EVOLVE SECURITY

2021 EVOLVE SECURITY
CYBERSECURITY SKILLS REPORT:

STATE OF THE CYBERSECURITY WORKFORCE

TABLE OF CONTENTS

INTRODUCTION

The cybersecurity industry is projected to triple year-over-year through 2022, yet the workforce shortage still stands at millions worldwide. Given a 141% increase (2019-2020) in the total number of records compromised in a single year – now over 37 billion within 3,932 publicly reported data breaches in 2020– employing more cybersecurity professionals is a never-ending challenge.

We are all familiar with the talent shortfall in cybersecurity:

There are nearly 465,000 job openings nationally with 3.1 million unfilled cybersecurity positions around the world. According to the 2020 (ISC)² Cybersecurity Workforce Study, "… the global cybersecurity workforce needs to grow 89% to effectively defend organizations' critical assets."

And while the workforce gap is slowly narrowing, there's active discussion about whether job requirements for both entry-level hires and experienced professionals are too excessive or out of touch.

This is the starting point for Evolve Security's first Cybersecurity Skills Report: State of the Cybersecurity Workforce. We aimed to name the gap, shed light on the market supply and demand, and specifically call out the technical skills hiring managers cannot find. Overall, we wanted to identify growth opportunities for both current and future cybersecurity professionals. We surveyed the entire cybersecurity ecosystem, from cybersecurity executives to c-suite directors, hiring managers, and cybersecurity professionals across the spectrum to get an inside-out look at the current state of the workforce.

Evolve Security's Cybersecurity Skills Report was designed to:

Gain insights into real-time cybersecurity hiring needs straight from industry leaders

Identify specific talent gaps and opportunities to close the cybersecurity workforce shortage

Baseline the top skills that exist on cyber teams today and identify the domains where pros are upskilling

More precisely:

1. **What are the areas of expertise execs most value now,** and do the current skills of the pros match up?
2. **Where are the pros focusing** their training goals and are they upskilling in the right direction?
3. Facing a talent gap, do execs prefer to **train in-house or look in the marketplace?**
4. **Where are the opportunities** for future training and jobs?
5. Finally, **do certifications matter** as much as we think, and which ones helped the pros land a job?

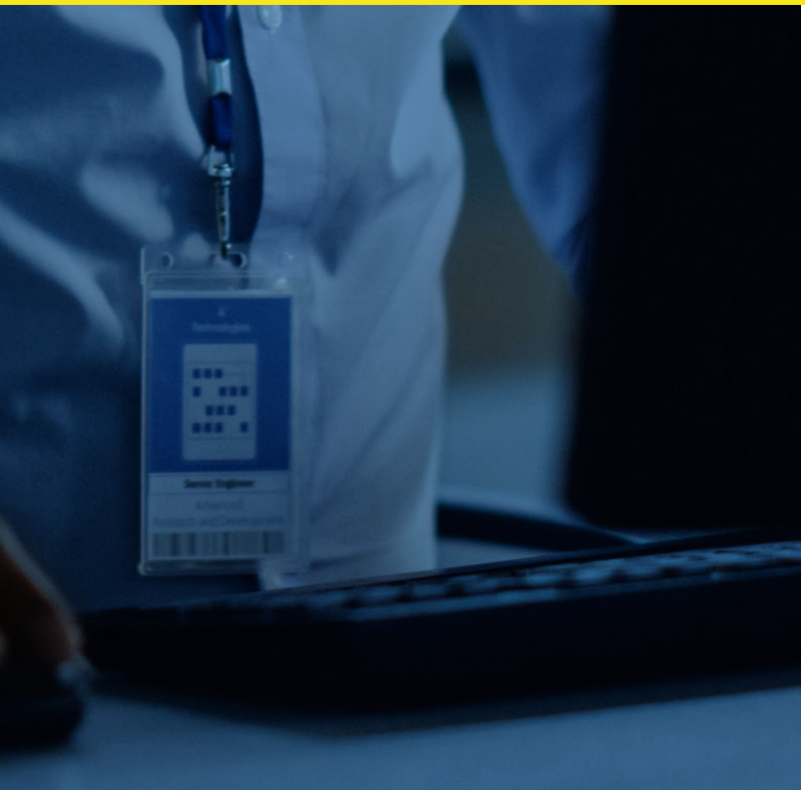
If you are a CISO asking why it is so hard to hire, our findings will help you see how talent might be more apparent than you think. If you are a cloud-savvy app developer with sharp network security skills contemplating your next step use this report to target your next specialization. Finally, if you are a sector-switcher with great analytical and communication skills wondering if cybersecurity is right for you, read on to learn more about in-demand points of entry into the field.

This report is for all of you. Stay tuned.

ABOUT EVOLVE SECURITY

Evolve Security is a full-scale technical services firm dedicated to the human element of cybersecurity, helping businesses improve their security posture where they are most vulnerable. We provide expertise in enterprise services, staffing augmentation, cybersecurity advising, and training through our top ranked Evolve Security Academy Bootcamps. Our leadership has been in the information security industry for over two decades. Our application penetration testers are current or former software developers, and our instructors are hackers with a teacher's heart, uniquely qualified to create custom training programs for your company and employees. We understand value comes from long-term partnerships over short-term, high-costs engagements.

For more information you can find us at
www.evolvesecurity.com



AT-A-GLANCE: SURVEY HIGHLIGHTS

This first *Evolve Security Cybersecurity Skills Report*: State of the Cybersecurity Workforce serves as a playbook with specific goals related to the cybersecurity skills gap:

To help cybersecurity executives (execs) take stock of the skills that are most prevalent in the current cybersecurity workforce

To help cybersecurity professionals (pros) quickly assess what the marketplace currently values, where the jobs are headed, and answer questions about what training or certification to consider next.

KEY TAKE-AWAYS:

1. CLOUD SECURITY REMAINS ON TOP.

83% of execs named Cloud Security as the most valued skill on their teams. The good news is that Cloud Security also ranks in the top three skill sets for current pros and where nearly 50% of the pros are upskilling. However, our survey revealed a noticeable gap in the cloud skills that are critical to landing a job. While the pros are actively pursuing AWS and Azure skills, hiring managers report Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Cloud Access Security Broker (CASB) Technology as well as Cloud Security Audit skills as the most difficult to find. An even closer look at training trends showed that **while 36% of pros are actively pursuing AWS certifications, AWS only represented 12% of all Cloud hires.** While Azure edged out AWS in hiring needs, neither ranked in the top five sought after skills. Overall, the hardest-to-find skills for the execs are platform independent, indicating the importance of competency in the basics of Cloud architecture.

of execs named Cloud Security as the most valued skill on their teams.

of execs reported GRC as a sought-after skill

2. GOVERNANCE, RISK AND COMPLIANCE (GRC) PRESENTS THE LARGEST SKILLS GAP.

75% of execs reported GRC as a sought-after skill, while 48% of pros said they currently possess GRC skills. In contrast to the value the execs place on GRC skills, only 23% of the pros said they were actively upskilling in GRC, with 25% planning on training within the next 6 months. **GRC represents the biggest training opportunity for current pros and those looking to enter the field.**

3. SECURITY FUNDAMENTALS ARE STILL GOLD.

There was close alignment between the technical skills organizations most reported needing, and the foundational skills the pros reported having, or intending to get. Networking & Data Communications, Understanding Data Architecture and Operations, Programming Languages, and Multi-platform Cybersecurity Controls topped both the execs and pros lists, confirming the critical nature of these core technical skills. This reaffirms a common mantra from practitioners:

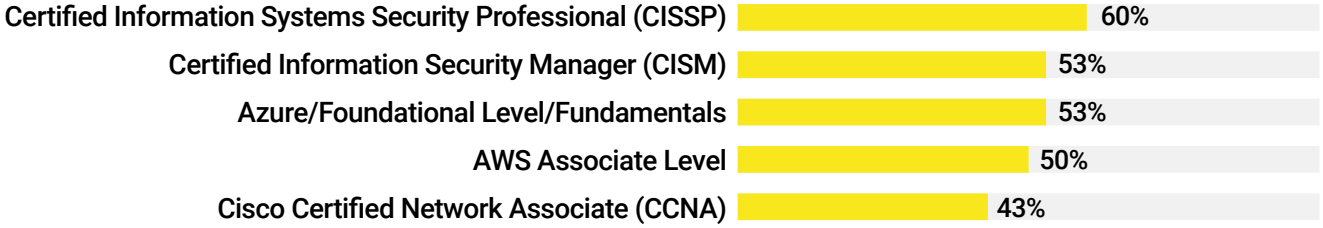
If you want to secure something, you need to know how it works.

4. ANALYTICAL AND COMMUNICATION SKILLS ARE ALSO CYBER SKILLS.

Cyber Risk Management, Audit and Change Management as well as knowledge of cybersecurity frameworks and the U.S. regulatory environment topped the "most-needed" and "hard-to-find" skill sets. Execs and pros equally highlighted the need for effective presentation skills and the ability to translate technical speak into plain language, critical for both clients and boards.

5. CERTIFICATIONS OPEN DOORS.

According to hiring managers, the top most valued certifications are the Certified Information Systems Security Professional (CISSP, 60%), Certified Information Security Manager (CISM, 53%), Azure Foundational Level/ Fundamentals (53%), AWS Associate Level (50%), and Cisco Certified Network Associate (CCNA, 43%). In general, 75% of cybersecurity leaders encourage certifications and prefer hiring people who have them. At the same time, demonstrated ability to apply skills on the job is critical. 73% of the pros highly valued the CISSP.



6. PROS WANT TO DO IT ALL BUT CONSIDER SPECIALIZATION TO KEEP PACE.

The value of eight major cybersecurity skills does not vary much among pros. Most pros either currently have or intend to upskill in the following areas: Security Engineering (66%), Cloud Security, Application Security and Pentesting, (all 54%). This tells us the cybersecurity skills gap is more nuanced, composed of a range of potentially overlooked and over-valued technical skills with an increasing need for a mix of soft skills.

The take-away? **Consider targeted training in cross-disciplinary skills such as GRC, Cloud Security Audit, Vendor Risk Management to stay on top of trends and internal controls valuable in the evolving threat landscape.**

Top skills currently possessed:

- **Security Engineering**

- **Cloud Security**
- **Application Security**
- **Pentesting**

7. EXECS ARE WILLING TO TRAIN, AND PRACTITIONERS WANT TO LEARN.

Over 46% of the execs reported "definitely or probably" willing to support training in-house and another 58% preferred external training. 76% of the pros are very willing to update their skills and pursue certifications for their current position versus to prepare for a job change - they just need to know the skills their execs need.

8. EXECS NEED TO SHARE THEIR GAPS AND BUILD A TRAINING CULTURE.

50% of execs confirmed if they cannot find the right fit for a role, they are "definitely willing" to keep looking, acknowledging the difficulty of on-the-job training and a preference to hire those who can hit the ground running in high-paced roles. But the more organizations do the work upfront to build a culture of continuous upskilling and communicate hiring needs to their teams, the closer we will be to closing the gap.

50%

of execs confirmed, they are "Definitely Willing" to keep looking

Survey Methodology: Who & What We Asked

Evolve Security's first *Cybersecurity Skills Survey: State of the Cyber Workforce* report was designed for an inside-out investigation into the cybersecurity talent gap. The survey aimed to baseline the top skill sets of active pros against the current hiring needs of industry leaders and managers. Second, it assessed if the pros are targeting their training in the areas where organizations need them most. Data from the survey can be used to identify current and future trends in the cybersecurity workforce and provide a roadmap for professionals to determine future training skills.

Who we asked:

Professionals from every level of the cybersecurity workforce ecosystem responded to the survey, providing comprehensive insight into the workforce skills gap. Evolve Security collected survey data from over 35 job categories across two key profiles in the cyber ecosystem:

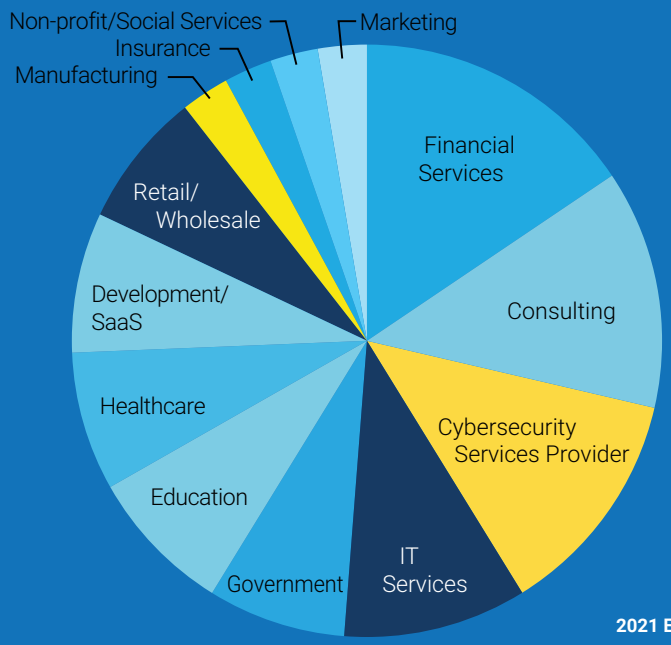
Cybersecurity Executives:

The c-suite: chief operating officers, chief information security officers, vice presidents of information technology, as well as cybersecurity directors and hiring managers

Cybersecurity Professionals:

Practitioners on the front lines: security architects, engineers and operators, consultants, penetration testers, analysts, and developers, and all actively working in the field.

Survey respondents by industry



Top industries reporting:

Cybersecurity Executives:
Financial Services, Consulting, Cybersecurity Service Providers

Cybersecurity Professionals:
IT Services, Cybersecurity Service Providers, Government

What was asked

We asked the following questions to better define the skills gap, baseline where the industry is today, compare the perceived value of skills, identify hiring and training trends, and assess the role of certifications in hiring requirements:

For the Cybersecurity Professionals

What is your current cybersecurity skill set?

Based on the selected skills possessed, rate the importance of each one..

What cybersecurity skills are you actively improving?

Tell us about the skills you are pursuing in the next six months?

What certifications do you have/are pursuing?

For the Cybersecurity Executives

What are the skills of the pros you hired in the last year?

When hiring what skills have you been unable to find?

If you cannot find someone for a role, did you train internally, externally, encourage certification, or continue searching?

What certifications does your organization value?

DEFINING THE GAP:

The Cyber Skills survey simultaneously polled execs and current pros to identify and name different categories of cyber skills gaps. Across some skills you will see alignment, where the market supply/demand appears to be in sync — for now. For others, we identified different types of gaps. We found a potential oversaturation of skills in the workforce, where the pros are actively or planning on training within the next six months and the hiring managers can already find what they need. These skills are highlighted under “proceed strategically” If you are entry-level, there is a lot of representation in these fields already and not a significant skills gap. In addition, a skills gap can represent opportunity for the pros to target training and find jobs.

Survey Limitations:

CYBERSECURITY TOOLS:

This skills survey was intentionally limited to capture high-level skill sets rather than individual cybersecurity tools across penetration testing, network defense, web scanning, encryption, networking monitoring and network intrusion detection.

QUALITATIVE SKILLS:

We acknowledge the inherent and increasing value of more qualitative, soft skills in cybersecurity (communication, analytical thinking, problem solving, empathy, emotional intelligence). However, this first this first survey concentrated primarily on the technical skill sets and certifications identified in cybersecurity job descriptions. Future surveys will aim to take a deeper dive into the value of soft skills across the cybersecurity ecosystem.

BREAKING DOWN THE GAP: CYBERSECURITY EXECUTIVES V. PROFESSIONALS

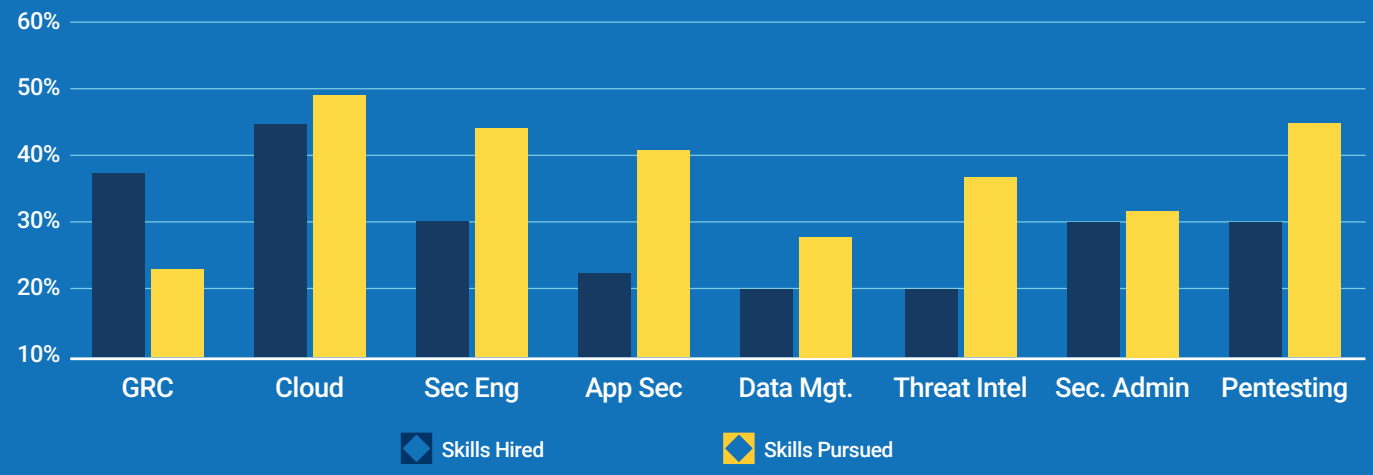
The Evolve Security Cybersecurity Skills Report: *State of the Cybersecurity Workforce Survey* aimed to better define the cybersecurity skills gap we hear so much about. Below you will see some over-arching cybersecurity skill domains as well as individual, cross-cutting competencies where we identified high alignment.. This means the market supply/demand appears to be in sync... for now. For other cyber skills, we identified different types of gaps. One potential gap is an oversaturation of skills in the workforce, where the pros are actively and/or planning on training within the next six months and the hiring managers can already find what they need. You will see these skills highlighted under "proceed strategically" particularly if you are entry-level, as there is a lot of representation in these fields already. Most critically, there is a gap related to an under-representation of skills: high demand from the execs and pros. Naming the gap represents a great opportunity for both seasoned experts and entry-level practitioners to upskill and find jobs, as well as widen the tent for opportunities in the cybersecurity field.

THE CYBER SKILLS ALIGNMENT

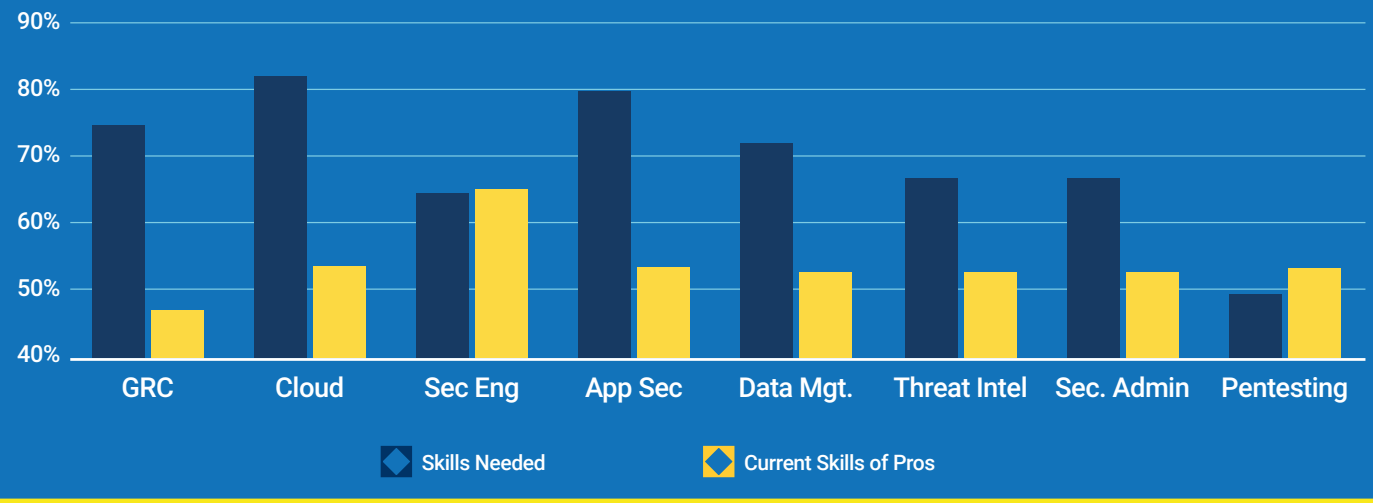
In the 2020-2021 hiring cycle, Evolve Security's Cybersecurity skills survey identified some natural alignment where market forces are in sync, at least for now. This represents where execs are hiring, and the skills possessed by current pros match up. For example, **execs and hiring managers were focused on filling vacancies in Cloud Security (45%); Governance, Risk, and Compliance (38%) and Security Engineering, Security Administration, and Penetration Testing (all 30%).** Application Security also ranked as a highly valued skill. In the same reporting time frame, the top three skills possessed by the pros were Security Engineering (66%), Penetration Testing, Application Security and Cloud Security (all 54%). The pros also reported upskilling in Cloud Security (49%), Penetration Testing (45%), Security Engineering (44%).

Additionally, there are cyber skills that uniquely hold high value across organizations and are also where the pros either have baseline skills or are actively improving their toolkit.

Skills execs hired vs Skills pros are actively pursuing



Skills execs need vs Current skill set of pros



CLOUD SECURITY:

The execs were clear: 83% of the C-Suite and Hiring Managers chose Cloud Security as a skill that is crucial to their organization. Cloud Security also ranks in the top three skill sets possessed by current pros and where nearly 50% of the pros are upskilling both now and in the next 6 months. While there were slightly more Cloud pros versus Cloud jobs, there is high alignment on overall skill importance. Cloud is a highly nuanced discipline in terms of identifying the exact skills gap, you will see it discussed in all three areas of this report.

APPLICATION SECURITY:

Approximately four out of five applications tested have at least one security flaw. While not all result in a significant risk, this data point reinforces the survey results identifying a strong alignment between the execs and pros on the value of Application Security in cybersecurity teams. Take a look at the chart below, there is high association between the roles hired, where the pros are training, as well as the Application Security roles that execs are desperate to fill. See the information below on how application and cloud security pair well together as a group of in-demand skills

Skills Hired		Skills Difficult to Find		Where the Pros are Actively Training	
Cloud IaaS/PaaS/ SaaS/CASB	21%	OWASP Secure Coding	27%	Vulnerability/Threat Research	21%
OWASP Secure Coding	21%	Programming Languages	20%	Programming Languages	21%
REST API Design, Development, and Testing	21%	REST API Design, Development, and Testing	20%	Secure DevOps	21%
Vulnerability/Threat Research	21%	Emerging Technologies/ Attack Vectors	20%	OWASP Secure Coding	21%
Multi-platform cybersecurity controls	16%	Networking and Data Communications	13%	Cloud IaaS/PaaS/ SaaS/CASB	16%

DATA MANAGEMENT:

While there was less hiring in Data Management over the survey period, 83% of the execs and 71% of pros value the skill as crucial or important, a nod that data management and security is at the core of every strong cybersecurity program to maintain the confidentiality, integrity, and availability of data aligned to an organization's risk strategy.

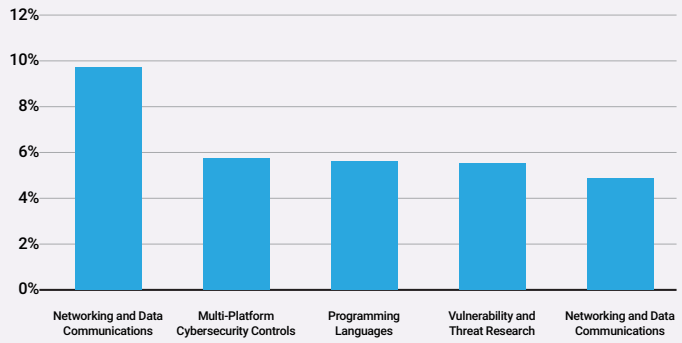
SECURITY ADMINISTRATION:

89% of all execs and 72% of the pros named Security Administration as the most valued skill in cybersecurity. Where we saw a gap was in the amount of jobs hired with security administration as their primary role. The data tell us that this will remain a top priority skill set, but there are not as many open roles in this domain as in some of the others we surveyed.

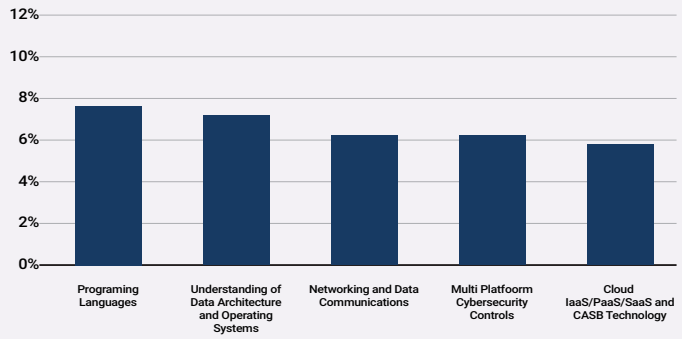
FOUNDATIONAL SKILLS:

Core, technical skills are consistently valued by execs and pros. The top five skills execs and pros need for their organizations are also the domains where the pros either most highly identify as their core skill set or have training goals to further upskill. Networking and Data Communications, Understanding Data Architecture and Operating Systems, Multi-Platform Cybersecurity Controls, Programming Languages, and Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Cloud Access Security Broker (CASB) Technology continue to carry intrinsic value. The ranking is near-equal except for the pros potentially over-valuing Programming Languages as a top skill compared to their hiring managers. **From understanding secure network architecture to discovering software vulnerabilities and detecting malicious code, these skills are important to every pro.** While the industry is never static, the execs and pros agree it's hard to protect something one does not inherently understand. The good news is that upskilling is always available, and you don't have to be 100% technical to be successful: **If you're an Exec, leverage this values alignment to support continuous training. If you're a pro, use this report to navigate the gaps and round out your skills. And if you are a newbie with technical aptitude, figure out the best training plan for you.**

Skills most important to execs



Skills the pros are planning on improving

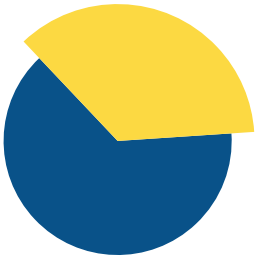


THE CYBER SKILLS GAP

While a skills alignment exists, so does a cybersecurity skills gap, and it's more nuanced than we think, composed of a range of potentially both over and under-valued technical skill sets with an increasing need for specialization, and a mix of necessary soft skills to support the business. The following skills were identified as either over-valued by pros or at a current market saturation. What's the best advice? If you are currently looking for jobs in these areas, proceed, but with a well-defined search strategy and targeted training in mind:

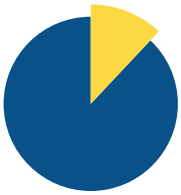
CLOUD SECURITY:

There is an apparent gap in what cloud skills are critical to landing a job. While the pros are actively pursuing AWS and Azure skills, hiring managers report Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Cloud Access Security Broker (CASB) Technology as well as Cloud Security audit skills as the most difficult to find. An even closer look at training trends showed that while 36% of pros are actively pursuing AWS certifications, AWS only represented 12% of all Cloud hires. While Azure edged out AWS in hiring needs, neither ranked in the top 5 skills sought after by the C-Suite. **The data reveal that the execs are more interested in the skills required to be effective on the Cloud than the certificate earned, but given the option, they will lean toward Azure as a preference.** Pros, on the other hand, overvalue AWS compared to Azure. The hardest-to-find skills for the execs are platform independent, indicating the importance of competency in the basics of Cloud architecture over specialization.



36%
of pros are actively pursuing AWS certifications

only 12%
are AWS Cloud hires

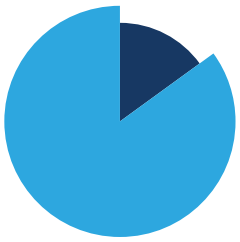


SECURITY ENGINEERING:

While valuable; with 66% of the pros reporting having this skill, and 44% actively improving it across the board, fewer execs and hiring managers reported hiring security engineers in the 2020-2021 period. Potential reasons for this trend can be that security engineering is an established core discipline and a skill many well-established and experienced pros possess. **Consider security engineering as a valuable steppingstone for practitioners to know, but not necessarily a high-growth area in the current job market, particularly if you are an entry-level candidate.**

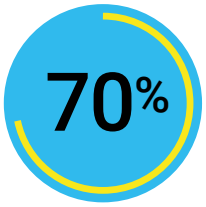
PENETRATION TESTING:

While 85% of execs continue to value pentesting as organization-critical, a 15% jobs gap was identified between where the pros were upskilling (45%) and jobs available (30%). Pentesting likely represents an area of cyber expertise the C-Suite finds important but is most willing to outsource, valuing an independent, third-party review with neutral parties preparing the results of their reports.



85%

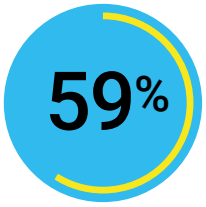
of execs continue to value pentesting as organization-critical



of pros called out Threat Intelligence as a highly valuable skill

CYBER THREAT INTELLIGENCE:

70% of pros called out Threat Intelligence as a highly valuable skill versus 59% of execs. Similarly, 25% of the pros reported actively training in Vulnerability and Threat Intelligence for Application Security, yet it did not rank in the skill sets the C-Suite reported as most difficult to find. Why? **Like Penetration Testing, Threat Intelligence may also represent an area of expertise execs are most willing to outsource**, recognizing the limitations of intelligence-sharing, and a desire to relieve some pressure on in-house cybersecurity teams to focus on day-to-day operations.



of execs called out Threat Intelligence as a highly valuable skill

THE CYBERSKILLS OPPORTUNITY

Are you an experienced Cybersecurity Professional considering your next step or a sector-switcher looking to enter the field? Look no further, here is the cybersecurity skills opportunity gap. These are the domains where execs are looking to hire and where there is an under-representation of pros. Some skills are great for the cybersecurity experts looking to pivot and others are accessible for those starting out in the field. Read on to learn what skills are best enter and grow in the industry!

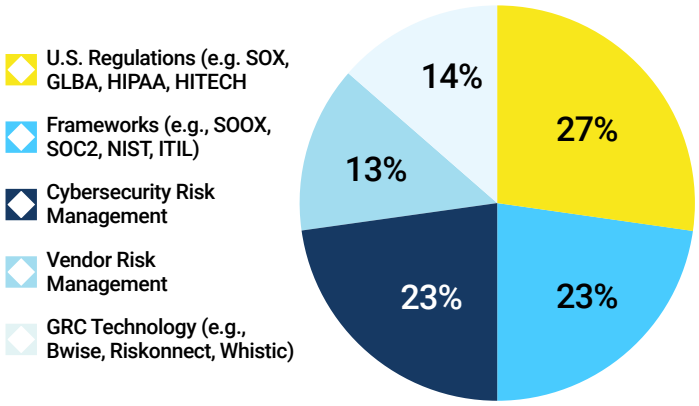
For the execs looking to hire in these domains, consider assessing your teams and get acquainted with their training plans. In turn, share your hiring plans to incentive and normalize seamless training opportunities to reduce the need for external recruiting. When given the option, pros prefer to upskill for their current role.

GOVERNANCE, RISK AND COMPLIANCE (GRC):

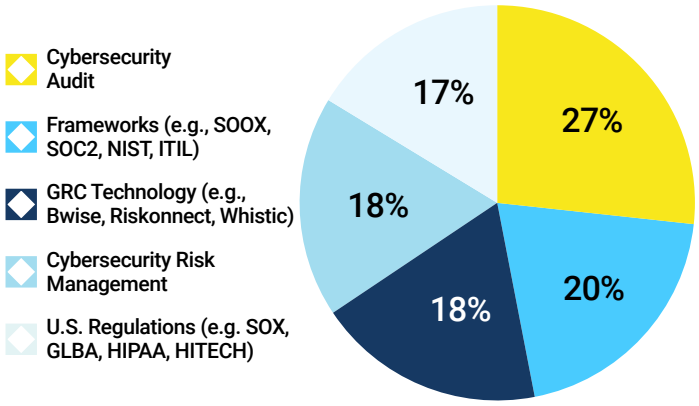
GRC skills: 65% of Cyber Executives ranked GRC as "Critical or Very Important" versus only 34% of the pros. **While 38% of hiring was in the GRC space, only 23% of Cybersecurity pros are currently improving in this domain.** Fortunately, 25% of pros said they were planning on upskilling in GRC within the next 6 months. The demand for GRC skills presents a great opportunity for both current pros as well as those looking to enter the cybersecurity field.

Specifically, those who did accept a GRC role in 2020-2021 had skills in Cybersecurity Risk Management, Cybersecurity Audit, Change Management, cybersecurity frameworks and U.S. Regulations. Additionally, an opportunity gap exists where the pros are starting to recognize GRC as a growth field and upskilling in the right direction. There is consistency among pros to target U.S. Regulations compliance training including the Sarbanes-Oxley (SOX) Act, Gramm-Leach-Bliley Act (GLBA), Health Information Privacy Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) as well as the skills to implement cybersecurity frameworks. These are domains where execs can't seem to fill all the available jobs. In the wake of SolarWinds hack we not surprisingly identified Vendor Risk Management as a growing field in GRC, although not currently on the pros radar. A recent SecureLink/Ponemon Institute report revealed not only a lack of comprehensive inventory for third-party vendors, but also limited visibility into third-party access and permissions, limited third-party monitoring,

GRC skills execs couldn't find



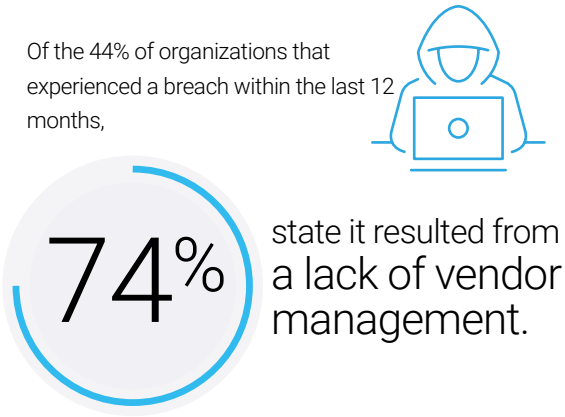
GRC skills pros are actively improving



and no centralized control: Of the 44% of organizations that experienced a breach within the last 12 months, 74% state it resulted from a lack of vendor risk management.

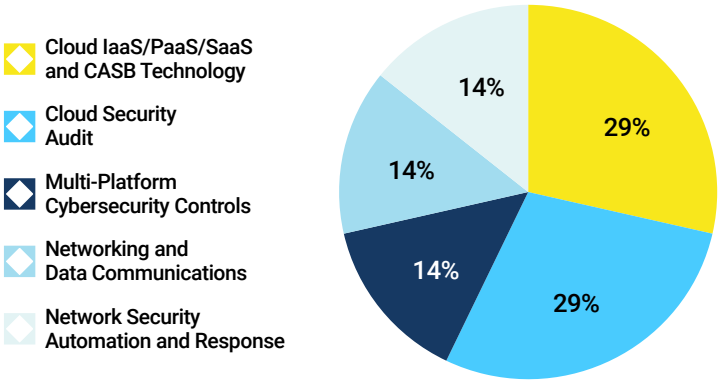
The Take-Away? If you're a Pro and think GRC is only for the policy people, think again, Vendor Risk Management needs more experts to combat the threat and you'll only add more value as a practitioner. Looking to pivot into cybersecurity? Knowledge of cybersecurity frameworks, U.S. Regulations and Cybersecurity Risk Management is a great place to start, and one of the more accessible areas for certifications.

Of the 44% of organizations that experienced a breach within the last 12 months,



state it resulted from a lack of vendor risk management.

Top 5 Cloud Computing Security Skills Execs Couldn't Find

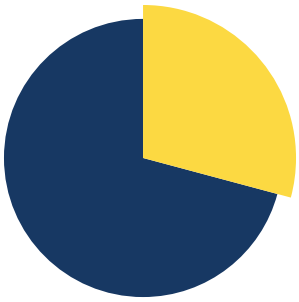


CLOUD SECURITY:

Cloud is a highly nuanced discipline in terms of pinpointing the exact skills gap, but vulnerabilities are increasing, creating plenty of growth opportunities for Cybersecurity Professionals, provided they target the right skills. While we previously discussed the over-valuation of AWS and Azure certifications, there are still great opportunities for professional growth in Cloud. According to the 2021 Verizon Data Breach Investigations Report, compromises on the Cloud are more common than on-premises assets. Breaches are increasingly focused on social and web application vectors, using compromised credentials against Cloud-based systems. Specifically consider:

CLOUD SECURITY AUDIT:

Cloud Audit presents a growing skill, capturing 22% of all Cloud skills hired and 29% of "most difficult to find" roles. At the same time, only 16% of the pros reported actively pursuing, and 17% planning on pursuing Cloud Security Audit training in the next few months. As the Cloud industry grows, a natural outcome is a simultaneous demand for security audits, particularly to manage access control.

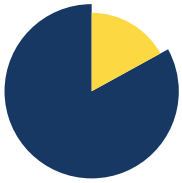


29%

of execs state Cloud Audit as a difficult to find skill

only 17%

of pros plan improving this area



> Everything seems to be migrating to the cloud… Cloud certification will become more important in the near future."

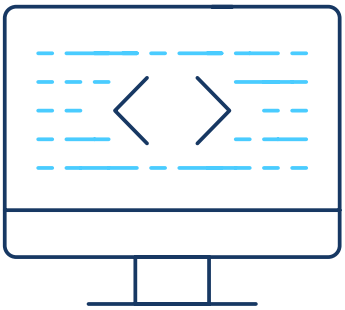
Technical Consultant,
Cybersecurity Services Provider

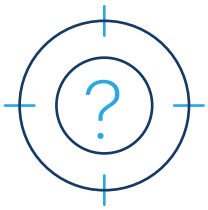
CLOUD IAAS/PAAS/SAAS AND CASB TECHNOLOGY:

The global Cloud market has increased by orders of magnitude in response to the rapid restructuring of business operation in the wake of COVID-19. 52% of organizations today use a form of IaaS, and security teams need to support these platforms. According to Gartner, "*…IaaS will see the highest growth in 2021 as CIOs face continued pressures to scale infrastructure that supports moving complex workloads to the Cloud and the demands of a hybrid workforce.*" In addition, the PaaS market is expected to grow 14.4% to $54.09 billion this year. Despite the fact that pros either reported having skills in this domain, currently upskilling or have active training plans (16%, 12% and 14%, respectively,) 29% of hiring managers reported a skills gap, unable to find the talent necessary to support the exponential growth of the cloud services market.

APPLICATION SECURITY:

Given the increasing number of organizations developing in-house applications, protecting their confidentiality, integrity and availability is more critical than ever for execs and Professionals to manage vulnerabilities and minimize risk. Like Penetration Testing (see below) the skills gap here is potentially more of a communication issue than an actual talent gap: For execs, tell your team what you need, the aptitude is there. For the Professionals, talk to your leadership, train with intention, and use this report as a guide: Currently If you are into Programming Languages or Open Web Application Security Project (OWASP) Secure Coding, keep at it. If you're looking for something new, consider REST API (RESTful API) Architecture Design, Development and Testing which did not rank in the actively pursuing or looking to pursue in the next 6 months for the pros. Programming Languages are always valuable, keep at it to raise the bar.



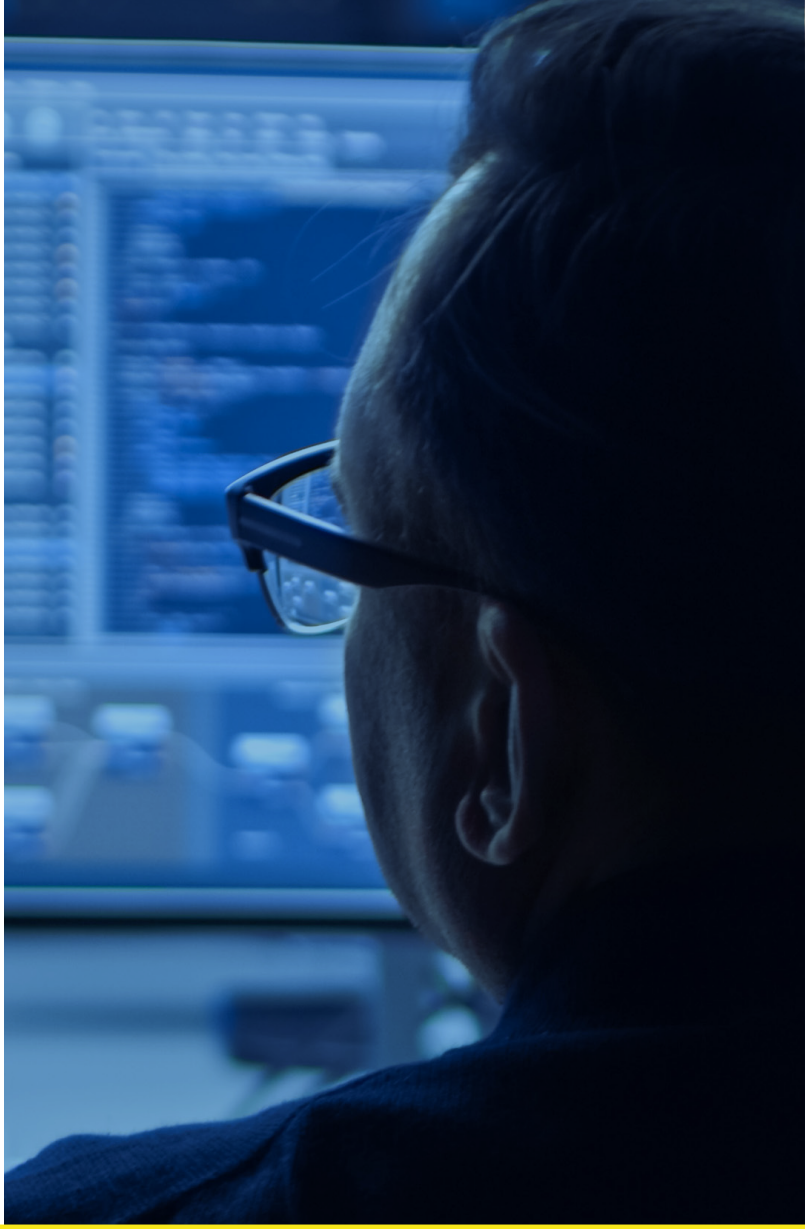


Hiring Managers said they could not find specific skills in Assessment Reporting

another **22%** **reported experience with Exploitation Tools as difficult to find.**

PENETRATION TESTING

While 85% of execs identified Pentesting as a "Critical" or "Very Important" skill, there was a reported 15% gap between where pros are upskilling and actual hiring for those jobs by execs. What does this mean? There is always room to specialize: **22% of execs and Hiring Managers said they could not find specific skills in Assessment Reporting;** another 22% reported experience with Exploitation Tools as difficult to find. The pros, in turn, did not rank either of these skills in their current or future training plans.



Filling the Gap: These Skills Will Get You Hired

Hiring gaps in governance, risk and compliance, cloud security, application security and penetration testing are excellent opportunities for execs and pros to better communicate their talent gaps and training plans. What might be perceived as a workforce gap could be remediated with better communication, planning and seamless training opportunities. See below for the top-ranked and most needed skill set in each domain.

THE CYBERSKILLS OPPORTUNITY

GRC

Vendor Risk Management

Change Management

U.S. Regulations (SOX, GLBA, HIPAA, HITECH)

Cybersecurity Frameworks (SOX, SOC2, NIST, ITIL)

Cybersecurity Risk Management

CLOUD SECURITY

IaaS/PaaS & CASB Technology

Cloud Security Audit

Multi-platform Cybersecurity Controls

Network Security Automation and Response

APPLICATION SECURITY

Emerging Technology and Attack Vectors

Networking and Data Communications

OWASP Secure Coding Practices

REST API Design, Development and Testing

Programming Languages

PENTESTING

Exploitation Tools

Understanding Data Architecture & Operating Systems

Assessment Reporting

Programming Languages

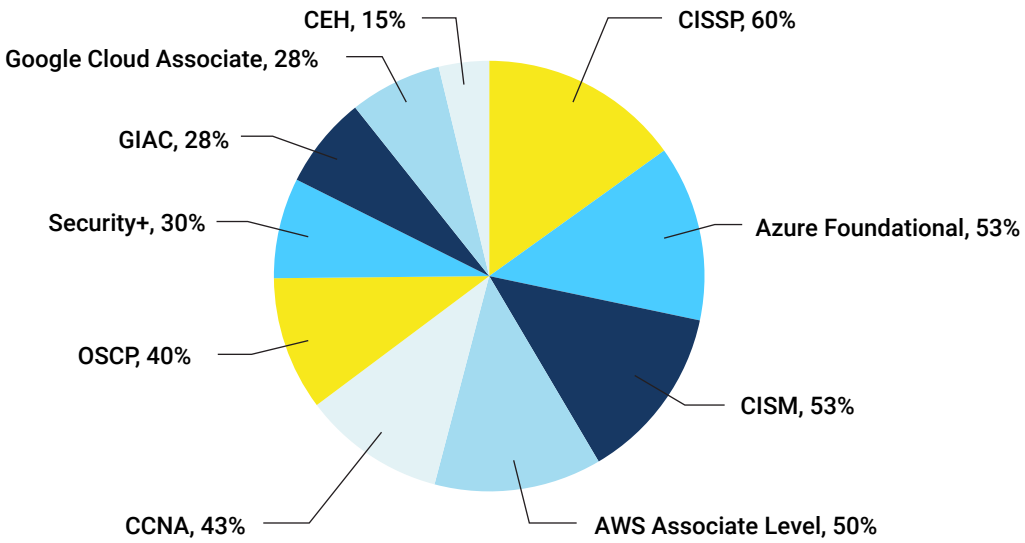
Vulnerability and Threat Research

GRC is a great point of entry for new Cyber pros!

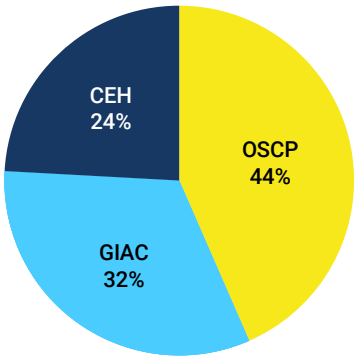
CERTIFICATION FINDINGS

Weather a seasoned pro or looking for a jump-start into the field, the Cybersecurity Skills Survey revealed certifications matter: 75% of Cybersecurity leaders overall encourage certifications to help get you in the door, although showing your skills on the job is most critical. If you're a Professional, take a close look below and see what would round out your toolkit; If you're a looking to enter the field, the Security+ is an accessible starting point.

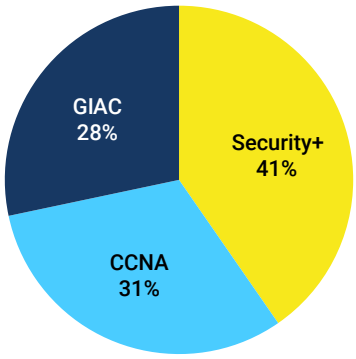
A View from the Execs: Top 10 Most Valued Certifications



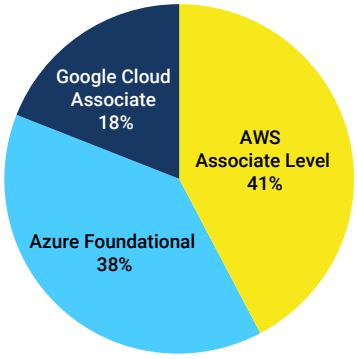
Top 3 Offensive Security Certifications



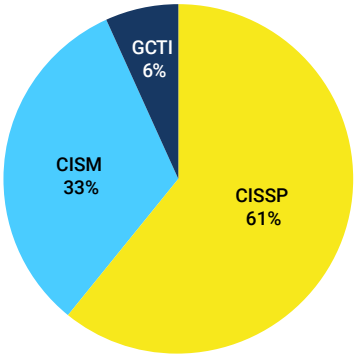
Top 3 Networking Certifications



Top 3 Cloud Certifications



Top 3 Security Management Certifications



RE-THINKING THE GAP, PART 1:

RECOMMENDATIONS FOR CYBERSECURITY EXECUTIVES

Learn insight into the strategies that executives, directors, and hiring managers can use to quickly close talent gaps and fill critical roles with qualified individuals. You can narrow the gap significantly using the tools and training. Even small investments can reap big rewards.

1. Don't look for unicorns. Your pros do not need to be superhuman, only passionate about what they do and willing to learn and grow with your organization. The pros are also hard-working and know the industry moves quickly: over 90% of our survey respondents reported they are actively working on improving their cybersecurity skills.

2. Keep communication channels open. Look to your team first for your next hire. Survey your pros regularly to know where they are training and where they want to go and carve out professional development pathways to get them there.

3. Hire what you cannot teach. Identify candidates with a growth mindset. Hire for core skills and train for the rest. Only 42% of the Cybersecurity pros reported they are upskilling to change jobs, while 72% do so for certification and 61% are doing it to be better at their current position. Leverage their aptitude and curiosity.

4. Invest in your bench. Save your onboarding costs and look to your team for your next "hard to fill" hire: You likely have diamonds in your own backyard, already on payroll, familiar with your organizational culture and appreciative of advancement opportunities. The investment will pay itself back with practitioners who plan their training in direct alignment with your business objectives.

5. Flex your organizational muscles. Professionalize mentorship for your pros. Find ways to sandbox and allow for mistakes. Not simple, but you will foster a strong internal training culture the practitioners love. Remember, you started out as a Pro once, too.

RE-THINKING THE GAP, PART 2:

NOTES FOR CURRENT AND FUTURE CYBERSECURITY PROFESSIONALS

Whether you are a seasoned veteran or a freshly minted professional, getting an edge is crucial to landing that next, or even first big role for your career. With the variety of training and skills to pursue available, making that decision can be challenging. Check out the top skills identified to focus your efforts and consider when deciding what to training to take on next.

1. Your managers value you. Share your goals; they are willing to support on-the-job training. 50% reported being willing to support upskilling in-house as well as another 75% preferring to outsource training off-site. Another 75% are willing to encourage certification and will value the effort.

2. Be strategic with your next training. When considering something new, think creatively and be deliberate about the best way to round out your skills. Do you have the foundational elements down? Could you be that unicorn if you upskilled in GRC or felt more confident leading change? Use this report to figure out your next best step.

3. Embrace the soft skills. Roles are fluid these days, especially if you are client-facing or targeting senior management. Do you prefer staying behind the monitor or in a SOC? Consider stretching out of your comfort zone, and don't be afraid to bring different thinking to your team. Cybersecurity supports the business so people who can communicate with a diverse set of stakeholders are needed. Overwhelmingly, the Professionals surveyed acknowledged the need for communication and presentation skills and the ability to translate tech when speaking with clients. Leadership sees the value as well.

4. If you are a Pro, specialize; If you're a newbie, start where you can grow: For those who have been in the field for some time, be really good at what you do, and target training based on industry demand. For example, if you're a pentester, be a darn good one and train up on the latest Exploitation Tools or Assessment Reporting – that's where the execs are looking to hire. And if you're just getting started in the field, consider GRC as a great on-ramp into the cyber field, especially if you are coming from another industry.

5. Keep communication channels open. Tell your manager where you're interested in taking your cyber career and where you want to upskill next. There might be more alignment than you think. Over half of Executive respondents report they are willing to train either internally or externally, and three-quarters will encourage certification.

CLOSING THE GAP: THOUGHTS FOR THE FUTURE CYBER WORKFORCE

Cybersecurity staff shortages are no doubt putting organizations at risk. COVID-19 and the rapid shift to remote work added more dimensions of pressures, forcing pros to adapt and upskill quickly. And despite economic uncertainty, 48% of organizations plan to increase cybersecurity staffing over the next 12 months, consistent with hiring plans from previous years.

On one hand there is evidence of what we have known all along: For organizations, it is less of a skills gap and more of a mindset shift. In May 2021, Evolve Security hosted a meetup on The Cybersecurity Talent Gap with expert chief information security officer panelists to help identify the root cause of this gap. These CISOs resoundingly found that in today's economy it is more about nurturing aptitude and re-thinking the DNA of what makes a successful Cybersecurity Professional. This is not to discount the value of core technical cyber skills, but rather be open to a soft-skills revolution. One recommendation is to take close look

at job descriptions: Does a hiring manager really need that unicorn which could take six months to find, or would they find their best candidates with a narrowed focus on what you cannot teach (think EQ, problem solving, and passion) and a willingness to train for the rest? Sometimes an organization may need a Pro to hit the ground running, but see what happens when companies foster a culture of seamless, continuous training and build a pipeline of talent.

As industry prepares for a post-pandemic hiring landscape, use this time to rethink what makes a great Cyber Pro and find efficient and effective ways for continuous upskilling. Just as our adversaries' tactics are always shifting, both execs and Professionals need to stay on top of their game.

For those looking to pivot into cybersecurity, now is your time. **Many of the skill sets valued by the C-Suite, from mastering Governance, Risk and Compliance to leading crisis response and change, are all great points of entry for a career in cybersecurity.** And for the uber-technical pros, look at the most difficult to find skills across the domains – where can you pivot to become that cyber unicorn?

And possibly most important, how can industry support strategic upskilling of non-traditional hires and those in pivot roles to open the aperture for sector-switchers with increased diversity and equity in the field? There are many possible paths to cybersecurity. Validated by the 2020 (ISC)² Cybersecurity Workforce Study:

> Consider non-traditional candidates, from career-changers to liberal arts graduates to ex-military personnel; the broader your net, the more potential candidates you can identify. Further opening the space, consider more work-from-home options for your cybersecurity workforce, as most professionals are learning to be just as productive and as effective working from home. This dramatically widens your available talent.- **2020 (ISC)² Cybersecurity Workforce Study**

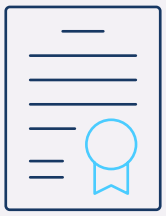
Finally, join the conversation again for the 2022 Evolve Security Cybersecurity Skills Report: State of the Cybersecurity Workforce. Next year's survey will further break down the skills gap by industry, assess the value of soft skills, and take a closer look at the entry-level versus experienced-hire talent gap. Additionally, it will assess steps to mitigate unconscious bias in cyber hires and increase representation in the cybersecurity field.

Learn more at www.evolvesecurity.com

EVOLVE SECURITY

Appendix: Evolve Security Training and Bootcamps

Cybersecurity Bootcamps: Evolve provides a holistic approach to cybersecurity education delivering hands-on lab-based learning and thorough job preparation to help transition professionals into the cybersecurity field. We offer a combination of live and on-line instruction, lab tutorials, and custom environments inspired by real-world scenarios. In addition, we provide an apprenticeship program offering real work experience and a voucher for the CompTIA Security+. We are one of two Offensive Security Certified Professional (OSCP) Bootcamp authorized to teach nationwide.



Enterprise Training: We are also a #1 ranked Cybersecurity Academy. Evolve Security Academy's primary goal is to develop and upskill top-tier cybersecurity talent and help launch cybersecurity careers. From DevSecOps to Security Awareness and Threat Detection, we deliver practical, hands-on training to provide (deliver repeated twice in same sentence) concrete skills to take your team to the next level.

Cybersecurity Advisory: We evolve with the threat landscape to effectively strengthen your security posture. Our offerings include Security Program and Policy, Security Strategy, Assessment and Advisory Services including Operations Security, Vendor Risk Management, Incident Management and Compliance Review.

Staffing with Oversight: It takes three months or longer to fill an empty security position, and the more technical the role, the more difficult to fill. Let Evolve assist you with your talent shortage need through temporary, long-term, or direct hire engagements.

Managed Penetration Testing: Services include automated network, application and Cloud vulnerability scanning and fully manual penetration testing with comprehensive and continuous vulnerability identification in a single report. We understand your challenges and will help your team remediate issues – fast.