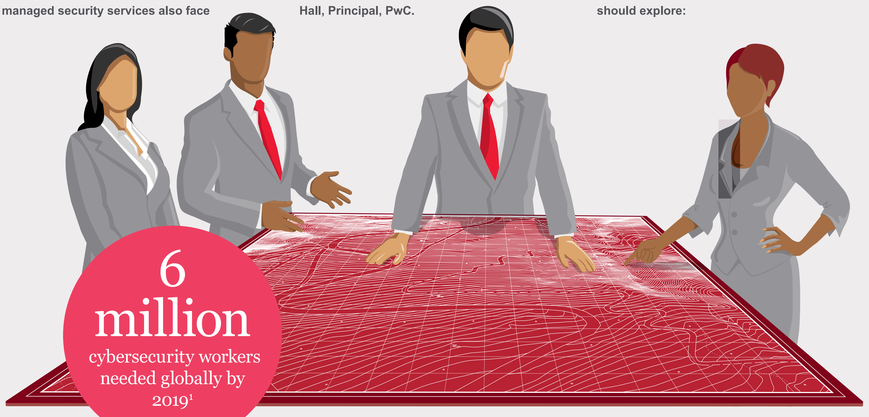
Cybersecurity Talent Gap

Navigating the skills shortage

The cybersecurity workforce gap will widen to 1.5 million job openings by 2019, up from 1 million last year worldwide, according to a recent report by Cybersecurity Ventures. Some tasks are being outsourced – 62% of respondents to PwC's latest Global State of Information Security Survey use managed security services for tasks including identity and access management and threat intelligence. Yet even with outside help (and managed security services also face a talent shortfall), organizations will lack the people they need to implement the most sensitive cybersecurity measures in-house. So what can companies do to help themselves? Certainly, the industry has never had a higher profile: "It's front of mind for all the boards and oversight committees we present to. They look at the news and frequently see a cybersecurity or related story," says Chris Hall, Principal, PwC.

Despite the publicity, are organizations giving cybersecurity the prominence it requires? Can existing staff be re-trained for cybersecurity roles – and do they want to work in this area? Does responsibility for expanding the pipeline of candidates lie squarely with private companies? And are companies looking broadly enough for the right candidates?

These are the areas organizations should explore:



6 million
cybersecurity workers needed globally by 2019[1]

Which skills are we looking for?

"You can find a good generalist who understands the frameworks of cybersecurity, but operating, improving and managing a specific technology? There's a big gap there," says Hall. "The technology landscape has exploded and there are a lot of point solutions on the market, so it becomes very challenging for existing resources to absorb these net new skills. "What we're hoping to see is large, enterprise-wide solutions taking on the areas that niche players are tackling. At present it's not uncommon for a client to have dozens of security technologies in place: they want to shrink the number of technology vendors in their environment and not only from the licensing and cost perspective, but from a talent perspective too. "If you're trained on one system and the vendor comes out with a new capability, conceivably it's easier to train on it because it has the same underlying framework."

How do we get the right graduates?

Successful programs have been a combination of private companies and academia - companies are providing insight to colleges and universities related to the areas into which it is difficult to find talent, and academia is developing the curricula to address the deficit.

Are we making cybersecurity an attractive career?

"Organizations do well when they raise the status of cybersecurity – when it becomes embedded in all aspects of their business," says Hall. "If you elevate it to the right level, people will feel they're important and they'll feel the work they do is valued by the organization and is meaningful." A company that values cybersecurity staff ensures they understand the business strategy, the IT strategy and the security strategy to support both. "You cannot do that stuck in a cubicle," he adds. "You've got to be ingrained in the whole business process." With an ever-changing threat landscape, ongoing investment in skills is also required. Regulated industries do better at this than those with fewer outside pressures, says Hall. Another reason to spend appropriately on keeping skills fresh? "Adversaries are continuously stepping up their game and have seemingly unlimited resources," he adds.

Are we looking for people in the right places?

Although cybersecurity incorporates a wide range of disciplines including threat assessment and risk management, operational roles require people with specific technology skills: "To run your operations center, you're more apt to recruit somebody who understands the technology and incident response than somebody who understands risk," says Hall. "Ideally the organization should be setting the tolerance for risk and the factors that mitigate and increase risk, and that gets applied as controls in the technology layer."

Cybersecurity recruiters may find themselves looking at a group of individuals other HR teams would avoid: people who have made a hobby of finding weaknesses in data security, a.k.a. hackers. However, Hall urges caution: "Not all the people who 'hack for fun' are malicious in intent, but you have to be extremely careful. There are ways to mitigate risk that don't involve solely attack and 'penetration testing,' also known as hacking, and companies are better served looking at these elements."

Beyond those essential technology skills, however, the cybersecurity industry has work to do to recruit a representative number of women and minorities: while women make up approximately half of college graduates, they represent just 11% of the global cybersecurity workforce, according to a recent (ISC)[2] Foundation and Executive Women's Forum study, sponsored by PwC. African-Americans, Asians and Hispanics account for less than 12% of information security analysts in the U.S., according to the Bureau of Labor Statistics.

Improving recruitment and retention among women and minorities would therefore provide a far wider cybersecurity talent pool. Practical steps that companies can take include:

- Reexamine how they recruit and include women and minorities in the interview process.
- Work with local universities, colleges and technical schools to communicate the company's interest in diversity. Doing so will help recruit new hires and develop a pipeline of educated professionals for the future.
- Pair new hires with strong role models and mentors within their organizations to build relationships and provide personal and professional support.
- Get involved in community IT programs and educational initiatives to promote the hiring of women and minorities.

11%
proportion of cybersecurity workers globally who are women, a number which has not changed for two years[2]

pwc

WSJ. Custom Studios is a unit of The Wall Street Journal Advertising Department. The Wall Street Journal news organization was not involved in the creation of this content.

[1] According to Michael Brown, former CEO at Symantec, the world's largest security software vendor
[2] (ISC)2 Foundation report

© 2017 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.