Building Resilient Cybersecurity Teams

IBM's Approach to Talent Management and Retention

Rosa Bolger
Vice President Cyber Defense
and Technology at IBM

With a global team of 400 cybersecurity professionals protecting 240,000 IBM employees, Rosa Bolger, Vice President of Cyber Defense, understands that cybersecurity talent management requires a unique approach.

"In cybersecurity, you work under crisis conditions 90% of the time," says Bolger. "You need to be very good at crisis management, working under pressure, and have specialized skills, especially in forensics and investigation."

Unlike other IT fields, cybersecurity requires continuous threat assessment and strategy adjustments. "You are the first line of defense, always tuning your security posture and defense strategy to the evolving threat landscape. It is an exciting space."

A Fresh Look at the Talent Challenge

Rather than viewing the cybersecurity talent gap as a numbers game, IBM emphasizes key behavioral qualities: crisis management, resilience, and "The biggest quality we look for, beyond IT expertise, is being analytical and determined," Bolger notes. "Success depends on building strong relationships and maintaining clear communication."

IBM's innovative strategies include apprenticeship programs that train professionals from various career backgrounds, including education, military service, and IT. In Singapore, for example, IBM trained 5,000 professionals through a government partnership. "Some of our top talent today started with completely different backgrounds. They bring fresh perspectives and, combined with technical training, they have become exceptional cybersecurity professionals."

Keys to Attracting and Retaining Top Talent

IBM acknowledges that retention is the real challenge in cybersecurity due to the high-pressure workload. The company addresses burnout with flexible work schedules: teams working four 10-hour days for four days get three days off to decompress. AI and automation increase efficiency and reduces the manual workload.

"Retention is an art because of the constant pressure. You must develop the right work environment and hire people with genuine passion for what they do." IBM also empowers managers to adjust schedules and workloads to address employee work-life balance.

IBM's 2025 SOC Initiative

To ensure cybersecurity professionals continue the development of their comprehensive skills, IBM is implementing an initiative requiring cybersecurity roles to spend two weeks a year working in the SOC. "It resets you; it reminds you of the problem statement, says Bolger. This experience enhances problem-solving skills, policy development, detection capabilities, and automation. It brings clarity to the mission, trains our people, and develops team culture, all of which positively impacts mission success."

"Retention of cybersecurity talent is an art because of the constant pressure."

Building a Future-Ready Security Team

IBM recruits veterans due to their crisis management and mission-critical experience. "In our space, especially in SOC and CSIRT, a good number of our people have served in the military. Veterans bring a broad range of skills to our teams, not just in demographics but also in experience and perspective."

Additionally, IBM partners with community colleges to source motivated talent and offers free cybersecurity training through the IBM SkillsBuild program.

Strengthening Teams in an Evolving Landscape

"The struggle isn't finding candidates, it's retaining them," Bolger emphasizes. IBM recognizes that recruiting is only the first step. To support long-term retention, the company offers resources like comprehensive support systems. These initiatives go beyond simple networking, creating communities that provide understanding and targeted skill development opportunities.

IBM's mentorship culture ensures mid-to-senior-level professionals work with three to five mentees, focusing on technical skills and career growth. "A good mentor highlights the mentee's strengths, helps them showcase achievements, and guides them on accelerating professional growth."

AI: Enhancement, Not Replacement

IBM sees AI as an augmentation tool, not a replacement for human talent. Junior team members use AI to accelerate their professional development and enhance their threat detection skills. "I see AI augmenting our staff's capabilities to respond faster and with better accuracy," Bolger states.

Final Takeaway

IBM's approach proves that cybersecurity talent challenges are not just a numbers game but about creating an environment where professionals can grow, contribute, and thrive.

Through training, hands-on experience, AI integration, and mentorship, IBM is building a resilient cybersecurity workforce.

This Case Study is Just the Beginning – Download the 2025 Cybersecurity Workforce Research Report for More Insights!

This case study is part of the *2025 Cybersecurity Workforce Research Report* published by SANS | GIAC. Informed by international survey results, the report delivers key insights on how HR and Cybersecurity Managers can collaborate to successfully build high-performing cybersecurity teams.

Download for More Insights