OCTOBER 2022

STEPPING UP TO THE MIC

Minorities in Cybersecurity

MiC TALENT SOLUTIONS

BASELINE REPORT

MiC Baseline Report

Minorities in Cybersecurity, Inc. and MiC Talent Solutions, Inc. co-sponsored a baseline study to get an understanding of the challenges minorities, women, and non-binary talent face in their cybersecurity careers, from landing their first cybersecurity role, navigating their careers for promotional opportunities, all the way up to the executive level and attempting to pivot to Board of Directors' opportunities.

The study took place in the month of August 2022. We interviewed approximately twenty-five (**25**) individuals and organizations, including those categorized as **MiC Aspirers™** (In college, college graduate or transitioning into the cybersecurity field), **MiC Builders™** (Entry to mid-career cybersecurity professionals), **MiC Communicators™** (People leaders), **MiC Directors™** (Director and above), human resource (HR) managers, recruiters and hiring managers. Multiple ethnic groups (African, Asian, Black, Hispanic, and White) were represented, multiple countries (US, Kenya, Jamaica, and India) and industries (public, private, academia and government).

Our purpose was twofold, to give a voice to underrepresented talent on their challenges when attempting to obtain their first cybersecurity role and growing their careers. In addition, to get a general sense from organizations of the challenges they face with attracting, obtaining, and retaining underrepresented talent. Our goal was to determine a path forward by finding common ground and actions both could take to move the needle.

Our findings were at times surprising and unfortunately at times highly predictable.

From the talent perspective there was still this nagging sense organizations question their mental and technical capability to perform well in the cybersecurity field. Oftentimes underrepresented talent, at all levels, believe organizations were not really trying to attract them, they believe their interviews were more of a **"check the box"** exercise and they were not seriously being considered for the role.

The truth remained, **100%** of those surveyed believed their direct manager had the most influence over their experience within an organization. The professionals we interviewed with supportive bosses (**29%**) had a positive outlook on their ability to grow and navigate their careers. Those professionals with questionable bosses (**71%**) were more pessimistic and actively seeking other job opportunities.

Almost every minority and woman leader we spoke to expressed **EXTREME** frustration at being single out and asked to lead their organizational Diversity, Equity, and Inclusion (DEI) initiatives for their cybersecurity teams. Those numbers were higher when individuals were in people leadership positions with **60%** of those surveyed at the MiC Communicators™ level and **100%** of those at the MiC Director™ level being asked to lead DEI initiatives.

Leaders were pushing back by either flat out refusing or purposefully stepping away from those responsibilities. Many expressed experiencing resistance and/or micro aggressions from their peers, felt they were not given credit for their efforts from their boss, including not being recognized for their efforts during performance reviews, and **0%** were offered any additional compensation.

When it comes to organizations, the most interesting thing we found was corporate human resource, talent acquisition and internal recruitment staff were oftentimes seen as the bottleneck when it came to identifying underrepresented cybersecurity talent. When asked about talent recruitment and what type of outreach their organizations were doing to attract underrepresented talent the responses were unanticipated. Some expressed frustration at the **“complete lack of transparency”** they had into the recruitment process. They received candidate resumes and often did not know where they came from. Others felt there was just a lack of knowledge and understanding about recent social challenges and the need to do things differently. One hiring manager described recruitment as a **"black hole"** and even though it was understood HR had overall hiring responsibilities for the company, it was a lack of understanding about the unique challenges when hiring for cybersecurity professionals in general, which led to their disappointing diversity statistics. Many companies were still relying on more traditional ways of sourcing for cybersecurity talent and those sources did not often include where diverse talent pools were located. Even when talking to recruiters directly assigned to cybersecurity teams, they expressed frustration with their failed attempts to change hiring practices by convincing internal stakeholders to promote senior level roles from within and backfill much easier to fill entry level roles with diverse candidates.

MiC Aspirers™

When talking to the MiC Aspirers™ group it became readily apparent organizations were not doing a very good job at defining the needs they had for entry-level roles. Just about every professional in this group described their frustration with unrealistic entry level job descriptions seeking two or more years of experience. They believed those roles were not entry level and they were not given credit for their choice to pursue a college degree. College graduates were frustrated in their degree being discounted versus certifications. Many believed certifications were important to obtaining an interview but not necessarily a determining factor in whether they would succeed in a cybersecurity role.

Although the professionals in this group had applied to a countless number of cybersecurity job opportunities, interviews were few and far between, with a success rate of application to interview around **33%**, with **0%** currently in a cybersecurity role. To make matters worse, follow up from organizations regarding their unsuccessful attempts was nonexistent. They did not know how they could improve their efforts or what they needed to be a better candidate. The areas of focus for applicants in this group were work life balance, job location and/or remote opportunities, US Visa sponsorship, salary, and career development opportunities.

MiC Aspirers™ Observations

For entry level and transitioning cybersecurity professionals in the MiC Aspirers™ category, organizations should do better defining what skills are really required for a candidate to have success in a role, starting with a better definition of the word **“experience”**. Depending on the role, relevant helpdesk, IT, risk management, audit, project management, etc. experience could suffice in an entry level cybersecurity role. Of course, it means an organization must have the appropriate training opportunities to assist these professionals to ensure their success. One thing is clear, what we should do for entry level talent is stop focusing on the need for all these certifications as a barrier to entry into the profession. An organization would do well in hiring entry level professionals with an unquenchable thirst for knowledge and a healthy curiosity for cybersecurity, instead of requiring unnecessary certifications.

MiC Builders™

In general, the sense we got from the individuals in the Builders category was they were lost. They spent so much time trying to get their first cybersecurity role and when they finally land in the space the challenge was knowing how to build a cybersecurity career. Once they had learned the basics and had a good handle on their first role they were at a loss and did not know what to do next, they felt they were starting all over again when searching for their next opportunity.

Some of the frustrations expressed by this group was a lack of training, guidance, support, and mentorship. There was a sense they either somehow learn how to swim or sink to the bottom of their career goals. Some stated **“junior people don’t get training or support”**, they feel **“senior level people were withholding information”** and **“leadership development programs were reserved for people already in leadership positions”**

MiC Builders™ Observations

We are failing as an industry by not having good career paths for cybersecurity professionals. Sure, some organizations have individual contributor or people leader tracks but what about moving from security operations to risk management, or from project manager to reverse engineering? At this point we are still in a situation where we are focusing on security operation center activities, **“hacking”** and other technical pieces. Instead of the entire ecosystem of the cybersecurity field. Our MiC Builders™ become lost, despondent, or leave the field because they quickly get bored with repetitive activities.

Another glaring issue is why do we reserve leadership training for individuals already in leadership positions? If a company wants their talent to remain engaged and loyal to the organization, it stands to reason they should provide their talent with some sort of roadmap for success. The **"quiet quitting"** scenario exists, in part, because professionals are not engaged or motivated in their working environment.

In general, because we are minorities in society and on our teams, we are operating in an area of insecurity. We don't necessarily know the rules and find it difficult, especially in those environments where networking is essential to ascension, to navigate how to build the appropriate working relationships required to assist with getting to the next level.

MiC Communicators™

For those underrepresented professionals who find themselves lucky enough to reach the MiC Communicators™ level, the road was even more bumpy. As often the case, the rise from individual contributor to people leader was directly attributed to someone believing in and taking a chance on an individual, with some saying they were told by bosses **"I believe in you."** However, Communicators expressed frustration not knowing what was being required of them. Not only was there a lack of training and support in understanding how to manage people, but training on how to prove their teams value to the organization was also missing.

The jump from individual contributor to people leader, for inherently introverted people, was a challenge, because the focus shifts from what they could do as a highly functioning individual contributor to motivating a team to perform effectively. There seemed to be very few opportunities available to prepare these leaders for this transition. Professionals at this level struggled with team dynamics, conflict resolution, and perception by their team and peers as being worthy to be in their role. Communicators describe this level as the beginning of **"internal politics"** and **"gamesmanship"** and where their cross functional relationships become more important.

MiC Communicators™ Observations

What's clear, when a leader does not have the appropriate resources and leadership training, they fail to reach their potential. Many of the MiC Communicators™ we spoke to stated they had peripheral knowledge of leadership training opportunities available at their organizations, however, they did not often have access to it. One described it as **"secret levels in a video game, and you must reach a certain level before leadership training magically appears."** Another described it like espionage and a person should actively listen to others around them to obtain the knowledge they need, then persistently ask a lot of questions, and **"put people on the spot"** until the organization is forced to offer you the same opportunities.

What's curious about the fact of leadership training being hidden or difficult to find, is that both MiC Builders™ and Communicators had the same experience! It begs the question, if Communicators have reached people leadership and are still not being offered the leadership training received by others, are they really being supported and seen as effective people leaders?

MiC Directors™

Rare air indeed!! Underrepresented individuals who reached the Director or above level in the cybersecurity field were difficult to find but when we did, they spoke very candidly and forthcoming on the challenges they faced, not only individually but when hiring other people in underrepresented groups.

They expressed the same challenges as more junior professionals, in as much as the feeling or lack thereof of belonging. MiC Directors™ had even more questions, from peers and directs, about their qualifications for being in their position. Some having to deal with being openly questioned in meetings about the validity of their qualifications. Examples of unconscious bias and micro aggressions were common for this group.

There was an overall feeling of being overwhelmed and burned out from dealing with their actual job which included running global teams, the smallest of which was 60, but also the exhaustion from the **"other side"** of the job and feeling they needed to protect their position. These leaders felt many eyes were on them, waiting in the wings for one mistake, as justification to remove them from their position. Some even being asked by supervisors to **"mentor"** other less qualified individuals who were openly jockeying for their position. Underrepresented individuals at this level felt they had to always be on guard. Female MiC Directors™ had an additional responsibility of walking a line of being **"too nice"** or being a **"bitch"**, being **"too emotional, angry, smiley"** etc. There was an emotional element to perception of female Directors which did not exist with their male counterparts.

As it relates to their teams, although there was diversity globally, it did not translate to the U.S., with female team members hovering around **10%** and people of color around **5%**. They did not feel their companies did a good job training their direct reports and below, reserving the leadership training for those at the Director level or above. These leaders also stated HR and recruiting were in the most important position to assist with their diversity hiring initiatives. However, they did not feel like they were being assisted by those teams and were not aware of any DEI training available for HR or recruiting.

When asked if these MiC Directors™ received access, direction, or training about how to transition as cybersecurity subject matter experts for nonprofit, private, or public Boards of Directors the answer was a resounding **"no."**

MiC Directors™ Observations

Few and far in between makes for a lonely existence. These professionals are often literally the **ONLY** underrepresented person at their level in their companies and are being asked to perform herculean tasks, to solve problems they did not create. The pressure they are under to do more than their white male peers when it comes to helping with DEI takes its toll. Many of those who decide to take on DEI initiatives are sometimes equated to nothing more than the **"diversity hire"** and not given credit for their subject matter expertise in the cybersecurity field.

This lack of respect often leads to the inability to ascend to the Chief Information Security Officer (CISO) level which limits Board opportunities, as many of Board opportunities are sourced from C-Level Executives. The most recent statistics found regarding underrepresented CISOs in Fortune 500 [1] companies **17%** identify as Women, **6.6%** are Hispanic or Latino, **6.5%** are Asian and **3%** are Black/African American.

Conclusion

The very fact that there are so few MiC Directors™ out there is a problem in of itself. The fact remains that at every level of their career underrepresented cybersecurity talent has to deal with so much more than just the job. It is my opinion and experience that because we operate at a level of social insecurity, we are almost always overly qualified for a role. Whether it is through degrees, certifications, etc. we would not be in a role if we were not capable, but it seems these biases, that we are not **"enough"** remain. We have a pipeline problem because we do not promote well qualified individuals into leadership roles and backfill them with capable professionals. No clear job descriptions for MiC Aspirers™ equals limited opportunities for MiC Builders™ equals smaller number of MiC Communicators™ in the pipeline, which equates to limited MiC Directors™ which totals little to nonexistent representation on Boards of Directors.

There are plenty of growth and engagement opportunities to be had between minority cybersecurity professionals and organizations looking for them. Luckily, there is not just one way to tackle the underrepresented talent in the cybersecurity industry problem, just like there is no silver bullet solution to solve all your cybersecurity risks. **“Defense in Depth”** is a concept most cybersecurity professionals are familiar with; it means if you are attempting to solve a cybersecurity problem you build defenses in multiple ways. Our proposition is **“DEI in Depth,”** and you need multiple ways to solve a known issue.

From this study what we found were many addressable miscommunications between both sides. Our study found opportunities and multiple techniques to increase representation starting with clear job roles, titles, and descriptions, as well as defined employee career paths which explain what is required for promotion. Another thing, from the beginning, if the certification is not needed for the role, it is acting as a barrier to entry to those talented professionals who may have opted for a degree or just do not have the extra money to spend on what amounts to **"window dressing."** Human resources and recruiters, also need training on how to effectively source for underrepresented cybersecurity talent.

There is an obvious need for leadership training at all levels. Transparency on the **“how”** and not hiding opportunities for advancement and leadership development at **“secret levels.”** On both sides of the equation there are barriers to be broken down for a successful relationship between organizations and their underrepresented talent.

In the end of all we found were new opportunities to do better and actionable ways to move forward. We must do the hard work!

[1] https://www.zippia.com/chief-information-officer-jobs/demographics/

About

Mary N. Chaney

Mary N. Chaney, Esq., CISSP, CIPP/US, has over 25 years of progressive experience in the fields of Information Security, Privacy, and Risk Management. She is currently the Chairwoman, CEO, and President of Minorities in Cybersecurity, as well as the Founder and CEO of its subsidiary, MiC Talent Solutions.

Stay connected!

Minorities in Cybersecurity

@MinoritiesInCybersecurity
@MiCLeadership
@mincybsec
@minoritiesincybersecurity

TALENT SOLUTIONS

@MiCTalentSolutions
@Talented_MiC
@mictalentsolutions
@talented_mic

Minorities in Cybersecurity, Inc. (www.mincybsec.org) is a 501(c)(3) nonprofit organization focused on the leadership development of underrepresented cybersecurity talent. The mission of MiC is to provide practical knowledge, training, and support to our members with the sole purpose of preparing them to become the next generation of global cybersecurity leaders.

MiC Talent Solutions, Inc. (www.mictalent.solutions) is a fully owned subsidiary of Minorities in Cybersecurity, Inc. (MiC) that provides cybersecurity recruiting, direct hire, augmented staff, and professional service contracting solutions for organizations searching for minority, women, and non-binary cybersecurity talent.