accenturesecurity

# ACCENTURE CYBERSECURITY FORUM

## THREE PERSPECTIVES TO CLOSE THE SECURITY TALENT GAP

**Virtual Roundtable Summary**
**January 16, 2020**

**On January 16, the Accenture Cybersecurity Forum (ACF) convened virtually for a 60-minute roundtable, "Three perspectives to close the security talent gap." CISOs and cybersecurity executives from multiple industries and organizations joined the call to discuss the cybersecurity talent shortage and how organizations are building more diverse teams.**

Building diverse cybersecurity teams benefits both the enterprise and the larger CISO community. CISOs compete with each other for talent, but should also be expanding and enriching the talent pool. That will require promoting greater gender diversity.

Our three subject-matter experts were a CISO of a financial services company; an HR executive in the Accenture CISO organization; and a cybersecurity talent advisor and author. The session was hosted by ACF Chair Andy Vautier, Accenture CISO.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

## CISO/CHRO collaboration

When the leaders of cybersecurity and human resources are aligned, the odds of closing the security talent gap improve significantly. At Accenture, for example, the CISO organization has a dedicated HR lead who is helping to implement a variety of initiatives to attract, develop and retain cybersecurity talent and promote gender diversity across the organization. These initiatives include:

- Fostering a close-knit leadership team that shares common goals and is committed to getting to know the people on their teams.

- Running internship and apprenticeship programs to fill the talent pipeline.
- Offering a robust training and certification program for all employees.
- Managing a women's program that features a variety of monthly events, sometimes with outside speakers, and a newsletter.
- Conducting a formal performance review process that helps employees track their career progress and identify the additional skills they need to succeed.

Most importantly, promoting growth and diversity is woven into the fabric of Accenture's security practice, and this focus is reflected in daily activities. There is tremendous value in having a program that is visible and explicit. Accenture has specific goals in terms of recruitment, retention, training and diversity. Leaders are visible in their support of the goals.

Several participants affirmed the effectiveness of having HR support embedded within the cybersecurity team. HR professionals learn about the team's strategy, challenges and roadmap, and act as partners. An HR/CISO partnership at Accenture, for example, is key to lower attrition and greater diversity.

## The value of diversity

Male CISOs may unknowingly "recruit in their shadow," hiring other males with a military, intelligence or STEM background. The preponderance of similar types of people in the cybersecurity industry can limit what Winston Churchill coined "corkscrew thinking" skills—the ability to see things in different ways, develop creative solutions and avoid being blindsided.

An "environment of many perspectives" increases an enterprise's collective intelligence. Attracting more women to careers in cybersecurity can diversify perceptions, ideas and reactions. The book ***InSecurity: Why a Failure to Attract and Retain Women in Cybersecurity Is Making Us All Less Safe*** cites a number of research studies about the value of diversity. Compared to more homogenous teams, diverse teams tend to be more productive, innovative and successful in meeting targets; achieve a higher level of performance; and have more composure and a sharper perception of risk. Collaboration among people with diverse thinking styles can increase our ability to see all risks, map out effective scenarios of response, and beat our adversaries.

## Technology tools to close the talent gap

One enterprise is deploying what the CISO described as a “version 1.0” automated career pathing tool that enables cybersecurity employees to assess their skills, experience and progress in defined career paths. It is not a performance management tool; in fact, managers do not have access to an employee’s input. The tool’s output assists employees in framing discussions about obtaining the skills they need to progress to the next level—and helps them envision a future at the company. The tool has served as a foundation for identifying and nurturing talent outside the traditional cybersecurity talent pool.

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181) establishes a taxonomy and common lexicon that describes cybersecurity work and workers. The framework can be used to help define categories, specialty areas and work roles in the enterprise. With a taxonomy in place, an organization can incorporate career experiences and “soft skills” to define potential career paths for employees.

## ACTIONS TO INCREASE DIVERSITY

Participants agreed that conscious efforts are needed to promote diversity in the cybersecurity field. CISOs can promote diversity in their organizations in a number of ways:

- **Set goals and objectives.** Retaining top talent requires "data-driven conversations" about career progression. Develop specific goals and objectives, and hold people accountable to measure progress. Leverage every touchpoint with employees to communicate messages that support your diversity goals.
- **Audit your team.** Identify the talents you have and those you need to add to the team. Think broadly and across functions in identifying your talent pool, beyond only STEM disciplines.
- **Know your enterprise stakeholders** and identify who in the enterprise beyond HR can help you recruit and develop talent. For example, one CISO reported success in tapping into the call center to identify potential cybersecurity talent.
- **Be conscious of unconscious bias,** particularly within the HR department and among hiring managers. An implicit-association test can be useful to investigate gender bias, for example, that might be a barrier to considering potential employees from non-traditional talent pools.
- **Establish a structured interview process.** Get potential candidates in front of hiring managers earlier in the process. Build a database to assess recruitment success.
- **Set up new hires for success.** Establish programs for training, coaching and mentoring.
- **Be realistic about longevity.** Use exit interviews to understand why someone is leaving the enterprise, and keep the door open for a return. Several CISOs cited cases of bringing employees back after life events or short-term career changes.

## BEST PRACTICES

The discussion yielded several insights and recommendations to help CISOs and their organizations close the talent gap and promote diversity:

- **Build a broader, deeper talent pool.** Stop looking for unicorns and focus on finding employees with adjacent skills, motivation and a willingness to learn. Think broadly and across functions. Don't focus solely on people with STEM backgrounds.
- **Create a true partnership between HR and cybersecurity.** Embedding HR support within the cybersecurity team can be highly effective. HR professionals can learn about the team's strategy, challenges and roadmap, and act as partners. An HR/CISO partnership at Accenture is key to lower attrition and greater diversity. CISOs may also need to engage HR in new ways. Build a reciprocal relationship by understanding how the HR team works, asking how you can help them.
- **Engage HR in new ways.** Build a reciprocal relationship by understanding how the HR team works and asking how you can help them. Counteract any risk aversion by communicating that you are receptive to considering candidates who may not upon first impression look like a perfect fit.
- **Keep an open mind about women's career paths.** Provide women with opportunities across the cybersecurity career spectrum, both technical and non-technical. Women need to have the opportunity to learn the technical aspects of cybersecurity and to have training, sponsors and mentors throughout their careers.

## CONCLUSION

In closing, Vautier reinforced that "more diversity drives more innovative and successful cybersecurity outcomes." Set goals, communicate expectations, and lead the effort to attract and retain diverse talent.

## CONTACT

**ANDY VAUTIER**
Accenture CISO
Accenture Cybersecurity
Forum Chair

## ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 505,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at **www.accenture.com.**

## ABOUT ACCENTURE SECURITY

**Accenture Security** helps organizations build resilience from the inside out, so they can confidently drive innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown.

Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

**Visit us at www.accenture.com**

**Follow us @AccentureSecure**

**Connect with us**