August 06, 2013

Cybersecurity threats: A people problem HR can solve

Maya Yankelevich, Senior Human Capital Consultant

Combatting cyber threats is not just about having the right technology, know how or preventative foresight. It is about an acute labor shortage. Widespread concern over the lack of talent available to fill cybersecurity roles has been building and the gap is only expected to increase.

In 2012 The Washington Post reported that the public and private sector will need to fill 50,000 cybersecurity jobs in the near future. The Pentagon alone plans to grow their cybersecurity force from 900 to 4,900 military and civilian personnel over the next several years, reported the Post in early 2013. Although numerous efforts have started in recent years to increase student interest in the field, the cyber threat will not wait until the new wave of cyber warriors is ready to take position. For HR professionals, this threat will require a new look at how cyber professionals are identified, hired and trained.

Reconsider the status quo

Organizations must take a hard look at their hiring and workforce development practices. In InformationWeek’s 2013 IT salary survey report of security professionals, they note that hiring professionals will need to continue educating themselves regarding how to identify, recruit and hire cybersecurity professionals. Currently, there is an overreliance on certifications and degrees and such requirements may preclude highly qualified individuals from ever being considered for a position.

Consider the fact that no one is screening attackers of our networks to see if they have a piece of paper confirming their credentials to be a serious cyber threat, yet they are still developing and launching sophisticated attacks! As hiring professionals, we may be focused on the wrong qualifications; a more progressive, and possibly liberal, approach to recruitment and selection may be necessary to ensure the most qualified candidates apply for these positions.

While education still is and should be a critical component, consider all of the backroom hackers and gamers majoring in subjects unrelated to information security or computer science. There are plenty of people with an innate interest and ability in cybersecurity related subjects who may never consider a career change or redirection without the right incentive. Organizations should take advantage of these opportunities to engage students and pave the path for ongoing relationships.

Numerous cyber competitions are held every year for high school and college students. This is a great place to identify future employees. Of course, matching rewards to unique interests of these non-traditional employees is crucial. Typical rewards may not be as meaningful as the opportunity to help solve complex security problems or time to "play" with new techniques or approaches.

Redeploy your current staff

Although the supply of potential cyber warriors is limited, all hope is not lost. Now it is essential for organizations to assess current employees' cybersecurity skills, identify cybersecurity potential and train those with the ability to fill critical roles.

In a report to the President from the Center for Strategic and International Studies on cyber issues, policy experts noted, "While billions of dollars are being spent on new technologies...it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success." Although it is not possible to create more people to fill the growing number of cybersecurity positions, it is possible to train and educate current employees to fill those gaps.

A broader perspective that encompasses all critical aspects of people, process and technology is required to attain a state of resilient cyber readiness. As recently noted in a DHS Cyber Skills Task Force Report, organizations require a model for assessing the competency of the cybersecurity workforce to identify current and potential talent and to target training for employees across the full cybersecurity lifecycle.

The National Cybersecurity Workforce Framework is an ideal starting point, as it defines cybersecurity specialty areas, typical tasks, and knowledge, skills, and abilities necessary for successful performance. Organizations need an innovative assessment and development program that leverages public and private sector best practices to build the cybersecurity workforce.

A two-phase cyber workforce management strategy should allow organizations to identify current capabilities and competency gaps, target training to address overall gaps as well as target training to the right people at the right time and forecast needs and plan for workforce growth and development.

Phase One: Organizational Competency Assessment. This provides a comprehensive assessment of the organization's current cybersecurity competence that is used to baseline existing capability and to identify critical skill gaps. The Organizational Competency Assessment is completed on a periodic basis (e.g., every 2 years) in order to track progress and ensure readiness to respond to ever-changing cyber threats.

Phase Two: Individual Cybersecurity Skill Assessment. This objective cybersecurity skill assessment is a more precise measure of capability and may be used at an individual level to select people into positions and tailor training programs to ensure specific skills are acquired for particular roles. Simulated cyber threats are used to provide a realistic, immersive assessment experience. Characteristics related to success in cybersecurity environments are assessed to ascertain individuals' potential to achieve in cyber roles. Results may be used for selection of new hires, diagnosis of strengths and development needs for individual development planning or an evaluation of training effectiveness.

Reinvigorate your thinking

Meeting the cybersecurity workforce challenge appears daunting, yet HR professionals must address it head on with innovative workforce planning and development strategies. Novel solutions to this crisis include identifying how to attract and hire nontraditional applicants and how to leverage the existing talent pool in nontraditional ways (i.e., assessing and training to take on cyber roles). Tremendous action is required, and only bold thinking will yield the necessary results.

Maya Yankelevich is a Senior Human Capital Consultant for PDRI, a CEB company. She has consulted with numerous public and private sector organizations in the areas of talent management, leadership development, and workforce planning, particularly in times of critical change and transformation. She led the PDRI team that developed the National Cybersecurity Workforce Framework for the National Initiative for Cybersecurity Education (NICE). For more, visit www.pdri.com.