PART OF PHAIDON INTERNATIONAL

GLO COMMS

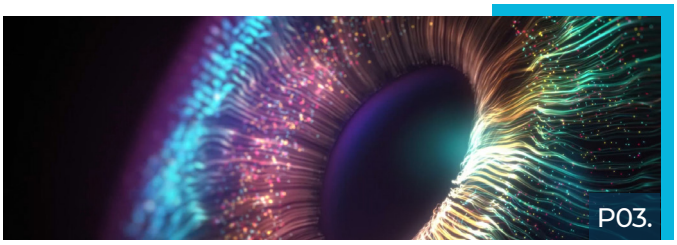
GLOBAL

INDUSTRY INSIGHTS

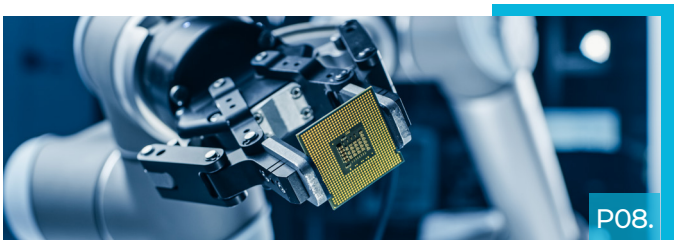
Cyber Security Talent Insights

Top hiring trends and challenges in the industry

Contents

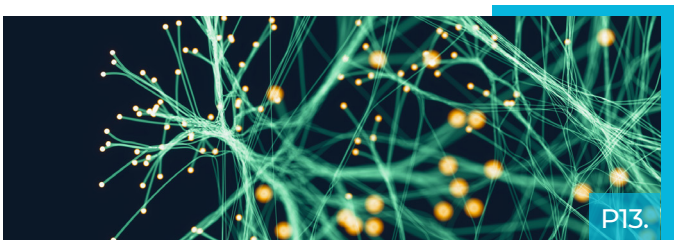


Securing our digital future

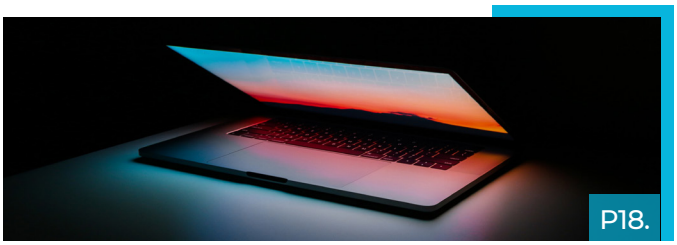


Balancing priorities

Top candidate priorities in cyber security



Challenging environments and career growth



Summary

Securing Our **Digital Future**

From the security engineers who protect our networks, to the analysts who identify key vulnerabilities, cyber security is becoming an integral part of businesses across all industries. Driven by a growing awareness of the need for security, the global cyber security market is projected to expand at a CAGR of 8.9% to 266 billion by 2027[1], with the McKinsey Institute estimating a $2 trillion market opportunity[2] waiting for cyber security tech and software providers.

With opportunity however, comes challenges. The market is facing multiple disruptions, from innovations introducing new vulnerabilities, to human risk and AI-enabled fraud.

Beyond technology, talent remains the biggest challenge. In our rapidly digitalizing world, skilled professionals are in high demand to secure the critical infrastructure of businesses and our day-to-day lives. Yet by 2030, there will be a need for 3.4 million additional security positions[3] but not nearly enough people to fill them, leaving organizations vulnerable.

To capitalize on the opportunities in the cyber security market - while protecting the confidentiality, integrity, and availability of systems, networks, and data against cyberattacks or unauthorized access - companies must develop effective hiring solutions. Such strategies encompass compelling offers that will attract qualified professionals and focus on measures to retain increasingly business-critical cyber security talent.

What a persuasive offer looks like in today's talent market is influenced by developments at international, national and regional levels. As a leading talent search partner with a global network of qualified professionals, Glocomms has a keen sense of candidates' top priorities, and we have been industry leaders for over a decade on how best to navigate the challenging technology talent landscape.

In this report, our experts provide deep insights into the state of cyber security today and share their key takeaways for hiring managers and professionals alike.

Key Trends in Cyber Security

1. INCREASING AWARENESS AND DIVERSIFYING RISKS

The surge in digitalization due to the pandemic led to a 38% increase in global cyber attacks[4], prompting organizations to reevaluate their cyber security capabilities.

While companies recognize the need for skilled professionals to secure their critical infrastructure, the dynamic nature of an innovative industry constantly introduces new digital vulnerabilities into existing systems and workflows. Meanwhile, new regulations pose a challenge for both tech engineers and compliance professionals alike.

However, the greatest risk to cyber security remains the human factor. With more than 85% of all attacks[5] caused by a company's own employees, it is even more essential today to find professionals who can seamlessly integrate with existing teams.

2. AUTOMATING PROCESSES

The days of large cyber security teams are giving way to more boutique solutions supported by automation, leading to a surge in demand for cyber security professionals with skills in this area. Security automation allows companies to detect and flag potential risks and threats at a speed impossible for humans, saving both time and money.

According to the IBM Cost of a Data Breach Report[6], fully deployed security AI and automation saves companies $3.05 million per data breach, a 65.2% difference in average breach cost. According to Rapid7[7], cyber security automation can reduce response time in the event of a threat by 83%.

Key Trends in Cyber Security

3. MITIGATING INSIDER RISK THROUGH A HUMAN-FIRST APPROACH

As awareness of vulnerabilities has increased, companies have begun to implement cyber security awareness programs. As **Katie Owston, Associate Vice President at Glocomms, says:**

> **"**Humans are humans. No matter how much technology you have in place, the biggest issue could be someone clicking a link in an email they think is from their boss.**"**

Verizon's Data Breach Report[8] found that 82% of security breaches are the result of human error. To mitigate that risk, organizations need cyber security professionals who are a cultural fit and can integrate into existing teams.

When we ask cyber security candidates what they would have done differently in their role if they knew then what they know now, the answers were clear: They would first build relationships with key stakeholders and individual team members. **According to Katie:**

> **"**Candidates tell us they tried to change the technology first, but it wasn't efficient. They realized that in order for their cyber security and awareness efforts to be successful, they needed to get everyone in the organization on board with them and how they were going to make it work.**"**

4. POSITIVE CANDIDATE EXPERIENCE AND THE INTERVIEW PROCESS

Securing the ideal cyber security talent, who fits both the company culture and the job requirements, begins with the interview process. **According to Katie Owston**, companies need to have a predetermined interview process and timeline prior to advertising a role and interviewing talent. This is to manage candidates' expectations accordingly, and also so they can share these timelines with other companies they are speaking with for better transparency and to build trust.

Another important factor is the experience of the interviews themselves. Candidates have become more attuned to how the process reflects company culture and evaluate a potential employer accordingly. If a company is perceived as not prioritizing the candidate and their time during the interview process, the candidate will be wary of signing with the company.

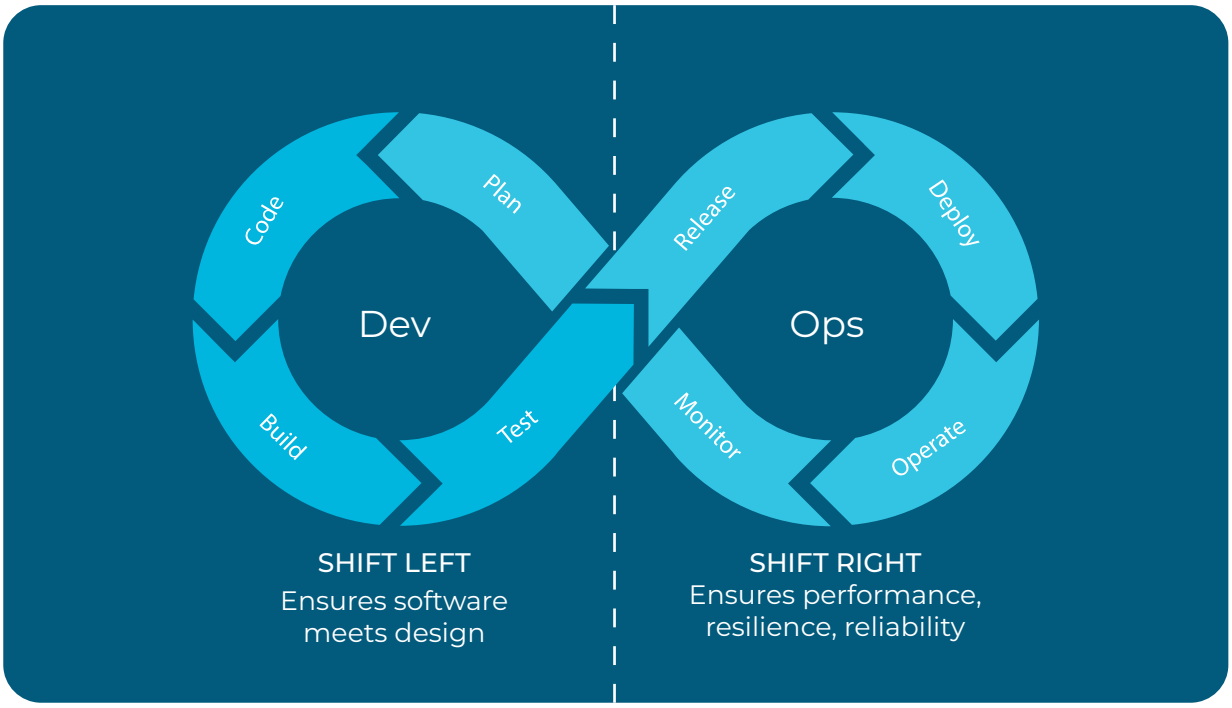
Having a job description is paramount to selling a role these days. It legitimizes a company's stance on the importance of a position within their business, helps outline what the job will entail, and shows that a company already knows how this person will impact the team and wider business. Not having a job description isn't a deal breaker, but it should be noted in a first interview why there isn't a job description in the first place.

Key Trends in Cyber Security

5. SHIFTING LEFT

Prior to the increased focus on cyber security, the software development lifecycle involved testing before releasing software, often resulting in delays should the product fail to meet functionality or security requirements. Software engineers would build an environment, then consult security engineers who would revise accordingly.

As skills and knowledge grew, organizations began to “shift left”. “Shift left” and “shift right” testing are core concepts of the DevOps methodology. To understand this evolution, you can think of the software development cycle as a continuous loop in which teams plan, develop, and test new software. Pre-production focuses on design criteria, while the right side of the loop releases, maintains, and improves the software in a reliable manner that aligns with business goals.



Today, teams test functionality as well as whether the product meets customer requirements early in the process. As a result, improvements are identified faster and the development process is accelerated. The shift to the left is critical to cost-effective development processes and reflects the growing role of cybersecurity concerns in software engineering.

“Shifting left” also impacts hiring, as the ability to build secure code from the start is one of the most sought-after skills in the DevOps world today.

Key Trends in Cyber Security

6. BLENDING WITH RISK

Given the complex nature of an organization's infrastructure, as well as the role of the human factor, implementing an effective cyber security strategy is critical to ensuring an organization's profitability.

Especially in larger organizations, technology risk and cyber security used to be clearly separated. While technology risk had more of an internal controls background, cyber security professionals focused on traditional forms of security.

However, as processes become more intertwined, technology risk and cyber security are joining forces to ensure effective and secure processes.

This, in turn, has had an impact on hiring, as **Katie confirms**. Increasingly, positions labeled "Head of Technology Risk" require candidates with a very hands-on cyber security background. These professionals can assess whether systems are safe and secure, and if not, assess the risk to the business and prioritize accordingly.

At Glocomms, we have seen professionals with an NSA background move into "Head of Risk" positions, which would not have been possible even five years ago.

This blending of disciplines also facilitates communication, **Katie explains:**

> "Individuals who come from a non-technical background who advise technical teams on what they do, or conduct internal risk evaluations in the business can sometimes struggle to understand how long from a technical standpoint something will take to accomplish. Having people that understand the technology and risk evaluation creates a more collaborative and seamless relationships between teams."

In other cases, **Katie says**, tech might expect an incredibly short turnaround for tasks that take a full week, which would create tension between departments.

For more on technology risk in Financial Sciences & Services, read the US and Europe risk reports produced by our partner brand **Selby Jennings**

DOWNLOAD TODAY

Key Trends in Cyber Security

7. BALANCING PRIORITIES

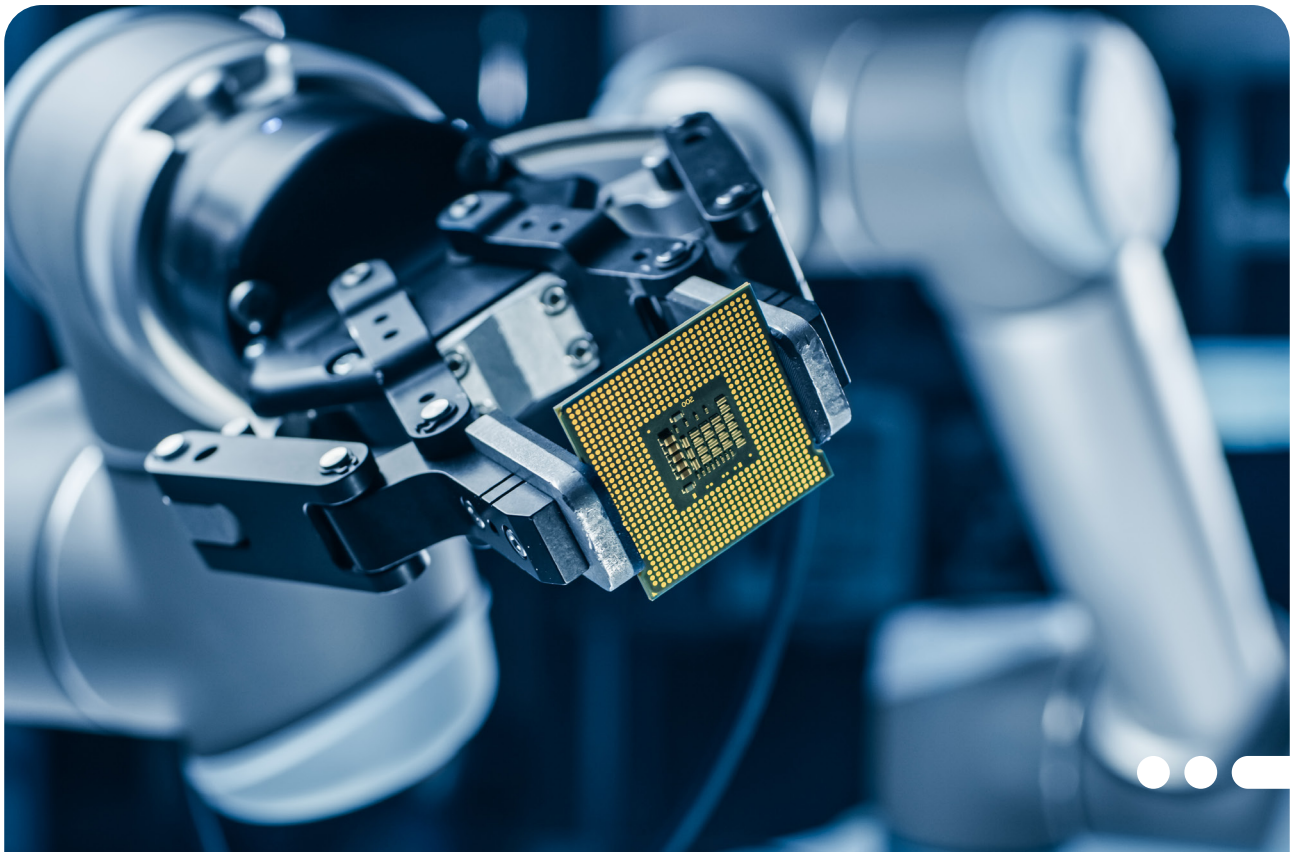
As much as organizations need a skilled cyber security leader to take a holistic view of the existing environment and effectively identify risks, they also need SecDevOps engineers who can take all the necessary steps to improve security and automation.

The question of which of these positions to fill first is a tricky one, and depends on each organization's unique situation. Talent partners such as Glocomms can help clarify cyber security hiring needs and priorities, with an eye toward long-term effectiveness and impact.

To balance the need for both a top-level perspective and ground-level performance, more and more companies are opting to hire security architects, either under that title of as a head of security. **As Katie explains**, security architects come from a software security engineering background, usually in DevSec Ops, and have been out of engineering for a few years.

They still have enough knowledge to make informed recommendations and help with coding needs when needed. Beyond technical skills, security architects are able to communicate with people in a non-technical capacity and explain requirements in a clear way.

As heads of security, former security architects are familiar with the entire development cycle, from left to right, and may even pioneer a company's cyber security department before hiring more engineers to maximize effectiveness.



Key Trends in Cyber Security

8. DIVERSITY

With the rapid growth of the cyber security sector comes a need for new ideas and fresh perspectives. Various research studies have proven that having a diverse workforce can lead to increased innovation and productivity.

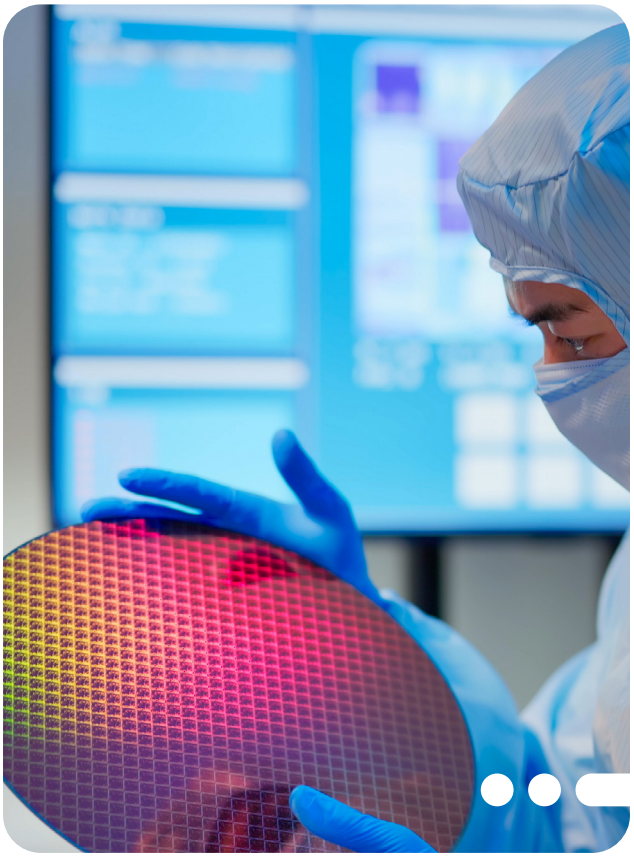
Yet, only 26% of cyber security professionals identify as an ethnic/racial minority according to the (ISC)[9] Innovation Through Inclusion: The Multicultural Cybersecurity Workforce report. The same organization's Women in Cybersecurity report[10] found that women represent 24% of cyber security positions. What's more, the people who identify as part of a racial or ethnic minority tend to occupy non-managerial positions.

While increasing diversity in cyber security is a long-term challenge for organizations across the globe, there are steps every company can take to demonstrate to candidates that they are committed to affecting change. The composition of the interview panel is one way - if there are minorities in senior positions, they need to be visible during the interview process.

One cyber security talent shared her experience to **Katie's team at Glocomms:**

> **"**Seeing a person of color at a director level position means a lot to me, because I can see what they say about diversity in their organization is true since I'm speaking with people who have lived that.**"**

Finding diverse talent is a high priority for the Glocomms team, yet sourcing such professionals is a challenge, with Katie suggesting that within cyber security, there is diverse talent with the right skill set, but it is harder to find these individuals.



Katie admits that many experienced individuals may not fit the standard mold, requiring an unconventional hiring approach:

> **"**Within cyber security, there is diverse talent with the right skill set, but you have to go outside normal circles to find these individuals.**"**

While there have been advancements in diversifying the cyber security sector, much of this has been in recent years. This means that a lot of diverse talent is just at the start of their career journeys, and therefore it will take some time to gain the experience needed to fill senior roles. At the rate that cyber security is changing and needing to adapt, they're not maturing fast enough.

This also affects prioritization. Not every sector can afford to focus on a diverse candidate shortlist because the talent gap is so severe that it's a challenge to fill the position at all, let alone with a diverse candidate.

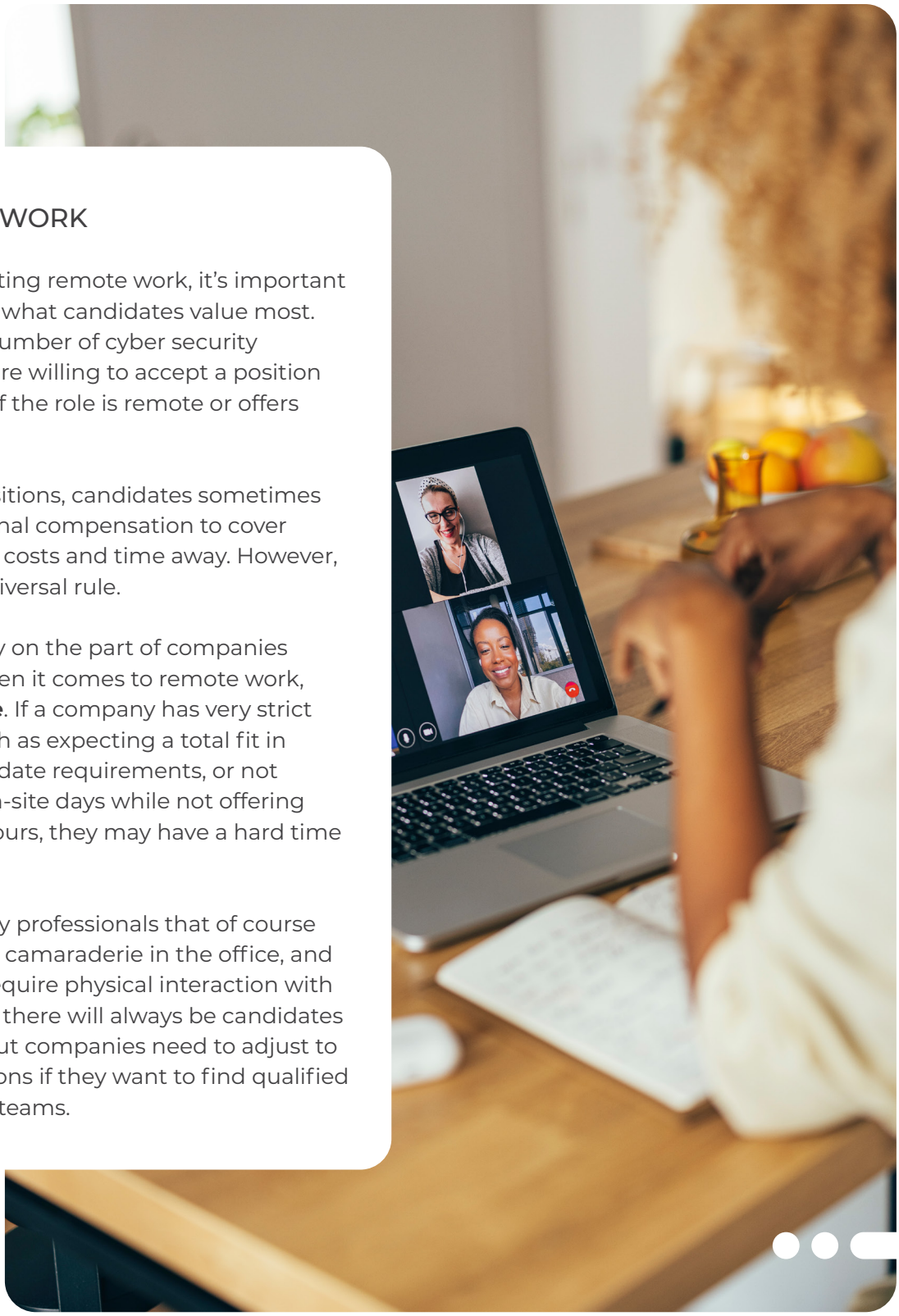
Top Candidate Priorities in Cyber Security

What do companies need to offer to attract high-caliber professionals?

Unfortunately, there is no magic combination of benefits that will appeal equally to every dream candidate. As an expert talent partner in cyber security, Glocomms continually engages in comprehensive conversations with the individuals we represent to ensure that their philosophy and aspirations align with the mission and culture of the company they choose to work for.

Top Candidate Priorities in Cyber Security

Katie Owston and her team are able to identify the key attractions and advise companies on how to optimize their offers for maximum impact.



1. FLEXIBLE WORK

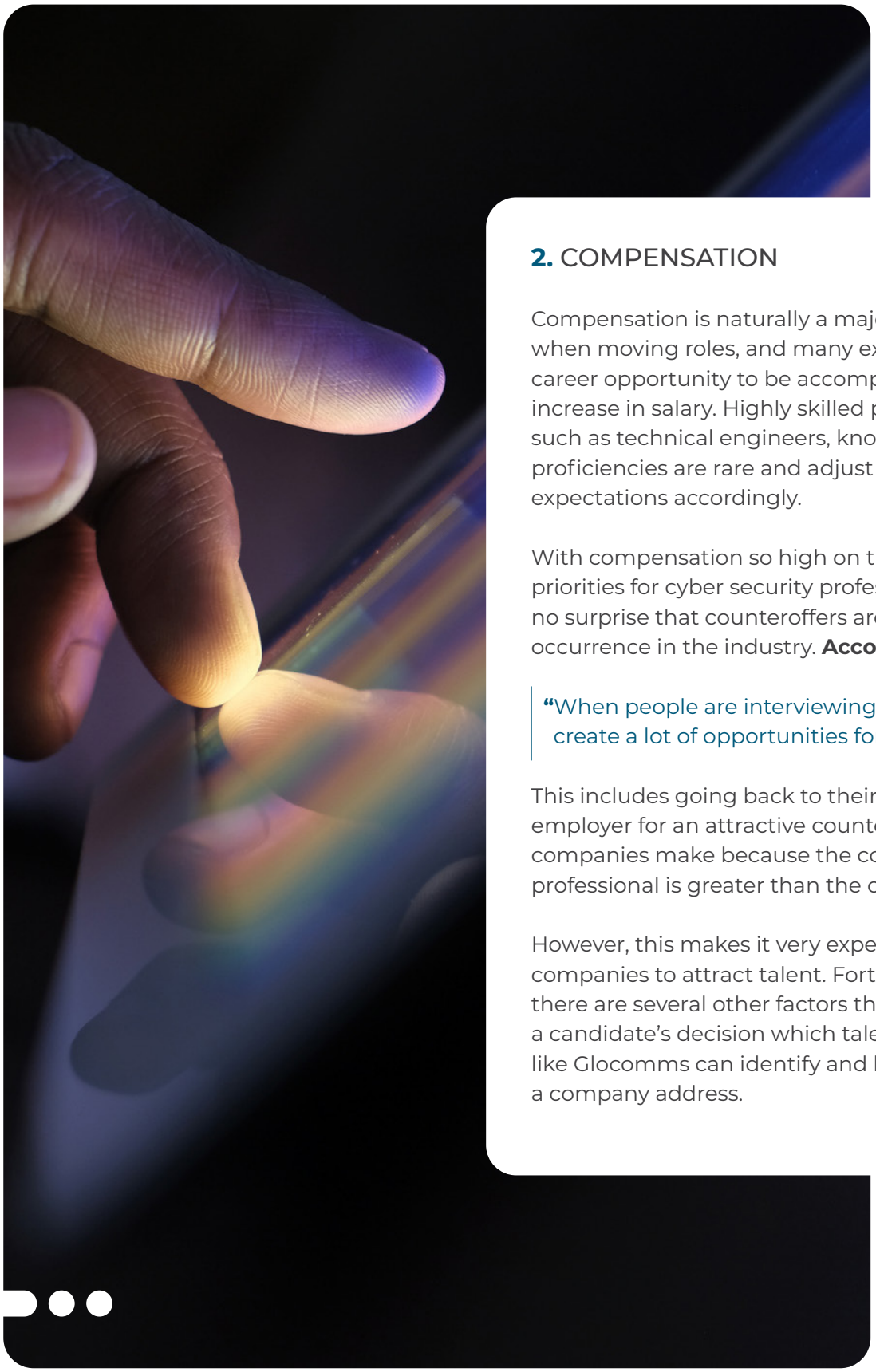
When negotiating remote work, it's important to understand what candidates value most. A significant number of cyber security professionals are willing to accept a position that pays less if the role is remote or offers flexibility.

For on-site positions, candidates sometimes expect additional compensation to cover transportation costs and time away. However, this is not a universal rule.

Some flexibility on the part of companies is essential when it comes to remote work, **cautions Katie**. If a company has very strict standards, such as expecting a total fit in terms of candidate requirements, or not budging on on-site days while not offering flexible core hours, they may have a hard time filling the role.

There are many professionals that of course appreciate the camaraderie in the office, and certain roles require physical interaction with technology, so there will always be candidates in the office, but companies need to adjust to new expectations if they want to find qualified cyber security teams.

Top Candidate Priorities in Cyber Security



2. COMPENSATION

Compensation is naturally a major factor when moving roles, and many expect a new career opportunity to be accompanied by an increase in salary. Highly skilled professionals, such as technical engineers, know that their proficiencies are rare and adjust their salary expectations accordingly.

With compensation so high on the list of priorities for cyber security professionals, it's no surprise that counteroffers are a regular occurrence in the industry. **According to Katie:**

> **"**When people are interviewing, they want to create a lot of opportunities for themselves.**"**

This includes going back to their current employer for an attractive counteroffer, which companies make because the cost of losing a professional is greater than the counteroffer.

However, this makes it very expensive for companies to attract talent. Fortunately, there are several other factors that influence a candidate's decision which talent partners like Glocomms can identify and help a company address.

Top Candidate Priorities in Cyber Security

3. CHALLENGING ENVIRONMENTS AND GROWTH OPPORTUNITIES

Our experts at Glocomms always ask a candidate, **"Where do you want to be in five years?"** This provides valuable insight into what growth opportunities a cyber security professional is looking for from a potential employer. Either they want to stay technical and become a subject matter expert, or they want to move into a management role and eventually fill a chief information or security officer position. If an organization can show them the path to that goal, it will help them attract high-caliber candidates.

In addition to career growth, day-to-day challenges are both a powerful attraction and a factor in reducing turnover. Larger companies may be more likely to silo professionals into niche areas and not provide as much exposure to the outside world. Cyber security professionals typically yearn to experience different aspects of technology and impact more than their field.

As such, a clear plan for professional growth and the opportunity to be challenged or work in a challenging work environment where they will learn is just as attractive to many candidates as compensation, **according to Katie**.

Top Candidate Priorities in Cyber Security

4. COMPANY CULTURE AND ED&I INITIATIVES

Strong culture fosters teamwork, a sense of community, and inclusion – leading to more employee engagement that ultimately benefits growth and revenue.

Sometimes the desire to work remotely can hinder the creation of company culture as it can be trickier to create culture online. At Glocomms, we advocate a middle ground in the form of flexible and core hours.

It is important to understand an individual's motivations as well as their personal circumstances. For some, being the only cyber security professional is what they thrive in. For others, not so much as there is a significant ownership that comes with a cyber security role. It is a partnership in knowing what motivates each and every person and therefore how you reward them. For example, if someone is the sole cyber security lead who is often on call, perhaps they are afforded more flexible hours in return.

When done effectively, improving employee well-being can increase employee productivity, company profitability, customer satisfaction, and reduce turnover.

One factor that influences a company's culture while also improving employee wellbeing is ED&I initiatives.

The tech industry is notorious for its lack of diverse leadership, so a change to the status quo could have profound effects on hiring. Candidates are typically looking for more inclusive, diverse work cultures. Therefore, more companies need to prioritize hiring candidates from less traditional backgrounds. Without true diversity at a company, any ED&I initiative will fall flat.

Top Candidate Priorities in Cyber Security

5. OTHER BENEFITS

In addition to flexibility, compensation and culture, other benefits can move the needle and convince a candidate to sign.

This depends on the individual and requires a deep connection with the candidate to uncover, as **Katie explains:**

> **"**We learnt with a recent placement that their partner was undergoing fertility treatment as they wanted to expand their family. Our candidate was concerned about moving roles and losing access to certain aspects of their healthcare, but by working with the candidate and client, we were able to find out that the new company could offer the same healthcare package, and in the end they could continue to cover that treatment for their spouse.**"**

In general, candidates appreciate benefits that also support a long-term commitment, such as health benefits, pension contributions or 401ks in the US. Whether equity is an attractive addition to compensation depends on the IPO status of the company. Bonuses can also be a factor in swaying candidates.

Key Takeaways for Hiring Managers

The factors that influence effective talent strategies are multifaceted and complex. The rapid growth of the industry and the ongoing shortage of qualified professionals further complicate the hiring landscape for the cyber security sector.

As talent experts, our consultants at Glocomms have identified several strategies and actions companies can take to improve their reach with promising candidates and increase retention.

1. REMOTE FLEXIBILITY IS ESSENTIAL FOR CYBER SECURITY PROFESSIONALS

The pandemic years have proven that certain roles can be easily performed remotely or partially remotely. As a result, cyber security candidates are increasingly reluctant to commit to onsite roles. Companies that don't offer remote options, especially in roles like cloud security, will find it very difficult to attract candidates. The desire for more flexible working arrangements is impacting salaries, **with Katie confirming** that candidates are willing to accept lower salaries in exchange for working remotely.

> **A very effective model, as Katie explains from experience, is to offer flexible hours to employees. Combined with two to three remote days a week, this can be a very attractive proposition for experienced cyber security professionals.**

2. PROVIDE A CHALLENGING ENVIRONMENT TO ATTRACT AND RETAIN CANDIDATES

Keeping cyber security professionals in their niche can prove detrimental to employee retention as security professionals may yearn to experience different aspects of technology and impact more than just their corner of the company.

Most cyber security experts are incredibly passionate and curious about their field. Working in an environment where they aren't the smartest person in a room holds tremendous excitement and can draw promising candidates to a company.

The human need for challenge and growth ties into employee well-being and their commitment to the company culture. Therefore, the challenges must not be viewed in a vacuum but rather as one piece of the company culture puzzle.

3. PRESENT A CLEAR CAREER PATH TO ATTRACT IDEAL FITS

Demonstrating to cyber security candidates a clear career path will support hiring strategies. What that path looks like will depend on each candidate's situation and goals, because some professionals want to move into more senior roles with management responsibilities, while others prefer to stay technical and become subject matter experts in their field.

A professional talent partner will provide insights into a candidate's goals when presenting or sharing a shortlist. In either scenario, a company can tailor its offer by outlining how this new position will support the candidate's career path. The benefit goes beyond attracting candidates – it also helps retain them by giving them a clear perspective.

Key Takeaways for Professionals

4. SEIZE THE SECTOR'S GROWTH OPPORTUNITIES

Cyber security is an exciting industry to be in with amazing opportunities for personal and professional development: The continuous merging of technology risk and cyber security means that the work environment is becoming increasingly challenging. With this growing awareness, companies have begun to shift their focus on building strong cyber security teams and making them an integral part of their operations.

While many organizations recognize that growth is essential to creating long-term perspectives for desired candidates, it is still necessary for professionals to voice their ambitions. This way, both parties can ensure they are aligned on career progression and goals before committing to each other.

5. APPLY A HUMAN-FIRST APPROACH IN A NEW ROLE

When asked what they would do differently in retrospect when starting a new role, the majority of Glocomms candidates said they would first build a personal rapport with other teams before implementing technological changes. This increases the likelihood of implementation and helps establish trust in awareness campaigns.

The fact that nearly all cyber attacks originate from human factors makes it even more important that new talent integrates seamlessly with existing teams.

6. PARTNER WITH AN INDUSTRY EXPERT TO MAXIMIZE YOUR POTENTIAL

From security engineer to cloud architect, from manager to director, the needs and goals of candidates in cyber security are as unique as the individuals themselves. In today's competitive landscape, identifying an opportunity that aligns with one's values and negotiating for key requirements can be a daunting task.

That's why a growing number of professionals are choosing to work with a talent expert who specializes in cyber security roles. These consultants have a deep network of connections within companies and organizations across multiple industries. They stay up to date with the latest jobs and can quickly identify roles that match a candidate's skills and experience.

Based on in-depth conversations with candidates, partners like Glocomms can effectively negotiate with companies and tailor a compelling offer that aligns with a candidate's priorities. At the same time, talent partners understand company culture and can offer expert advice when a candidate has competing offers or is struggling to make a decision.

Summary

The cyber security landscape is rapidly evolving as technologies such as artificial intelligence, cloud computing, and beyond continue to advance and become an integral part of businesses and homes alike. With this swift progress comes an increased risk of cyber attacks and data breaches, which can threaten an organization's operations and financial stability.

As awareness delete and replace with of cyber security grows, so does the demand for qualified professionals to mitigate these risks. Companies are struggling to fill positions ranging from security analysts to architects, engineers, and specialists in areas like cloud security, application security, and more.

While this report has shown that there are several key strategies available to organizations to attract and retain top talent, there is no magic fix that will ensure all criteria are met. Meanwhile, candidates enjoy the promise of exciting opportunities, but finding the right fit on both a cultural and professional level remains a challenge.

Despite these obstacles, cyber security presents exciting opportunities for companies and businesses alike. With experts predicting continued growth, it is up to each individual to find the right partners to navigate this dynamic environment.

About Glocomms

It has never been more imperative to make smart hiring decisions in the technology industry.

Cyber security attacks have reached an all-time high, with networks now increasingly complex and businesses often leaving traditional systems and migrating towards cloud infrastructure. Having top talent in place to mitigate these threats is therefore absolutely critical.

Specializing in solving hiring challenges for the world's largest Big Tech firms and data providers to innovative tech start-ups and leading financial firms, we pride ourselves on engaging with top talent worldwide and providing businesses with the right people, exactly when they're needed.

OUR SPECIALISMS

- Cloud & Infrastructure
- Commercial Services
- Cyber Security
- Data & Analytics
- Development & Engineering
- Enterprise Solutions

Contact Glocomms

Giancarlo Hirsch
Managing Director, Glocomms
New York, USA

Contact Giancarlo

Paul Norman
Managing Director, Glocomms
London, Europe

Contact Paul

Brian Vigorita
Director, Glocomms
New York, USA

Contact Brian

Katie Owston
AVP, Head of Cyber Security
New York, USA

Contact Katie

Harry Moore
Cyber & Information Security Team Lead
London, Europe

Contact Harry

UPLOAD YOUR RESUME | SUBMIT A VACANCY | NEW OPPORTUNITIES

1. https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=EAIaIQobChMIyKK_hLTY_QIV55BoCR1dlwOSEAAYBCAAEgLpJPD_BwE

2. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

3. https://www.cybersecuritydive.com/news/cybersecurity-talent-gap-worker-shortage/639724/

4. https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022

5. https://sosafe-awareness.com/resources/reports/human-risk-review/

6. https://www.ibm.com/reports/data-breach

7. https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-roi-orchestration-automation-whitepaper.pdf

8. https://www.verizon.com/business/resources/reports/dbir/

9. https://www.isc2.org/Research/Cybersecurity-Diversity

10. https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx