Tips from the Top: Corporate Security Leaders Share How to Build a Team Today That's Fit to Tackle Tomorrow's Risks

Did you know that in 2021 the global estimated shortage of cybersecurity professionals was 2.72 million[1]? Today, according to a study by (ISC)2, the global cybersecurity workforce gap has increased to 3.4 million people[2].

Staff shortages are an all-to-familiar problem for corporate security teams, which is getting more complicated to solve. The skills needed to do these jobs are expanding because corporate security teams perform more duties outside their traditional security role.
For example, during the pandemic, some corporate security teams became the de facto health and safety officers charged with keeping employees safe wherever they were working.

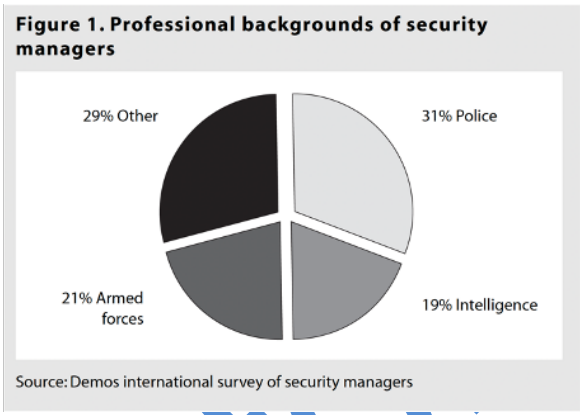
Corporate security teams are adjusting to new sophisticated threats from bad actors – both individual and state-sponsored. Plus, teams are creating new innovative threat-response strategies because of geopolitics, economic uncertainty, and rising political tensions. One strategy recruiters are trying is how and where they find new talent.

New corporate security job descriptions require candidates to have more soft skills, like business acumen, effective communication, and traditional security experience. According to a

[1] National Institute of Standards and Technology, *Cybersecurity Workforce Demand, 2021*.
[2] (ISC)[2], 2022 Cyber Workforce Study, The Cybersecurity Workplace Evolves as Staff Shortages Grow, 2022

report by Demos that surveyed heads of security, 22% had some form of business experience before assuming their current role.

Additionally, recruiters are searching for candidates with diverse career backgrounds. For example, Demos' report shows that nearly three out of four security professionals come from a law enforcement background. (See figure 1)



Demos' report also showed a lack of gender diversity among talent pools. Rachel Biggs, an author of the report, says that 94% of candidates globally for the industry are men. Female candidates within the U.S. are mostly non-existent, with 3% of applicants being women.

Arian Avila, Vice President of Security Operations and Solutions at Capital One, shared that some of the best teams she's worked with are an "amalgamation of different backgrounds and experiences."

"We had an opera singer, a graphic designer, and a biochemistry major," Avila said. "We had somebody with no college background that came [to the team] after doing customer service the whole time."

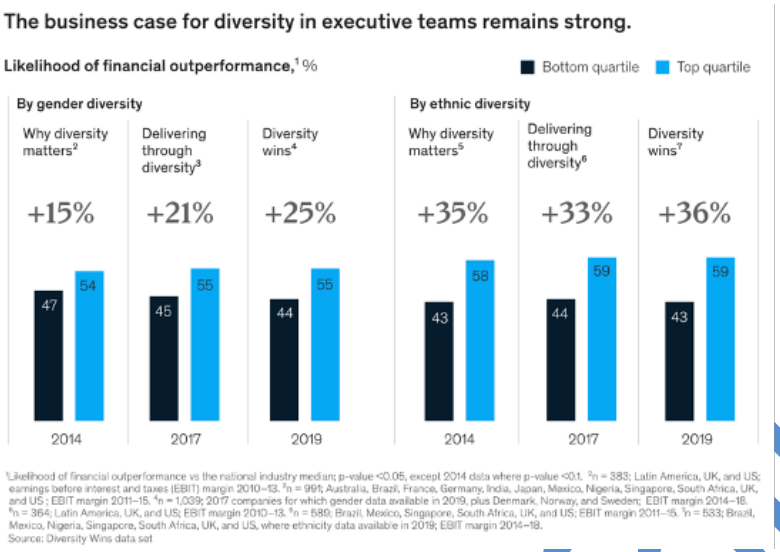
Corporate security teams recognize that diversity in experience and ethnicity is critical, and they've realized that diversity in thought is also essential.

"I'm always looking for diversity in all of its different shapes, colors, sizes, and everything. But one of the things I tend to crave is diversity in thought," Dr. Lewis Eakins, Vice President of Public Safety and Emergency Preparedness at Ivy Tech Community College System, said. Eakins continued by saying that the lack of thought diversity can encourage groupthink and unconscious bias that may negatively impact the team's success.

Avila echoed his thoughts saying, "Surrounding yourself with just different experiences and life experiences forces the team to come up with really creative solutions, especially when you're in a time of crunch."

Diversity, equity, and inclusion (DE&I) is more than a buzzword. Research shows a correlation between a company's diversity and revenue.

A 2019 analysis by McKinsey & Company reveals that companies with diverse gender and ethnic backgrounds are 25% more likely to have above-average profitability.



[1]Likelihood of financial outperformance vs the national industry median; p-value <0.05, except 2014 data where p-value <0.1. [2]n = 383; Latin America, UK, and US; earnings before interest and taxes (EBIT) margin 2010–13. [3]n = 991; Australia, Brazil, France, Germany, India, Japan, Mexico, Nigeria, Singapore, South Africa, UK, and US; EBIT margin 2011–15. [4]n = 1,039; 2017 companies for which gender data available in 2019, plus Denmark, Norway, and Sweden; EBIT margin 2014–18. [5]n = 364; Latin America, UK, and US; EBIT margin 2010–13. [6]n = 589; Brazil, Mexico, Singapore, South Africa, UK, and US; EBIT margin 2011–15. [7]n = 533; Brazil, Mexico, Nigeria, Singapore, South Africa, UK, and US, where ethnicity data available in 2019; EBIT margin 2014–18.
Source: Diversity Wins data set

Along with attracting new talent, retaining them is another critical factor for building the security teams of tomorrow. And it's becoming more challenging because security professionals face new pressures.

As reported by VMWare in its Global Incident Response Threat Report: Weathering the Storm, nearly 47% of cybersecurity and incident response professionals said they had experienced burnout or extreme stress in 2022. That same report revealed that 69% of respondents experiencing burnout symptoms are still considering leaving their jobs – up 5% from 2021.

Sandy Perez, Intelligence Analyst at Alcon, said an effective way to retain top talent is by designing a clear pathway for career growth. "Having those growth and development opportunities, sometimes even flexibility with schedules is really helpful in retaining [talent], especially in the post-COVID world," she said.

She continued to share that she regularly checks in with her teams to see "what's working, what's not working, and to gauge where your team is at and what we need to develop."

Another way leaders are building teams today to tackle tomorrow's risks is by tying the team's impact to the company's revenue.

Keith White, Chief of Safety and Security at Salesforce, coaches his team to connect any security initiatives to the company's core business objectives.

"Everything that we do should have some type of relationship to something that [the board] sees as a top priority," White said. "And it promotes relevancy for your organization."

Ontic's Executive Director of Threat Management, Marisa Randazzo, agrees that today's corporate security teams must illustrate how their initiatives impact a company's business objectives.

"Modern corporate security teams need to have the awareness and knowledge about the business aspects their programs support," Randazzo said. "Understanding how board members think regarding business outcomes and avoiding typical industry acronyms allows others to understand how important your team is to the business."

Avila reiterated the importance of connecting the team's outcomes to a business objective.

"Pay really close attention to what's happening economically and in your business," she said. "Because it may not be the time to pitch that brand new role that's going to be transformative. Maybe now is the time to just hire somebody that's going to help me nail the basics."

Avila also advised on how leaders can build a security workforce for tomorrow. "I think [it] needs to reflect the skills and competencies that are necessary to meet the demands of the dynamic and ever-changing business environment."

Forming a corporate security team that can meet tomorrow's threats is challenging. Leaders must consider multiple things to build their teams, including DE&I, soft skills, business acumen, and the mental agility to handle the extreme pressure from the industry.

Ontic is helping companies navigate the new complexities of building and training the security team of tomorrow. Check out our resource library focused on the security teams of tomorrow.