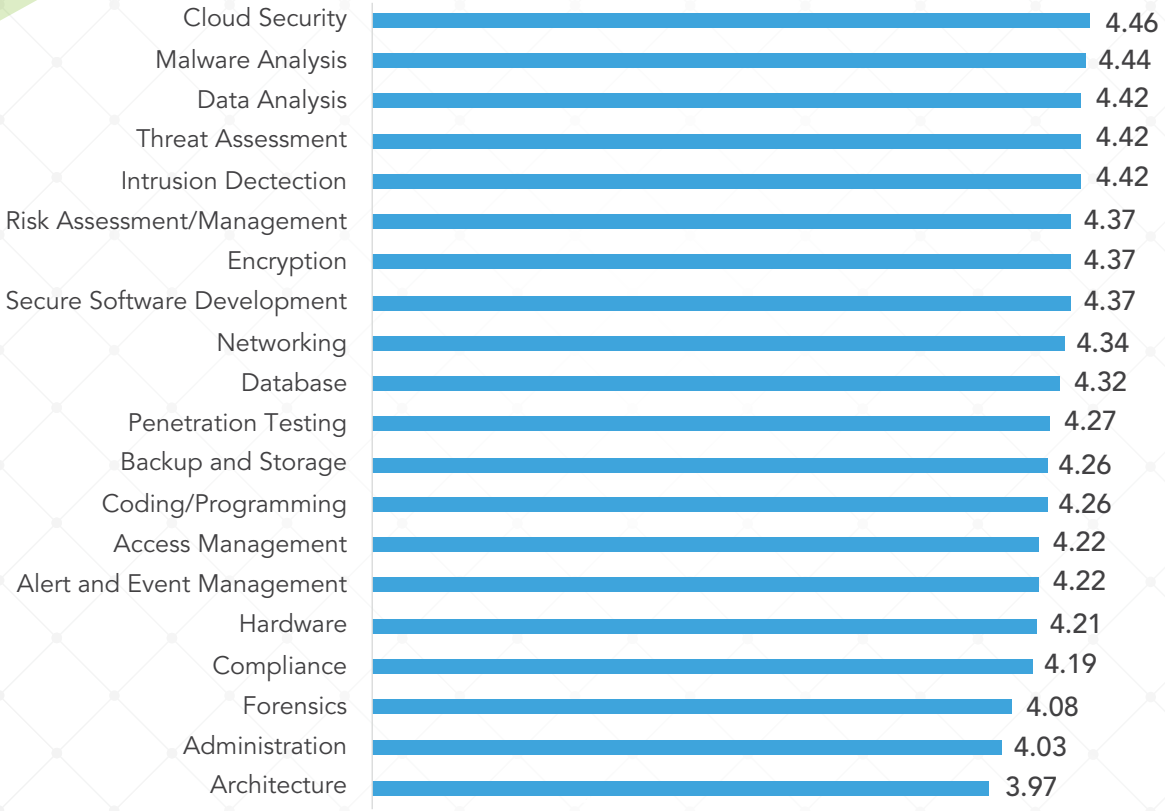
Current jobholders say the following are the top 10 technical concepts or systems cybersecurity pursuers should understand:

TOP 10
TECHNICAL CONCEPTS

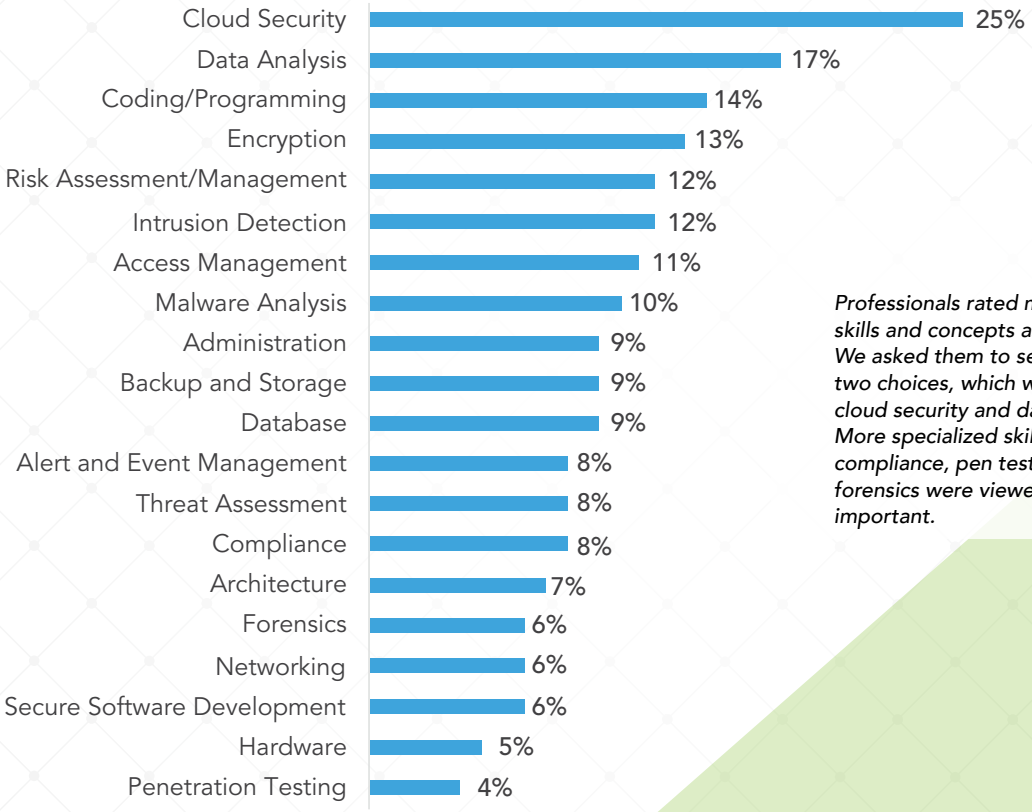
1. Cloud Security
2. Data Analysis
3. Coding and Programming
4. Encryption
5. Risk Assessment/ Management
6. Intrusion Detection
7. Access Management
8. Malware Analysis
9. Administration
10. Backup and Storage

Professionals:

Most Important Technical Skills (Average Rating from 1 to 5)



Top 2 Most Important Technical Skills

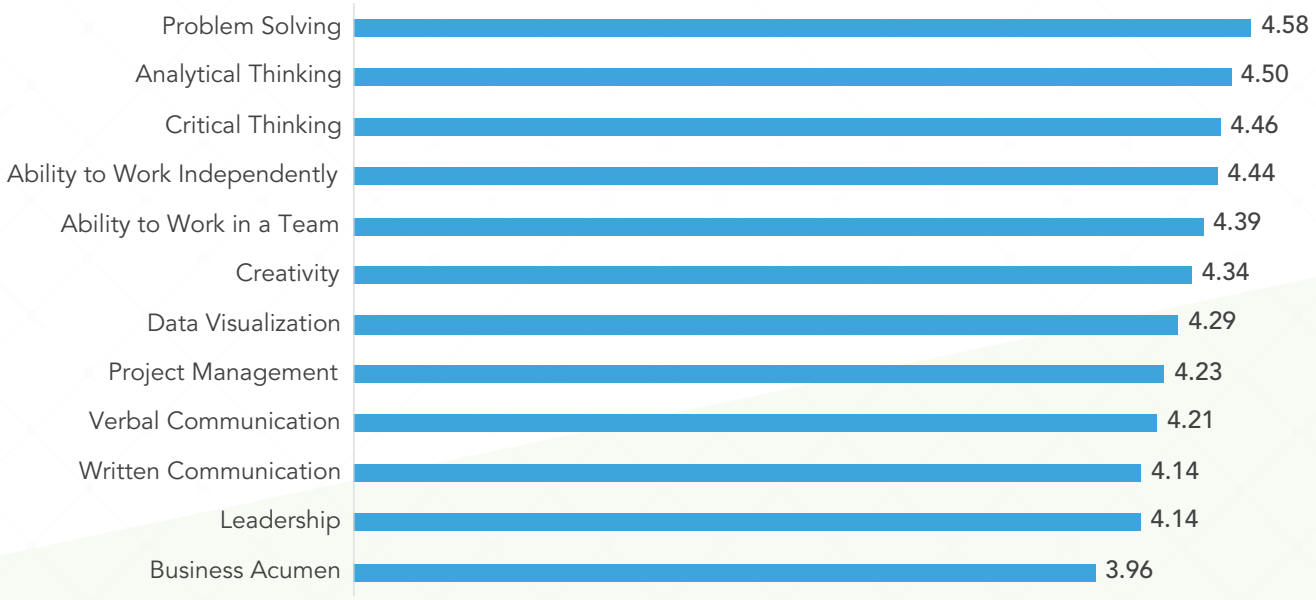


Professionals rated many technical skills and concepts as important. We asked them to select their top two choices, which were led by cloud security and data analysis. More specialized skills such as compliance, pen testing and forensics were viewed as less important.

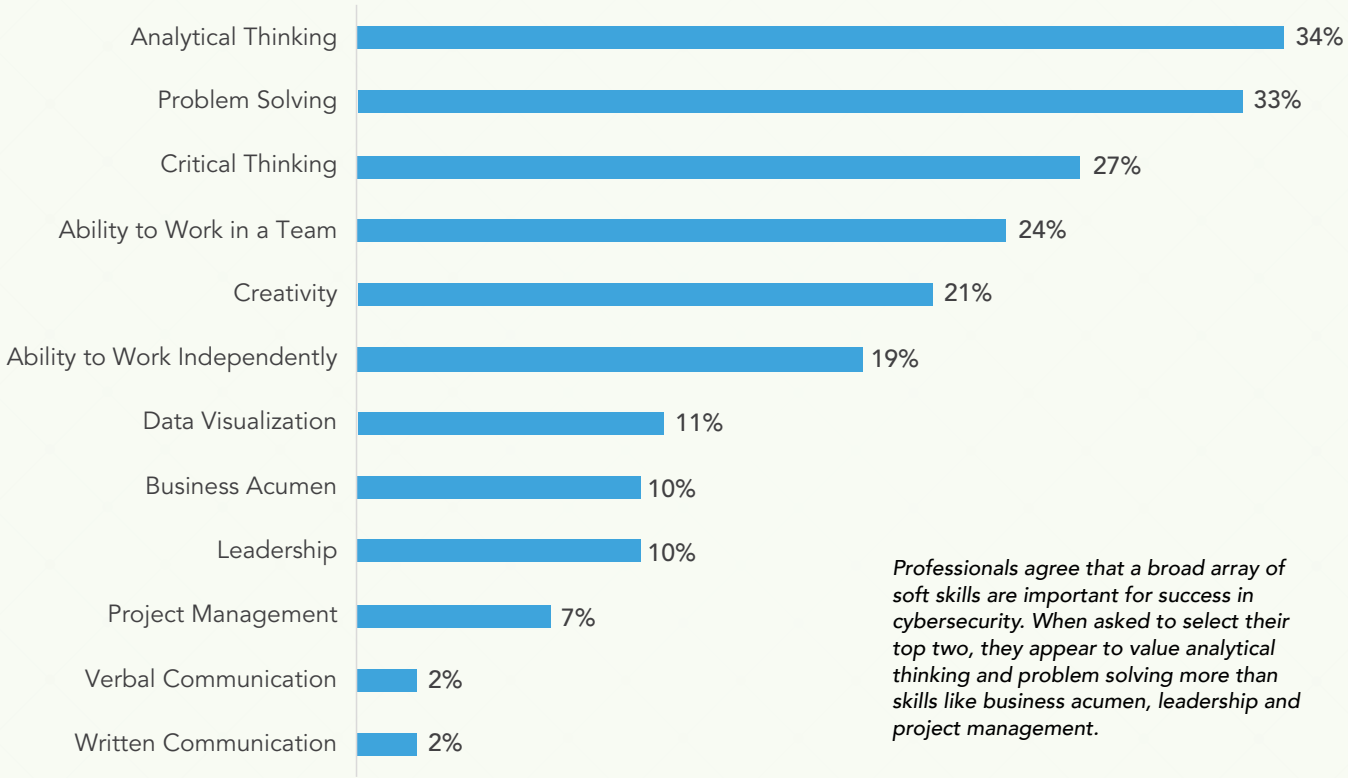
Professionals value an array of non-technical skills they deem important including, analytical thinking, problem solving, critical thinking, ability to work in a team and creativity.

Professionals:

Most Important Soft Skills for Cybersecurity Professionals (Average Rating from 1 to 5)



Top 2 Most Important Soft Skills for Cybersecurity Professionals



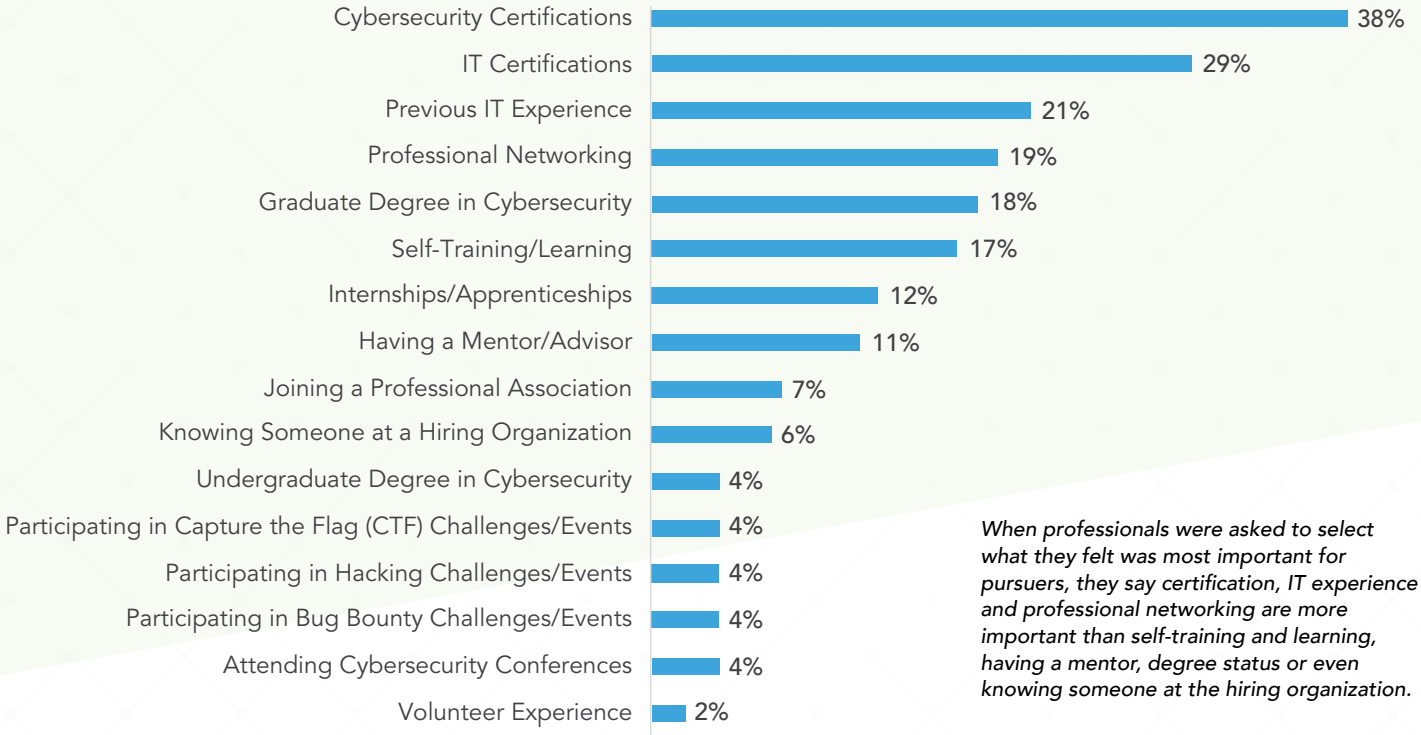
Professionals agree that a broad array of soft skills are important for success in cybersecurity. When asked to select their top two, they appear to value analytical thinking and problem solving more than skills like business acumen, leadership and project management.

As for getting started on their careers, professionals suggest pursuers focus on cybersecurity certifications, IT certifications, pervious IT experience, professional networking and getting a degree in cybersecurity.

Professionals:

What's Most Important for Pursuers? (Average Rating from 1 to 5)

What's Most Important (Top 2) for Pursuers?



When professionals were asked to select what they felt was most important for pursuers, they say certification, IT experience and professional networking are more important than self-training and learning, having a mentor, degree status or even knowing someone at the hiring organization.

THE PROFESSIONAL'S JOURNEY

In addition to our quantitative analysis of what skills and attributes professionals feel are important for those seeking a cybersecurity career, we asked existing professionals the following open-ended questions:

What tasks were you assigned in your first 1-3 years as a cybersecurity professional that helped you the most in your career?

What early successes or challenges did you experience in your first 1-3 years as a cybersecurity professional that served as the best learning experiences?

How did you gain confidence in your first 1-3 years as a cybersecurity professional that cybersecurity was the right profession for you?

The more than 1,000 responses to each question are diverse and revealing. They provide a great deal of insight for organizations and cybersecurity leaders. While common themes – both positive and negative – emerge, responses suggest workers' experiences vary greatly by organization and the relative maturity of their teams, toolsets, processes and other factors.

Common themes among professionals include:

"Thrown into the Deep End" – Professionals speak of being overwhelmed in their first few years and having to survive in a "sink-or-swim" environment. While those professionals who outlast the relentless pace and pressure of their first several years in cybersecurity may ultimately succeed, it may be a high bar for other entry-level and early-career professionals. Many candidates – especially those without previous IT experience but who may offer more diverse perspectives to the team – may become frustrated, lose interest or move on to be successful at another organization.

"First Jobs" – Professionals shared insight into their early responsibilities, including alert and network monitoring, malware analysis, threat remediation, compliance and auditing, policy review, reporting, learning new tools, privacy policy review, and configuring solutions like perimeter and endpoint security defenses. In a field as broad as cybersecurity it may not be a surprise that junior staffers are assigned to such a diverse slate of responsibilities. However, it may suggest a lack of standard, consistent pathways into the field for those taking on their first jobs, as well as unclear routes to advancement and success for many team members.

"Patience and Support" – Professionals often say being part of a team, being able to shadow others and having a more senior team member they can turn to was beneficial in the early years of their careers. Even professionals who felt "Thrown into the Deep End," cite the ability to escalate issues, having clear support and encouragement from management, and receiving guidance from others as beneficial to their long-term success and gaining confidence in their roles.

"Mentors" – Professionals share the value of being paired with a more senior colleague they could turn to outside immediate on-the-job needs like escalating a possible threat. This enables new entrants in the field to learn the intangibles of how to navigate the job, convey critical topics to those outside the team, how to "ask the right questions" and build their support network. In a field that lacks a standard, progressive path for new hires, having a mentor is key for many to learn "how things work" at their organization.

"The Big Project" – Professionals pointed to a significant project they were assigned or contributed to that helped demonstrate their skills to others and bolstered their self-confidence. Some say they were paired with a senior team member on a project or asked to head an initiative on their own for the first time. Early successes, including being assigned to high-profile projects, seem to help professionals gain confidence, feel empowered and better prepare themselves for advancement and greater responsibilities.

"Certifications as Achievements" – Professionals tell us that cybersecurity certifications are important, but they are not necessarily viewed as critical prior to the first years on the job. Many say certifications were a milestone in their professional growth. They point to earning certifications as achievements and another proof point to employers, peers and themselves to validate their skills.

IN THEIR OWN WORDS

The following is a sampling of input we received from professionals. Each row captures responses from the same study participant.

What tasks were you assigned in your first 1-3 years as a cybersecurity professional that helped you the most in your career?	What early successes or challenges did you experience in your first 1-3 years as a cybersecurity professional that served as the best learning experiences?	How did you gain confidence in your first 1-3 years as a cybersecurity professional that cybersecurity was the right profession for you?
I was tasked with updating the security signatures on all endpoint machines during a short period of time. I was also on a team to forensically analyze a major malware intrusion and to cleanse all systems of it afterwards.	Our team was able to contain and cleanse a major malware attack within four hours of detecting its presence.	I was told by my boss/mentor that I had the right aptitude and skills to critically analyze how viruses and malwares can infect our workplace.
Data analysis, trends, process improvements to change management.	Learning to conceptually think in analyzing data and traffic.	Having the light turn on and begin seeing the data differently.
Mentored by a seasoned expert for over a year who taught me to ask questions and look for answers.	Investigating fraud involving multiple countries and organizations.	I always wanted to figure out solutions to why something is happening.
I was assigned to IT management at a security firm out of college and that gave me the base I needed to go in to cybersecurity.	I was able to stop anyone from breaching any firewalls that we put in our systems.	I just gradually, over time, got better at my job and better with solutions.
Working with teams, solving problems with limited time, critical thinking out of the box problems solving and dedicated to the job.	Lack of skills and being active and working super hard to solve problems and maintaining all the crisis at the same time.	Instincts. Having a clear path of helping people and protecting infrastructure. And the high salary inspired me.
I was an early apprentice assigned to a senior security expert which allowed me to learn under fire.	A number of routine security failures, penetrations, and discoveries emboldened me to be the best at my profession.	Experience gained on the job positioned me well in my craft.
Working a help desk that focused on problems was beneficial to me.	I learned by trial and error. Baptism by fire is the best way.	I had a patient mentor, and I was willing to learn.
I was tasked with analyzing access data to determine if there had been any successful hacks and assess the level of risk within the system. I really didn't have any coding experience, but this hands-on task helped me to start coding.	The first few years I wasn't really able to get a clear big picture of the systems and how they interact. As my knowledge base grew, so did my ability to troubleshoot issues. It's critical to be able to analyze data and then look at the bigger picture.	At the end of my first year on the job, I got a large cash bonus and it was bigger than anyone else got. I figured I was doing a good job if my bosses gave me such a large bonus.

What tasks were you assigned in your first 1-3 years as a cybersecurity professional that helped you the most in your career?	What early successes or challenges did you experience in your first 1-3 years as a cybersecurity professional that served as the best learning experiences?	How did you gain confidence in your first 1-3 years as a cybersecurity professional that cybersecurity was the right profession for you?
I assigned my own tasks and went from one plateau to another. I only had the basic understanding of cybersecurity when I first started.	Moving from administration to security ... or at least taking on more was a slow transition at first; however, once I was focused, I was able to complete anything I attempted.	It was never my prime responsibility but I ended up loving the field once I was exposed to it.
I was scanning systems for viruses. I have been working in cybersecurity since we carried around a [vendor name removed] anti-virus on a diskette and the internet was not available.	I was removing viruses from computers when many people didn't even believe they existed.	My career evolved into Cybersecurity from hardware repair to network design and troubleshooting to cyber threat response and remediation.
First, I was building security firewalls, and then trouble shooting problems associated with the overall networking.	Some challenges that I endured in my first years were being able to decipher between what was a threat and how to effectively combat it through the use of advanced technology.	I learned by trial and error, and was able to handle any system breaches.
I was assigned many tasks including working with security tools and software.	There was a steep learning curve and many things to become familiar with.	I had good success and worked with many strong staff members in my first few years.
I was assigned forensic audits and risk assessments.	I enjoyed great mentoring that enabled me to work with confidence. It was a steep learning curve as things are continually evolving in this field.	Working with a mentor.
When you first get started, it was really helpful to shadow and be mentored by someone with more experience.	Challenges and difficult situations are always great learning experiences in this field of work.	As you start experiencing success, your confidence will grow and it grows from there.
Working with cybersecurity teams pushed me out of my comfort zone and helped me learn the most.	Everything was a challenge the first few years, and there was a huge learning curve. Perseverance was the key.	Realizing that I could handle things that I didn't think I could.
I was able to shadow someone I perceived as an expert in the field. The man really knew his stuff.	Massive failure! It was hard but it taught me the best; failure always teaches you.	By failing and learning from my failures, it motived me.
Security analyzer and it helped me a lot in my following years because it gave me critical information	I really got promoted a lot in my recent years and now I am responsible for the security of my company.	I loved cybersecurity since day one and because of that I was really confident that this is the right field for me.

What tasks were you assigned in your first 1-3 years as a cybersecurity professional that helped you the most in your career?	What early successes or challenges did you experience in your first 1-3 years as a cybersecurity professional that served as the best learning experiences?	How did you gain confidence in your first 1-3 years as a cybersecurity professional that cybersecurity was the right profession for you?
Initially worked on the cyber threat team working closely with AML Compliance to identify incidents where there were hacking attempts or incidents to penetrate customer data for fraudulent activity. I learned a great deal in that role and formed good business relationships.	It was a challenge learning regulatory compliance requirements, picking up legal ramifications but it was very rewarding working closely with fellow cybersecurity, Compliance and Legal colleagues.	I studied hard learning my role, researched on my own time, earned certifications, attended training courses and conferences. All of that helped me to grow in my career.
I was tasked with looking for possible threats, and putting into place best practices to mitigate any risks.	My earliest success was getting certified in the first place since it was quite an ordeal getting that done. My greatest challenge was dealing with accessibility issues that come with working with different types of software. I am totally blind, and this can make things very interesting at times.	I had gained my confidence, and still continue to do so, through colleagues and mentors.
In the first three years, I was assigned to cybercrime, cloud computing and database which, in the future, helped me in my career.	As for me, cloud computing was the most challenging task and it served as the best learning experience.	I loved this profession. Moreover, a senior officer always guided me and helped me gaining confidence. And that's why I'm a cybersecurity job holder.
It was the typical cybersecurity analyst jobs that allowed me to be well acquainted with the job and its various layers, namely: installing firewall, setting up encryption, breach discovery and reporting breaches, documenting system weak spots, and running simulated threats / attacks to find vulnerabilities.	Setting up a process and plan for threat detection, alerting, and response protocols when there were no systems in place previously, generally for clients who had no dedicated security personnel or consultants prior to our arrival.	Having a mentor/mentee relationship with a more experienced group of people. They shadowed me and backed up my work and decision making with their own expertise until I was strong enough to stand on my own without allowing threats to become concerns in client environments.
Basic detection and intrusion models.	We stopped a lot of bugs and didn't bother with false positives.	I solved a lot of problems and it showed I was on the right career path.
I was tasked to shadow my mentor when I first started and that helped tremendously being able to see how he handled everything and what was expected of me on a daily basis.	Just day-to-day experience and constantly learning. You can never have too much knowledge as the job and threats are constantly evolving. The first time an issue comes up and you're able to deal with it, it gives you so much confidence in your ability and yourself.	My mentor helped a lot. He guided me through what was expected of me and helped me get the job in the first place. I was very fortunate as not everyone will have that. It gave me a lot of confidence knowing someone was always there for me and someone that I could go to.

WHO ARE THE PURSUERS?

1,010 study participants are actively seeking a role in cybersecurity. Since IT has historically been a significant source of cybersecurity talent, our sampling methodology for pursuers was designed to ensure a balance of perspectives by including a mix of pursuers currently in IT roles and pursuers currently employed in other fields. The final composition of our pursuers participants was 58% in an IT role and 42% not in an IT role.

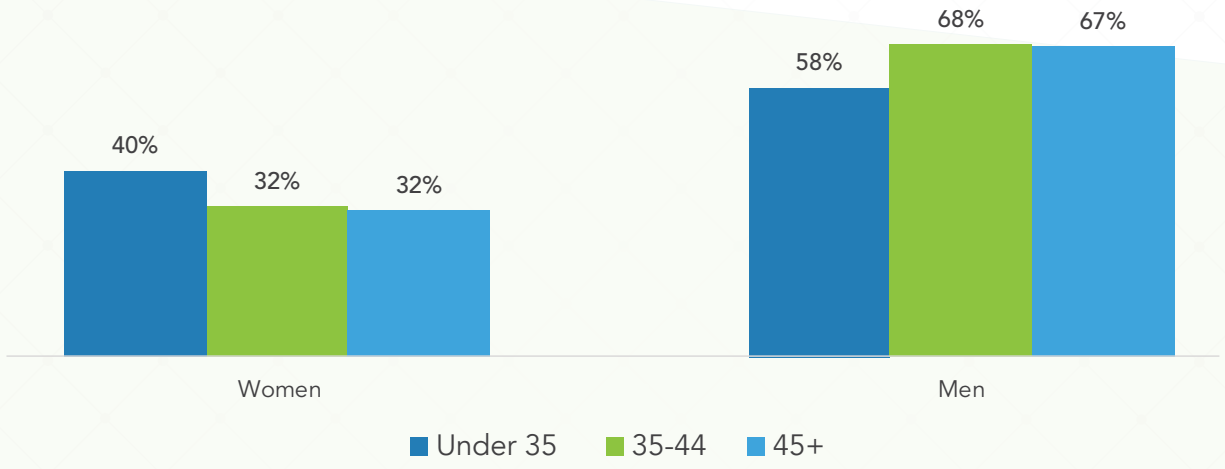
We asked this group many of the same questions as professionals already in the field. Our goal was to understand if their expectations and perceptions align with those currently in the workforce. Sharing these findings can help hiring organizations better understand how to attract, retain and develop these new cybersecurity workers.

Generally, cybersecurity job pursuers are younger than those already in the field. Most pursuers (58%) are younger than 40 years old, with 48% of them between 30 and 39. Still, more than a third of pursuers (36%) are between the ages of 40 and 59.

The gender breakdown among pursuer participants is 65% men and 35% women*, which is nearly equal to the gender distribution of existing professionals we spoke to.

More than half (58%) of pursuers in our study currently work in IT roles. Findings indicate the 34% of pursuers with 3 to 6 years of experience in IT show the strongest interest in pursuing cybersecurity jobs, followed by the 26% with 7 to 10 years of experience in an IT role.

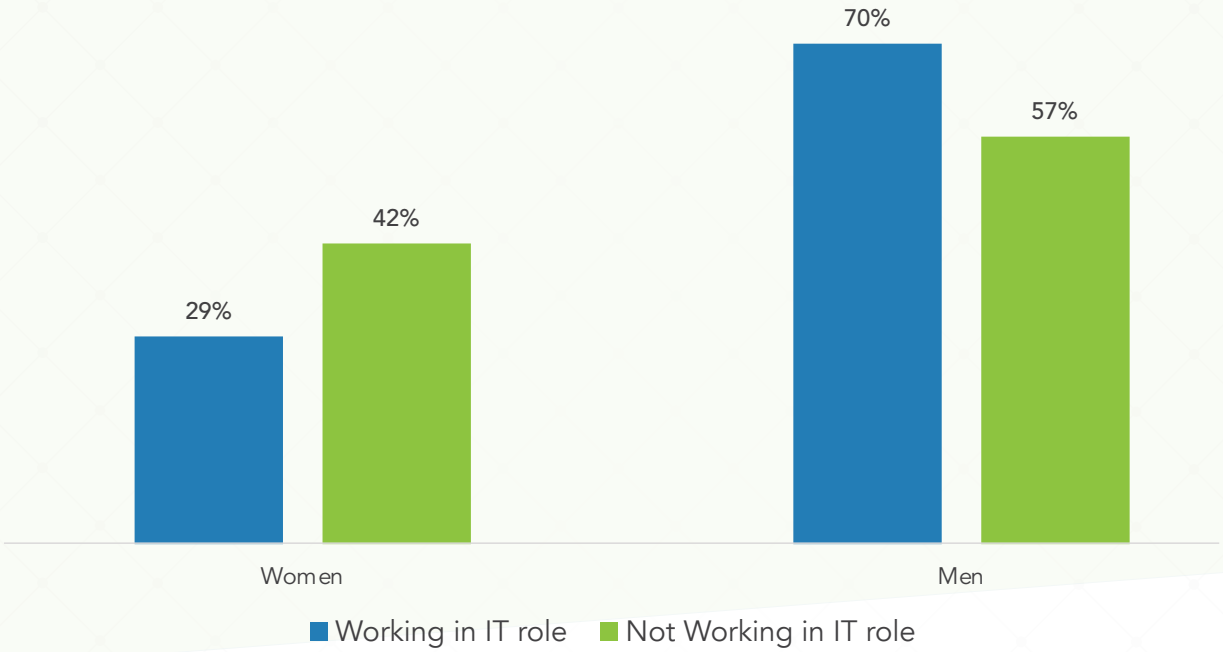
Pursuers: Breakdown by Age and Gender



The highest percentages of women pursing a cybersecurity job are under 35. Data also suggests that men start to consider cybersecurity later in their careers.

Women with IT roles seem to show interest in pursuing cybersecurity earlier in their IT careers compared to men. Of pursuers with less than 3 years of experience in IT, 26% of women are already interested in landing cybersecurity jobs compared to 18% of men. This trend continues for those with 3 to 6 years of experience, when 40% of women compared to 32% of men are actively pursuing cybersecurity jobs. Higher percentages of women than men appear to be pursuing cybersecurity positions earlier in their careers.

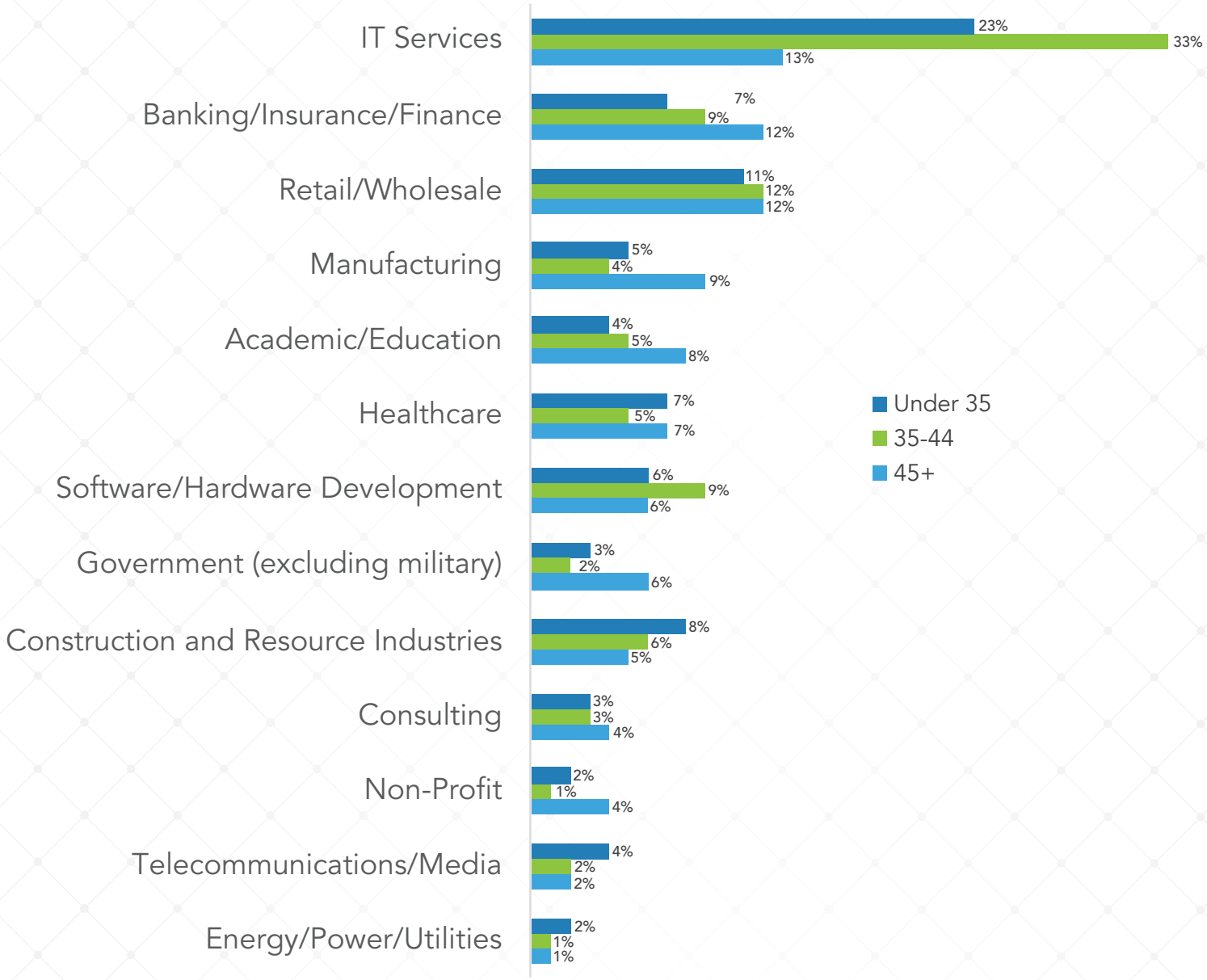
Pursuers: Higher Interest Among Women Without IT Roles



There is more interest in pursuing a cybersecurity role among women without IT roles (42%) compared to the 29% of women pursuers who have IT roles.

There is also more interest in the field for those not in an IT role among younger study participants. 36% of those without IT roles pursuing a cybersecurity job are under the age of 35 compared to 28% of those with IT roles.

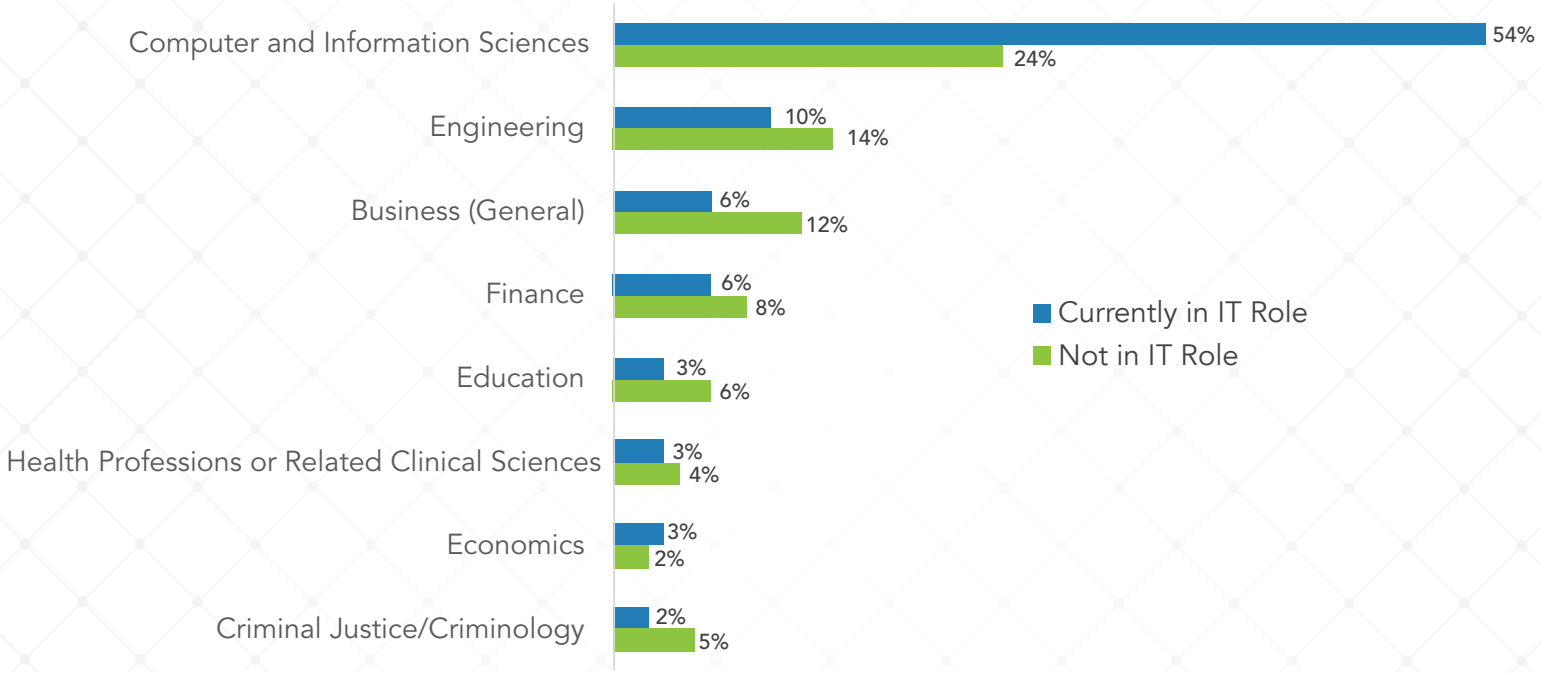
Pursuers: Where They Work Now



The highest percent of pursuers in our study currently work in IT services, suggesting this field is fertile ground for new entrants especially among those 35 to 44 years old who may be prime candidates for transitioning to security roles.

Like those already in the field, pursuers are well educated, with 64% holding a bachelor's or master's degree, and 5% holding a doctorate. Close to half of all pursuers (42%) sought education in computer and information sciences. This increased to 54% among those with IT roles, but 24% of pursuers not currently working in an IT role also studied computer and information sciences.

Pursuers: Educational Background

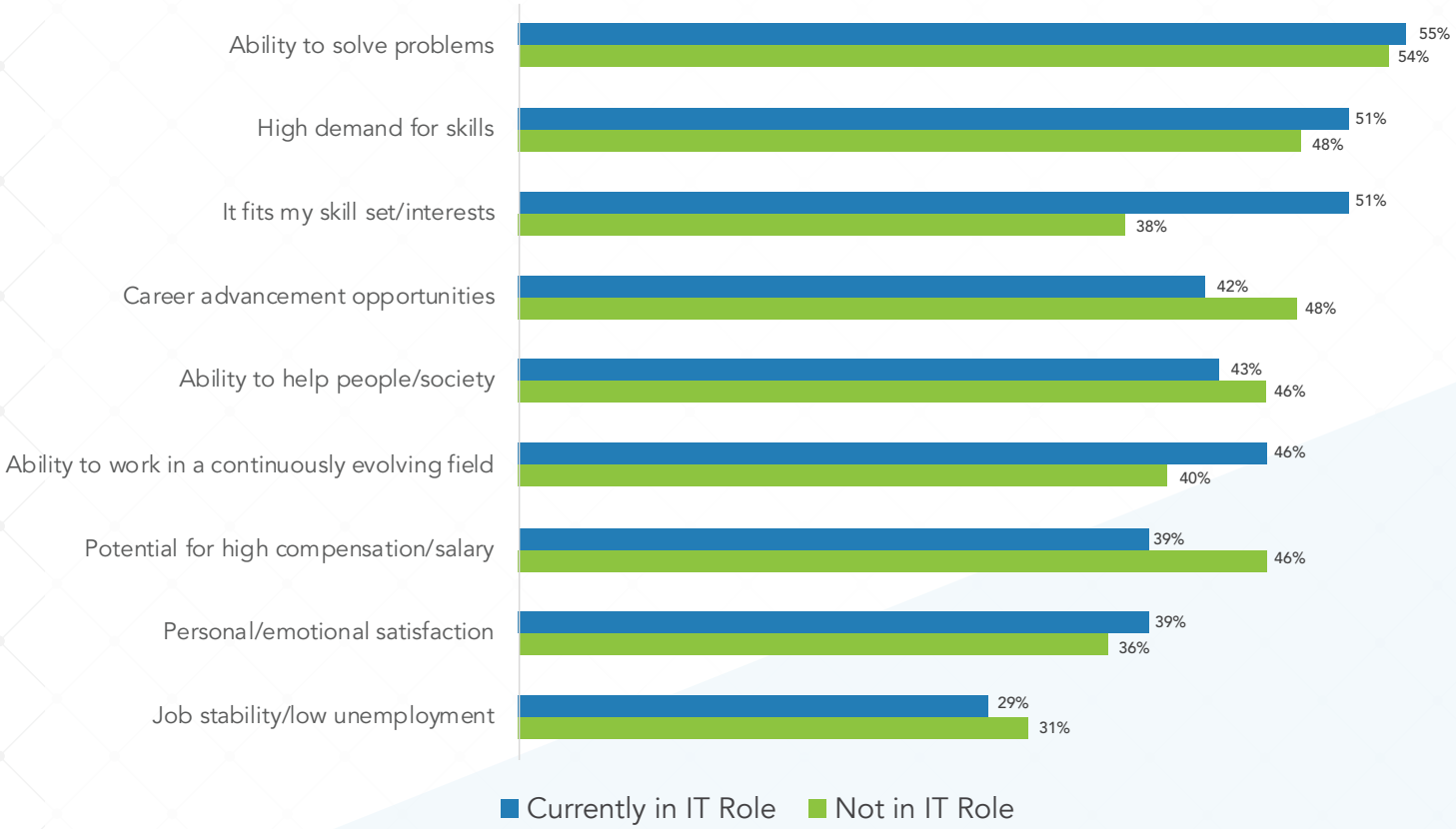


54% of pursuers with an IT role pursued education in computer and information sciences. Pursers not currently working in IT come from a much broader range of disciplines.

Among pursuers, 9% are active or retired military, and 8% are working in or retired from law enforcement.

When asked what motivates them to join the cybersecurity field, pursuers cite as most important: *ability to solve problems* (54%), *high demand for skills* (50%), *it fits my skill set/interests* (46%), *career advancement opportunities* (45%), and *ability to help people/society* (44%). High salary ranked lower (42%) as a motivator.

Pursuers: What Motivates Them?



When asked what motivates them to seek a job in cybersecurity, pursuers cited a range of factors. There were some differences between pursuers with IT roles and those without. 51% of pursuers with an IT role felt that cybersecurity fit their skill set compared to 38% of those without. Meanwhile, salary was a stronger motivator for those without an IT role.

THE NEXT GENERATION:
CONFIDENT AND UNCERTAIN.

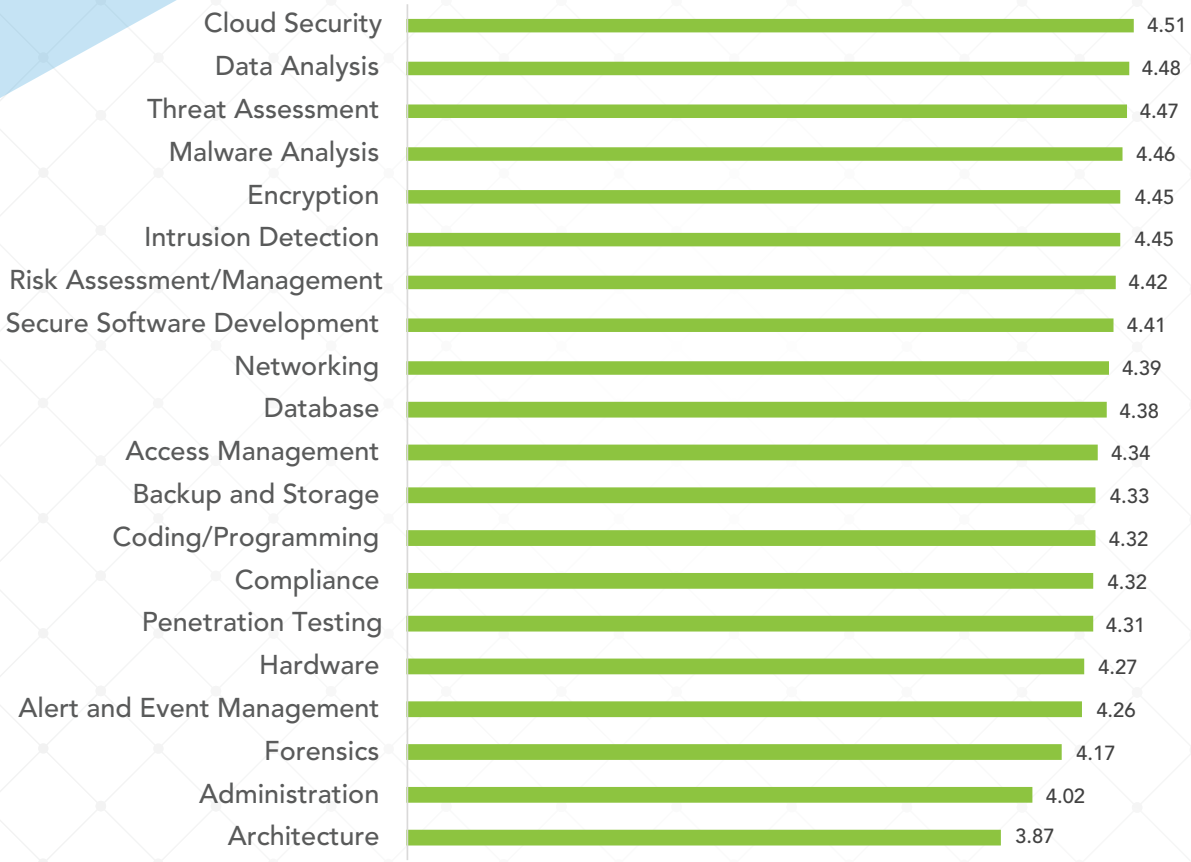
We asked pursuers to rate a broad range of attributes, including technical and soft skills, to produce weighted *Top Lists* of what they feel is most important for success in their future cybersecurity roles.

When asked what technical concepts or systems are most important to understand for those seeking their first cybersecurity job, there were striking similarities between pursuers and professionals. Pursuers listed the following as their most important technical skills:

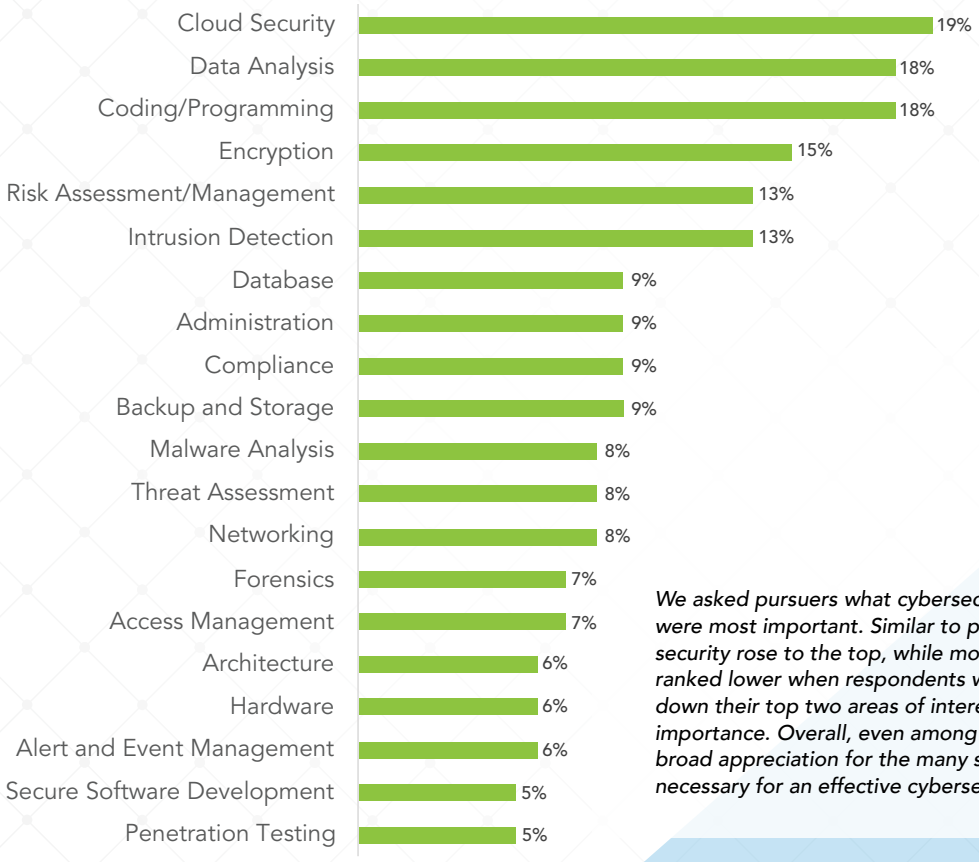
TOP 5
TECHNICAL CONCEPTS

1. Cloud Security
2. Data Analysis
3. Coding/Programming
4. Encryption
5. Risk Assessment/ Management

Pursuers: Most Important Technical Concepts (Average Rating From 1 to 5)



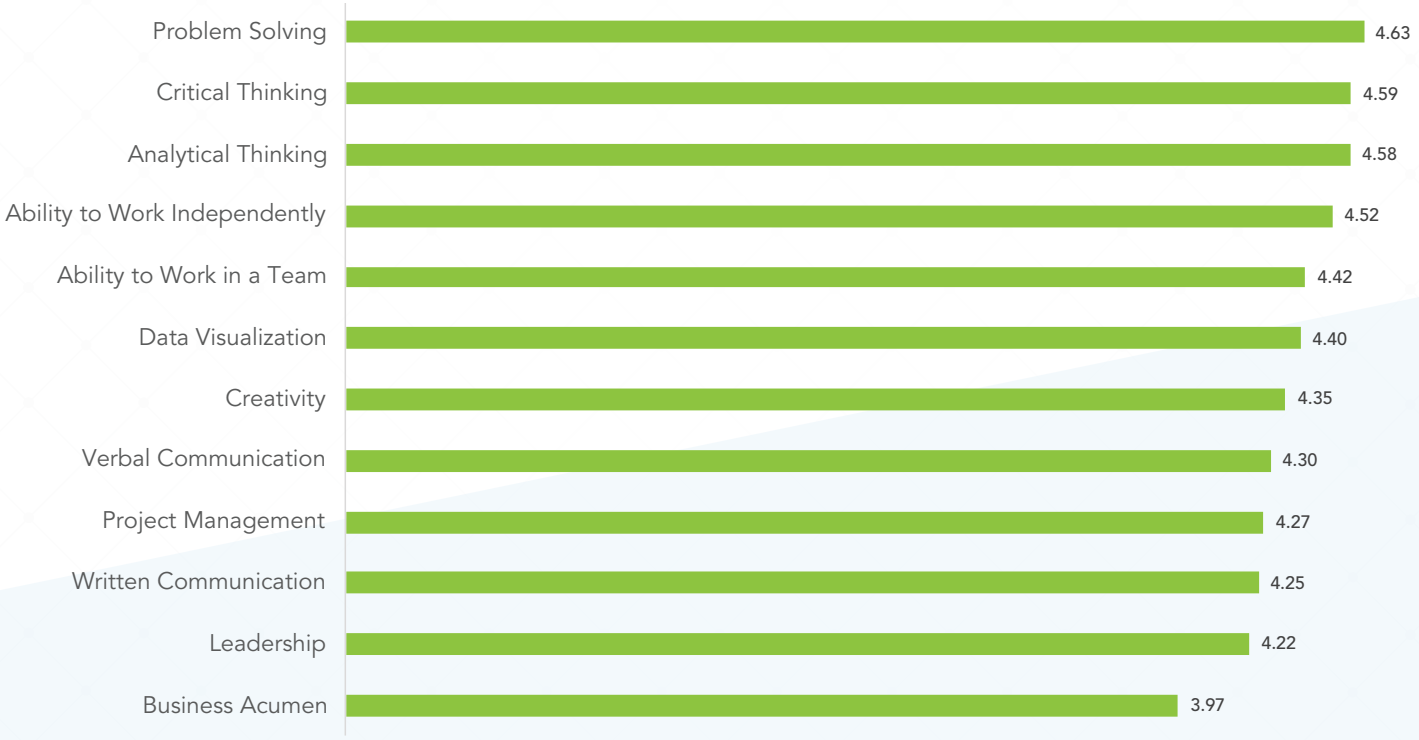
Top 2 Most Important Technical Concepts



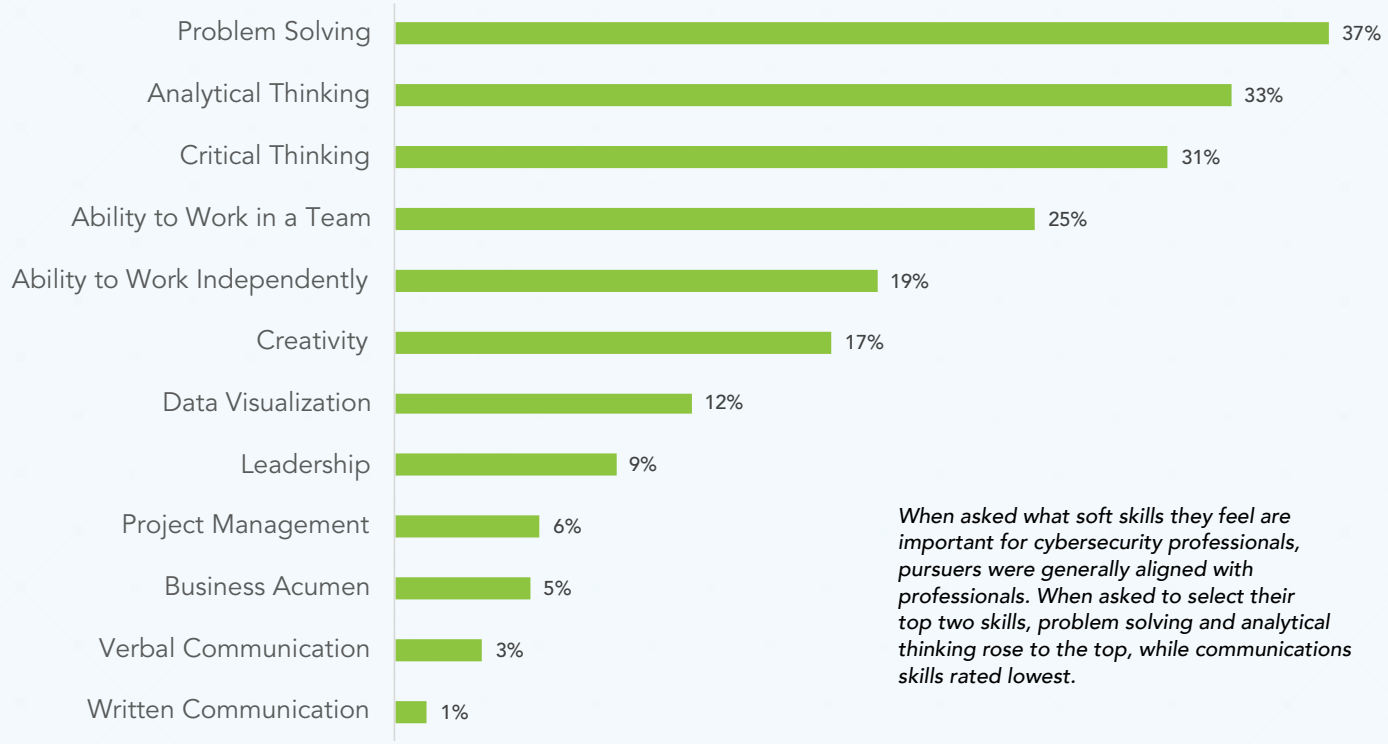
We asked pursuers what cybersecurity technical skills were most important. Similar to professionals, cloud security rose to the top, while more specialized skills ranked lower when respondents were asked to narrow down their top two areas of interest based on perceived importance. Overall, even among pursuers, there is broad appreciation for the many skills and disciplines necessary for an effective cybersecurity program.

When asked about non-technical skills that will be important to cybersecurity workers, pursuers cited problem solving, analytical thinking, creative thinking, ability to work in a team and ability to work independently.

Pursuers: Most Important Soft Skills for Success (Average Rating From 1 to 5)



Top 2 Most Important Soft Skills

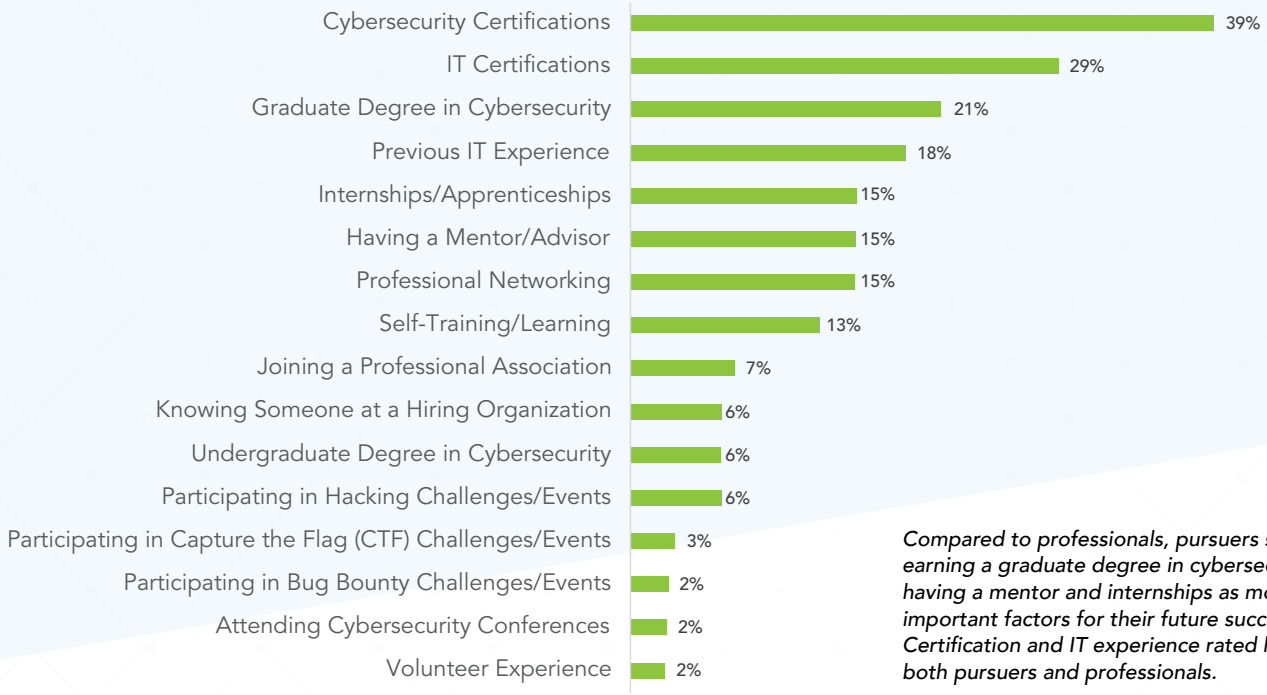


When asked what soft skills they feel are important for cybersecurity professionals, pursuers were generally aligned with professionals. When asked to select their top two skills, problem solving and analytical thinking rose to the top, while communications skills rated lowest.

As for getting started on their careers, pursuers believe the following are most important for their success: cybersecurity certifications, IT certifications, degrees in cybersecurity, IT experience, having a mentor, professional networking and internships.

Pursuers: Most Important Keys to Success in Cybersecurity (Average Rating from 1 to 5)

Top 2 Most Important Keys to Success in Cybersecurity



Compared to professionals, pursuers saw earning a graduate degree in cybersecurity, having a mentor and internships as more important factors for their future success. Certification and IT experience rated high for both pursuers and professionals.

THE PURSUER'S JOURNEY

Similar to the open-ended questions we asked existing professionals participating in our study, we also asked a series of questions to pursuers. Our goal was to uncover any misalignment in expectations for what cybersecurity jobs may entail, challenges they'll face and why they feel they are right for cybersecurity. We asked the following questions

What tasks or responsibilities do you expect to be assigned in your first 1-3 years as a cybersecurity professional?

What do you believe will be the biggest challenges you will face in the first 1-3 years of your cybersecurity career?

How confident are you that cybersecurity is the right career choice for you and why?

The more than 1,000 responses provided to each of the questions above reveal that many pursuers are unsure about what kind of tasks they will be asked to perform. This varies to a degree when comparing results from pursuers with an IT role and those without. Respondents with an IT role typically expect technical security challenges and tasks.

Common themes among pursuers include:

"I Don't Know" – While less prevalent among pursuers with IT roles, many participants simply state they do not yet know what to expect from their first cybersecurity job. For a profession that can touch upon everything from security operations, risk assessment and management, privacy, user training, compliance, governance, policy, forensics, pen-testing and more, it may be that pursuers – especially those outside of IT – find it difficult to define the role. Previous (ISC)² research found that perceptions of cybersecurity jobs are often shaped by media and not by first-hand knowledge or access to people already on the job.[vii]

"Starting from Scratch" – Pursuers seem undaunted by the fact that they may not know exactly what to expect on day one. They anticipate they will need to start from scratch and work their way up. This is even true of pursuers with years of IT experience. Many feel they will be given basic tasks to help them learn and gradually earn more responsibilities.

"Will Need Training" – Pursuers expect training to be available. They cite on-the-job training to become proficient at the tasks assigned, as well as some degree of assistance or at least patience from their employer as they pursue additional education and work to earn cybersecurity certifications.

"Perceived Barriers" – Despite the high demand for cybersecurity talent, pursuers seeking their first cybersecurity role – even those with IT experience – say finding a job is difficult. They expect learning on the job and then performing the role will be "hard work." They also anticipate the challenge of keeping up with evolving threats and the security solutions they will be using. While they are uncertain of many aspects of the job, they say they are willing to put in the time and work to grow and be successful. Additionally, some cite lack of coding skills as a barrier, underscoring a potential pitfall that may not be insurmountable for many depending on the role they acquire.

"Aware of the Basics" – Many pursuers – including those with and without IT roles – are aware of the prevalence of different threats and continuing security issues. For example, they specifically cite phishing, ransomware, malware, intrusion detection, cloud security, user behavior, threat detection and other relevant topics without prompting. This suggests that pursuers aren't merely intrigued by an in-demand field, but instead have some knowledge and interest in the concepts and challenges facing the field.

"Very Confident and Motivated" – Despite the recognition that they will need to start from scratch and need to be patient as they learn a new field, pursuers are eager and passionate about entering the cybersecurity profession. They tell us how important cybersecurity is for organizations. They feel they can make an impact. They welcome the challenge. They have a strong interest in the field. They view it as career advancement opportunity and entering a profession that is in high demand.

IN THEIR OWN WORDS *(Pursuers not working in an IT role)*

The following is a sampling of input we received from cybersecurity job pursuers not working in an IT role. Each row captures responses from the same study participant.

What tasks or responsibilities do you expect to be assigned in your first 1-3 years as a cybersecurity professional?	What do you believe the biggest challenges you will face in the first 1-3 years of your cybersecurity career?	How confident are you that cybersecurity is the right career choice for you and why?
Mostly just shadowing and learning about the new organization's general procedures and internal infrastructure.	Having the time to keep up with the latest trends and gaining the proper knowledge in order to advance in my career.	I'm interested in pursuing new opportunities because I always like learning new things. And I know that there is ever increasing interest and concern when it comes to cybersecurity.
Compliance, intrusion detection.	Detecting intrusion.	Fits my skills. Job security. Good salary.
To keep the systems threat-free.	The nuances of threats.	I am very confident that cybersecurity is the right career choice for me because I have always had a passion for the field starting from a young child.
I certainly expect to start at the bottom and do the most basic tasks.	Finding the right connections and path to succeed.	I love the process and the challenge. Everyone should try to do something that they love.
I am not entirely sure, but I expect it to be pretty entry level.	Adapting to a whole new list of tasks each day.	Pretty confident, as I am looking to transition into a new field, where I am able to utilize what I consider to be my great problem-solving skills.
I think some sort of apprenticeship where you could learn, propose and design. I do not think (even with certifications) that you will receive a major project out of the gate.	I think a short learning curve will be a challenge as well as keeping your skills current.	I think it is the future - it is interesting, challenging and will be a more in-demand career path in the near term (and long term).
Compliance with regulations based on the system.	Staying current with ever changing technology and business needs.	I am very confident because our world is becoming more and more dependent on technology.
Installing, maintaining and troubleshooting anti-virus software along with firewalls.	Understanding that once I'm in the field, that I'll have to always keep learning about new threats. My understanding won't stop at what I learned from my degree.	I'm very confident, because with how our economy is becoming more dependent on the online economy and transaction, I think this will be both not only lucrative and in demand, but highly respected and fun.

What tasks or responsibilities do you expect to be assigned in your first 1-3 years as a cybersecurity professional?	What do you believe the biggest challenges you will face in the first 1-3 years of your cybersecurity career?	How confident are you that cybersecurity is the right career choice for you and why?
Setting user access controls; monitoring network for irregular activity; detect and patch vulnerabilities; document and assess causes of breaches.	I think that, as a woman, the biggest challenges that I will face in establishing a cybersecurity career will relate to finding employment in the male-dominated field of IT.	I am confident that cybersecurity is the right career choice for me because I am an excellent problem-solver and very good at thinking critically. I expect that there will be many opportunities in the near future, especially now that so many businesses have gone digital due to COVID.
I have no idea what to expect. It could be anything from password reset to identifying threats.	Getting caught up to speed as far as the latest cybersecurity threats.	I am someone that has grown up with technology and have seen my own computer problems. I'm confident I could love most issues.
At first, mainly the maintenance and troubleshooting of existing infrastructure. Securing endpoints, updating employee devices, providing helpdesk support. Ensuring policy and governing requirements are met: Ensuring compliance.	Continuing education and training to receive the proper certifications and other required credentials.	Extremely confident. I have a background in computer science and some experience helping end users with security concerns and incidents as a remote tech for 3+ years. Also, being in the corrections industry know it would be a great blend of my current skills.
Setting up security parameters and tracking the effectiveness, constant upgrades.	The dynamic field will be a challenge. Criminals are always finding new ways to commit high tech fraud and other crimes.	I am confident that it is right for me, I am always trying to figure out ways to improve upon security and find it rewarding helping people keep their information safe.
Ransomware issues, phishing attacks, web application security, network security and defense.	I need to be patient, and not get frustrated when things get difficult. I have to be willing to ask for help. I hear that persistence is everything.	It's an evolving field, that requires analytical thinking and resolving problems. I'm good at that. It will always be in demand and pays good money.
I will perform security assessments and penetration testing of hardware, software, and network products including third party products.	All the technical knowledge that I have to learn.	Very confident because I feel very passionate about cybersecurity.
Identify threats, upgrade and implementation of security controls, performance reports, assess and patch vulnerabilities.	I believe that it will be a challenge for me to find employment because I have not been working in IT for a number of years.	I feel confident that cybersecurity is the right career choice for me because I enjoy working with IT and there will be many more career opportunities in the future.
I would like to work at a small to medium sized company with an in-house IT.	Getting the right certifications and experience to establish myself as knowledgeable and qualified.	I find the field to be fascinating and challenging at the same time. I am confident that my skills will be an asset.

IN THEIR OWN WORDS *(Pursuers working in an IT role)*

The following is a sampling of input we received from cybersecurity job pursuers with IT experience. Each row captures responses from the same study participant.

What tasks or responsibilities do you expect to be assigned in your first 1-3 years as a cybersecurity professional?	What do you believe will be the biggest challenges you will face in the first 1-3 years of your cybersecurity career?	How confident are you that cybersecurity is the right career choice for you and why?
I expect to be responsible for tracking intrusions and setting up criteria studies.	Learning all the various products for security.	It's an area that's very popular and my area is shrinking these days.
Evaluate existing systems, perform threat assessments, provide solutions.	Finding time to go to school for the certifications.	Very confident because I see many instances in my current IT work where security is not emphasized; and I am passionate about it.
Getting your feet wet by getting exposed to the various aspects of the cybersecurity field before getting specialized in any one particular domain.	The evolving nature of the field of cybersecurity and to constantly update myself to keep up with the changes in that field.	Because of the vast future potential that it has and because we are seeing only the tip of the iceberg of the cybersecurity field.
Monitor network and application performance to identify irregular activity. perform regular audits to ensure security practices are compliant.	To do my jobs as well as is expected from me.	Very confident because I find my qualities are the best for the job.
Intrusion prevention, risk mitigation, data breach analysis.	It's going to be the grasping of all information and fundamentals of the cybersecurity field. This will be the greatest challenge, as well as applying what I have learned in real-world scenarios within the company I will be working with.	I am just slightly confident for now, but I am positive that it is the right career choice for me because I want to challenge myself and excel in this field.
I expect to work on security technologies and applications.	The lack of experience.	It has a promising future.
Keeping the department you are responsible for safe from threats the whole time.	The continuous updates of security and new threats nearly every month.	Extremely confident because it's my hobby and dream job and have a lot of knowledge in this field.
Pen Testing and active security response assessment.	Catching up to the leaders in my field in experience and skill sets.	Because it clicks with my mindset and I already excel at it.

What tasks or responsibilities do you expect to be assigned in your first 1-3 years as a cybersecurity professional?	What do you believe the biggest challenges you will face in the first 1-3 years of your cybersecurity career?	How confident are you that cybersecurity is the right career choice for you and why?
Training and apprenticeships, cloud management, supervision.	Lack of adequate training and practice in cybersecurity there might be some problems that may occur to me.	I have complete confidence in this option. I like my job to be this way, and I find myself adept at it.
Looking for vulnerabilities and risks in hardware and software.	Building firewalls into network infrastructures.	Frankly, I am interested in cybersecurity because it protects data against hacking and theft.
Set up security to monitor the security, and programs ... monitor activity of each computer.	Technology is changing so rapidly. The biggest threat is the changes and keeping up with them.	I am not confident, but I believe it would be an added benefit in the job market.
Learning the risks our organization faces and beginning to build a plan to prevent them.	Just catching up to all that is going on and trying to anticipate.	I'm very confident.
Firewall maintenance and penetration testing.	Keeping up with the changing technology.	I'm pretty confident as I enjoy working individually and in a team environment protecting my network and company.
Security Framework Analysis, Basic Firewall Security, and Data/ Information Systems Security.	Furthering my education, out of the classroom/office.	The interest and job security are both winning formulas.
Obtain professional security certificate, help the company develop business, safeguard the company's interests, and prevent the company from losing data.	For dealing with security tasks, it is difficult at the beginning and needs to communicate in time when there are difficulties.	This is a very helpful career for the development of the company's industry. It has great potential, has a large market, and has enough salary.
Email security, Network security, Web security, forensics.	Too many areas to learn for a good security strategy	A critical challenge of cybersecurity is the lack of qualified professionals to do the job. A career in cybersecurity can be stressful, it's also extremely rewarding. I am a problem solver, a quick learner, an avenger, self-motivated, with passion and creative.
I would like to create plans and write code on how to defend against cybersecurity threats. I want to be able to handle projects in this line of work.	Learning the basics and finding an organization that will hire me to do so.	I enjoy IT work. So, it seems cybersecurity is a natural career transition. I enjoy the challenge of keeping online systems secure and free from attacks.

PROFESSIONALS AND PURSUERS

How Different are They?

PROFESSIONALS

PURSUERS

Age Breakdown

26%: < 35 years
48%: 35-44 years
26% : 45+ years

< 35 years: 31%
35-44 years: 45%
45+ years: 24%

Gender Breakdown

33% Women 67% Men

Women 35% Men 65%

Education Undergraduate or Higher

81% — 69%

Computer Science Degree

51% — 42%

Employed in IT Services

34% — 25%

Are drawn to cybersecurity to help people/society

37% — 44%

Rank creativity as a top soft skill for cybersecurity professionals

21% — 17%

Rank cybersecurity certifications as the most important attribute for pursuers

38% — 39%

Rank cloud security as the most important technical skill for cybersecurity pursuers

25% — 19%

Think having an education in cybersecurity is critical for cybersecurity pursuers

42% — 37%

Think having IT experience is critical for cybersecurity pursuers

57% — 55%

SMARTER TEAM BUILDING

The reality facing organizations today is that there are simply not enough skilled cybersecurity professionals to adequately defend their critical assets. At a time when it has never been more essential to build resilient organizations ready to respond to any cybersecurity crisis, there is no abatement to the cybersecurity workforce gap.[viii] While spending on security technologies continues to grow, organizations still struggle to address the vital, central piece of the equation: the human element. No amount of automation or machine-learning algorithms can replace the experience, strategy, instinct, creativity and determination of a skilled cybersecurity team.

Organizations need to take it upon themselves to build well-staffed teams across key functional areas with depth at each level.

While state, local and federal governments are including cybersecurity in programs to reskill workers, and academic institutions are introducing new cybersecurity curriculum and programs, there have been only modest gains in new entrants into the field.[ix]

Consequently, more organizations need to shift their mindset when it comes to recruiting for cybersecurity roles. That starts by acknowledging the need to stop hunting for increasingly rare cybersecurity "All Stars" with decades of experience, advanced knowledge of nearly all security technologies, equally adept at managing a SOC or presenting to the C-Suite, and holding all the most in-demand certifications. These individuals are few and far between. And while they may be great leaders or star performers, they can't play every position all the time.

Organizations need to take it upon themselves to build well-staffed teams across key functional areas with depth at each level. They need to focus on new talent to sustain long-term, self-replenishing teams that will grow more experienced and confident, with junior members ready to advance and take on new challenges for years to come.

Our study provides 10 key insights to help inform organizations' cybersecurity team building strategies.

1. Look Inward – Talent is already within your organization. If you are willing to invest in people without direct cybersecurity experience, why not start by working with people you know and trust, and who already understand your systems, processes and culture? Look for the traits that professionals tell us matter most, including analytical thinking, problem solving, ability to work on a team and creativity. Look for team members who share the same motivating factors as professionals and pursuers. Make cybersecurity career opportunities available to all team members in your organization, especially those looking for advancement. Perhaps create a shadow program for these potential team members to know if the job is a good fit. Cybersecurity leaders may be surprised to discover like-minded individuals across their organization who understand how data moves through the enterprise and who can add value when it comes to developing the policy and controls to help defend it.

2. A Balanced Approach to IT Talent – With 55% of cybersecurity professionals getting their start in IT, it's easy to consider IT departments – even your own – as a source for talent for your cybersecurity team. We know that most pursuers with IT roles are starting to look for their first cybersecurity jobs during their first 3 to 10 years in IT. If these individuals already have made the choice to work in cybersecurity and transition out of IT, make sure they don't leave your organization to work on someone else's team. Be prudent, though. Diversity of experience and mindset will be important when building your team. Pursuers with IT experience tended to focus more on the technical aspects of security and not on policy, risk and compliance, governance and other areas that are equally important to your program's success. IT skill has its place on your team, but diverse perspectives are also critical.

3. Hire for Attitude and Aptitude – When evaluating and recruiting candidates for your cybersecurity positions, look beyond the resume and CV to find people driven by the same motivations as your existing team. Look for critical thinkers, team players and creative individuals passionate about solving problems and finding a role that fits their skills. Like existing professionals, pursuers tend be highly educated. They will learn. They are looking for a cause and a mission, and few professions can help make an immediate impact more than cybersecurity. Work closely with your HR partners and your team to develop the key attributes and skills you need to build a foundation for future success. Make the commitment to take a chance. Invest in finding the right people and make a commitment to their professional development. You'll build team member engagement, foster higher employee satisfaction and reduce attrition – all of which will ultimately strengthen the resilience of your cybersecurity program.

4. Create Realistic Job Descriptions – Discussing best practices for cybersecurity hiring often feels like an endless debate, with the only agreement being universal resentment for "kitchen-sink" job descriptions with unrealistic qualifications, responsibilities and experience requirements. End these practices. Collaborate with HR to clearly articulate expectations and create roles across key functional areas that align with your objectives and ultimately lead to an adequately staffed operation that will deliver on your mission. Think about the types of positions you want to fill and how your recruitment tactics need to adapt to attract the right type of individuals for the right roles. Your cybersecurity team and needs are unique. Invest the time and energy to create the roles and responsibilities you need to accomplish your mission. Resist the urge to ask too much of new hires, especially for entry and early-career roles. Make sure your experience requirements are also aligned with the level of talent you're looking for. Requiring a mid- to senior-level cybersecurity certification for junior roles will only lead to unfilled roles and frustrated under-staffed teams.

5. Invest in Education – A concerted effort is going to be needed to get new entrants up to speed and contributing to your team, and that's just the beginning. Education in cybersecurity is ongoing and career-long. Adopt a comprehensive education strategy that focuses on the best practices and skills necessary for the professional development of your entire team at all career stages. Cybersecurity professionals must keep learning if they are to reach the top levels of their field and effectively perform in today's constantly changing business and technical landscapes. Every organization needs a formal, standards-based cybersecurity education program for the employees responsible for securing their digital assets.[x]

6. Take the Long View – As data suggests, cybersecurity responsibilities will be a new experience for many of today's pursuers. Be patient as your team navigates the onboarding and professional development pathway your organization creates for them. Not everyone is going to pan out. Develop your team-building strategy and have patience to see it through. With breach headlines growing more urgent every day, it's easy to grow restless and want to solve our cybersecurity challenges instantly. However, a measured strategy with investment focused on building the right team is perhaps the most crucial step any organization can make today.

7. Foster Mentorships – Professionals say that having a mentor to shadow and rely on for guidance in their first three years in the field was invaluable for their success. Encourage your senior team members to take on this role of leadership. Listen to what they learn about your team members. How are they doing? Where are they struggling? How can the team or organization adapt its approach to assist? Mentorship is not only an opportunity to help train new entrants to the field, but it is a chance for senior members to take on more responsibility they otherwise may not. You may be surprised how mentorship can instill confidence in both the mentee and the senior team members sharing their knowledge. You may find leaders you didn't know you had on your team.

8. Recognition Builds Confidence – Ensure recognition and encouragement is part of your team building. Professionals say that receiving reassurance they were on the right path was important for their success and gaining confidence that a job in cybersecurity was right for them. This may include recognizing their skill with increasingly challenging projects, promotions or just a casual "good job." Let junior members of the team co-lead or lead important projects when they are ready. Successfully completing those initiatives will help instill additional confidence, fostering an empowered team more willing and able to react as necessary when crisis strikes.

9. Keep the Team Together – Shifting how you recruit for your team can be a significant cultural change for existing team members. It's critical that your senior team members are involved in the process and are active in helping hiring managers and cybersecurity leadership identify the talent you hope to attract. Challenge your team to help champion this effort and assist with identifying the skills and qualities your team needs across all roles. Ensure they understand your efforts are all aimed at providing them with the help they need to do their jobs and effectively defend your assets. Ask your team similar questions to this study and understand what made them successful and emulate that.

10. Embrace Diversity – By looking outside traditional pathways to the cybersecurity profession, organizations will discover a wealth of diverse talent. Diversity in experience, gender, race, nationality, age and more is an asset that forward-looking organizations embrace. Diverse perspectives help generate the bold and innovative ideas necessary to solve the complex security challenges facing global organizations. Work with your HR team to ensure you are attracting and developing a more diverse talent pipeline, accelerating more inclusive and equitable workplace policies and cultures, and supporting full and equal participation in cybersecurity employment at all career levels.

CONCLUSION

There is no near-term solution to the cybersecurity workforce gap on the horizon. There simply aren't enough cybersecurity "All-Stars" available for every organization. Competing for the same limited pool of talent only perpetuates cycles of staff turnover and knowledge drain, which ultimately degrades an organization's ability to respond to cybersecurity incidents. Organizations, hiring managers and cybersecurity leaders need to adopt new strategies that generate sustainable pipelines of talent.

This study provides the insights organizations need to better understand the highly educated and motivated individuals who wish to enter the cybersecurity workforce. Despite its challenges, this is an opportunity for organizations. By focusing on candidates with the skills and motivations that will complement their existing team, cybersecurity leaders who implement a strategy now to build the team they need will foster more resilient organizations in the future.

METHODOLOGY

The Cybersecurity Career Pursuers Study was a blind survey conducted by (ISC)² and Market Cube in December 2020. The total respondent base included 2,034 cybersecurity professionals and cybersecurity jobseekers throughout the U.S. and Canada (1,024 cybersecurity professionals and 1,010 jobseekers pursuing their first cybersecurity role). The margin of error for the descriptive statistics of each group individually, cybersecurity professionals and cybersecurity jobseekers, is plus or minus 3.1% at a 95% confidence level.

*Research Note: Sampling strategies were designed to provide a balance of perspectives across years of experience within the field for cybersecurity professionals, as well as understanding the differences or similarities between pursuers currently in an IT role and pursuers currently not in an IT role. Gender representation within our study, as well as the relative rates of seniority among professionals and pursuers with or without IT roles are not intended to be reflective of the U.S. population as a whole. These findings provide insights into the opinions and motivations of those currently in the field and those choosing to pursue a cybersecurity career.

About (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, more than 150,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for The Center for Cyber Safety and Education™. For more information on (ISC)², visit www.isc2.org, follow us on Twitter or connect with us on Facebook and LinkedIn.

[i] *The 2020 (ISC)² Cybersecurity Perception Study*, (ISC)² Research, 2020
[ii] *Companies Urged to Adjust Hiring Requirements for Cyber Jobs*, The Wall Street Journal, Nov. 30, 2020
[iii] *Building a Resilient Cybersecurity Culture*, (ISC)² Research, 2019
[iv] *Hiring and Retaining Top Cybersecurity Talent*, (ISC)² Research, 2018
[v] *2020 IT Skills and Salary Report*, Global Knowledge, 2020
[vi] *EMPLOYMENT FOR SECURITY ANALYSTS TO GROW 31% BY 2029*, (ISC)² Blog
[vii] *The 2020 (ISC)² Cybersecurity Perception Study*, (ISC)² Research, 2020
[viii] *The 2020 Cybersecurity Workforce Study*, (ISC)² Research, 2020
[ix] *The State of Cybersecurity Hiring: Recruiting Watchers for the Virtual Walls*, Burning Glass Technologies, 2019
[x] *The Enterprise Guide to Establishing a Cybersecurity Training Program*, (ISC)², 2020