KRC Research conducted a national survey of 250 senior information technology (IT) decision makers from March 23 to April 4, 2018. The survey was conducted online. All respondents have responsibility for (or are part of a group that shares responsibility for) recruiting, interviewing, and hiring cybersecurity talent at their companies. Respondents work in a wide range of industries and sectors, including banking, telecommunications, healthcare, government, and defense. Key findings from the survey include:

1. **C-SUITE EXECUTIVES, BOARDS OF DIRECTORS, AND INVESTORS ARE HIGHLY CONCERNED ABOUT THE RISK OF CYBER THREATS—AND INVESTORS ARE INCREASINGLY HOLDING SENIOR EXECUTIVES ACCOUNTABLE.**
   - Most (61%) view cybercrime as a high risk within their industries or sectors, and nearly half (47%) view the risk to their own companies as high.
   - Senior IT decision makers report high levels of concern among C-suite executives (62%), followed by investors (57%), and company boards of directors (55%).
   - Three-quarters (74%) report that investors are increasingly holding senior executives accountable for a cyber incident.

2. **MOST SENIOR IT DECISION MAKERS HAVE TALENT GAPS—AND FILLING CYBER TALENT JOBS IS A HIGH PRIORITY. BUT FINDING AND HIRING EXPERIENCED NEW TALENT IS DIFFICULT AND COMPETITIVE.**
   - While most senior IT decision makers are at least somewhat confident they currently have appropriate levels of cybersecurity talent to protect their company from a cyberattack (94%), most also say they have immediate talent gaps to fill (83)—and the jobs they need are the hardest to fill: experienced/specialized positions (56%) and mid-level positions (36%), compared to junior positions (4%).
   - These gaps, they report, are putting added stress on current cybersecurity staff (90%). In fact, nearly half (45%) report that employees work longer hours.
   - Considering this stress, 53% of senior IT decision makers say that hiring cybersecurity talent at this particular time is a high priority.
   - Employee retention (58%) and hiring new talent is currently difficult (72%). Hiring difficulties usually stem from challenges finding candidates with strong experience (53%) and an absence of trained talent with a specialty skill set (40%).

3. **COMPANIES HAVE SHORT-TERM SOLUTIONS IN PLACE TO MANAGE THE GAP.**
   - In addition to having staff work longer hours, senior IT decision makers report using tools and software to compensate or offset cybersecurity talent (56%), training non-cybersecurity employees outside of their role (52%), and outsourcing (32%).
4. COMPANIES RECOGNIZE THE RISKS ASSOCIATED WITH UNDERSTAFFING, BUT THEY ARE A STEP BEHIND WHERE THEY NEED TO BE TO PREVENT AND DEFEND AGAINST CYBER ATTACKS. MANY DO NOT APPEAR TO FULLY RECOGNIZE THE BRAND REPUTATION RISK.

- Most senior IT decision makers recognize risks inherent in understaffing cybersecurity talent—including being more vulnerable to cybercrime and theft (40%) because staff and existing tools cannot consume the inputs to uncover all threats (29%), nor invest time in continuing education to keep up with the latest threats (26%). This fosters high levels of staff stress (34%) and turnover related to burnout (29%), making recruiting more difficult (28%). Finally, the ultimate danger is to the company’s reputation (29%) and brand damage (19%).

5. AS THE MARKET BECOMES INCREASINGLY COMPETITIVE, COMPANIES ARE OFFERING INCENTIVES TO BOTH RETAIN CURRENT AND HIRE NEW CYBERSECURITY TALENT—but this spiral is putting the pressure on for better benefits, better recruiting and hiring processes, and training.

- To hire cybersecurity employees, companies are offering competitive compensation and benefits (54%), investing continuously in the latest cyber technologies (51%), and paying for professional certifications and association memberships (47%).

- When it comes to retaining cybersecurity employees, companies are offering similar incentives, including investing continuously in the latest cyber technologies (47%), offering more competitive compensation and benefits (47%), and paying for professional certifications and association memberships (42%).

- When asked what additional strategies their company needs to put in place, senior IT decision makers say they need to offer enhanced benefits (31%), improved hiring (16%) and recruiting (14%) processes, a better work environment where people feel valued (14%), and more training (9%) and advancement (5%) opportunities.

6. MOST THINK STAFFING WILL BECOME EVEN HARDER. THEY SUGGEST INTRODUCING PEOPLE TO CYBERSECURITY CAREER OPPORTUNITIES IN THEIR FORMATIVE HIGH SCHOOL AND COLLEGE YEARS.

- Over the next 5 years, most expect hiring to get even more difficult than it is now (57% more vs. 15% less); 26% think it will stay at the same level of difficulty.

- For the long term, most suggest introducing the world of cybersecurity to an up-and-coming workforce at a young age: in high school (42%) or in the freshman or sophomore year of college (20%).

About Booz Allen Hamilton

Booz Allen Hamilton (NYSE: BAH) has been at the forefront of strategy and technology for more than one hundred years. Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and not-for-profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.

With international headquarters in McLean, Virginia, the firm employs approximately 24,225 people globally, and had revenue of $5.80 billion for the 12 months ended March 31, 2017. To learn more, visit www.boozallen.com.

Media Contact

JOSEPH CAMPBELL
703-377-4422
campbell_joseph@bah.com