Human Capital Challenges in Cybersecurity

The costs of cybersecurity breaches are staggering. A recent estimate placed the average cost to an organization hit by a cyberattack at about $3.9 million, with the costs of mega breaches (breaches of 50+ million records) approaching $350 million.[1]

The danger is clear, and yet the threat seems to have caught many organizations flat-footed. Consider the following:

- Hundreds of thousands of cyber jobs in the U.S are currently vacant.
- Postings for cyber jobs take longer to fill than postings in general.
- Many cybersecurity experts warn that employees present as much of a threat as outside hackers.

These figures illustrate a stark reality: the cyber threat is a people challenge. Our work has helped organizations recruit and hire the people who can help prevent cyberattacks and has also led to a better understanding of who is likely to perpetrate such attacks.

Growing Cyber Talent

HumRRO's expertise includes every part of the cyber talent equation: understanding the requirements of cyber jobs, helping students and employees match their skills to those requirements, and finding the right people to fill cyber jobs.

Understanding Cyber Jobs. We have gained rich insight into cyber job requirements through a variety of sources. As one example, we conducted a comprehensive job analysis of the special agents who work in the cyber field for the Federal Bureau of Investigation (FBI). Additionally, our work helping populate the Occupational Information Network (O*NET) affords us an ideal opportunity to understand the fundamentals of cyber occupations.

Exploring Cyber Careers. Over 80% of millennials report that no high school teacher or guidance counselor ever discussed cyber careers with them.[2] Our career exploration work helps close this gap. We played a central role in creating YouScience's Latitude system—a groundbreaking online tool that helps students identify their interests and aptitudes and find college majors and occupations that fit them, including cyber careers. We also developed federal career exploration systems that allow users to assess the fit between their education, experience, skills, and interests and hundreds of different occupations, again including cyber.

Assessing Cyber Talents. In the coming years, the cyber workforce is expected to grow at four times the rate of other fields and double the rate of information technology fields in general.[3] We understand how to effectively assess the talents needed for cyber jobs using methods ranging from innovative rich-media simulations to more traditional knowledge- and ability-based assessments. We developed a knowledge test to select entry-level cyber professionals for the U.S. military that is currently being administered to tens of thousands of applicants a year.

> *Understanding how people perpetuate a cyber threat is important. However, understanding why they engage in damaging cyber behavior is equally critical and often overlooked...*

In addition, HumRRO is currently part of a team supporting the Department of Homeland Security (DHS) in hiring and retaining the next generation of cyber professionals. For this effort, we are developing proficiency assessments for multiple cybersecurity positions.

Unlocking the Cyber Threat Mindset

We have also been instrumental in helping organizations identify "insider threats"—employees who steal confidential data or sabotage critical information systems. HumRRO has contributed to the development of models for predicting and detecting malicious insider attacks through projects funded by the Defense Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Agency (IARPA).

Understanding how people perpetuate a cyber threat is important. However, understanding why they engage in damaging cyber behavior is equally critical and often overlooked by cybersecurity professionals. Our research on insider threats has found the following:

- People with a certain personality profile are particularly likely to potentially engage in malicious cyber behavior.
- Personality data is not enough to predict insider threats. More often than not, dynamic situational or environmental factors serve as triggers (e.g., life or work stressors), increasing the risk of insider attacks.

Our insider threat work involves complex statistical analyses, including Bayesian analyses, data simulations, and structural equation models. These tools are examples of our rich quantitative technical expertise, which allows us to formulate unique and creative approaches to thorny measurement and assessment challenges.

We are well-known for our technical rigor, integrity, and collaborative approach to working with clients in the cyber domain and beyond. Our research and methodological expertise, coupled with a deep understanding of the environment, constraints, and vision of our client organization allows us to work in partnership to create effective solutions.

---

[1] *2018 Cost of a Data Breach Study* (Ponemon Institute, under sponsorship by IBM Security)
[2] *Preparing Millennials to Lead in Cyberspace* (Raytheon)
[3] *Bureau of Labor Statistics Occupational Outlook Handbook* (retrieved on 21 February, 2019; https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.html)

For more information contact:

DAVID DORSEY, Ph.D.
Vice President,
Business Development Division
phone: 703.706.5670
e-mail: ddorsey@humrro.org

Visit **HumRRO.org** for additional information about all our services.

HumRRO was established in 1951 and is an independent, nonprofit corporation dedicated to the development and application of state-of-the-art scientific principles and technologies to solve the real-world challenges facing private and public sector organizations and educational institutions. Our professional staff is composed of psychologists with diverse expertise in: personnel selection, classification, and promotion; education assessment and accountability; strategic human capital management; program evaluation and policy analysis; employee development and training; credentialing; modeling and simulation; and survey research. Our client base includes the military, government agencies, private industry, and professional associations. HumRRO is an industry leader in working collaboratively with clients to create customized, best-practice solutions.

REV: 03/2019