Cybersecurity Talent Gap
Navigating the skills shortage

The cybersecurity workforce gap will widen to 5.5 million job openings by 2029, 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 management.

Cybersecurity is a whole new deal (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. “With a flood of news 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 the 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 lie squarely with private companies? Are companies looking closely enough into the right candidates, including threat assessment and risk management? Operational risks require people with specific technology skills.

“The way you operate your company, you might want to oversee somebody who understands the technology and incident response more than somebody who understands risk,” says Hall. “Nearly the organization should be setting the framework for 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 grid that stretches for two years and beyond: 2019 and 2021. People will shift jobs based on pay and benefits, and what organizations choose to do to recruit a representative workforce, according to the Bureau of Labor Statistics. Analysts in the U.S., according to (ISC)² Foundation and Executive Women Inc., sponsored by PwC.

Cybersecurity recruiters may find themselves looking at a grid that stretches for two years and beyond: 2019 and 2021. People will shift jobs based on pay and benefits, and what organizations choose to do to recruit a representative workforce, according to the Bureau of Labor Statistics. Analysts in the U.S., according to (ISC)² Foundation and Executive Women Inc., sponsored by PwC.

“Organizations do well when they raise the stature of cybersecurity,” says Hall. “If you elevate it to the right level, people who feel they’re important and that they do the work they do get valued by the organization and is meaningful.” A company that raises cybersecurity to the right level understands the business strategy, the IT strategy and the security strategy to support both. “You cannot do that stuck in a silo,” he says. “You’ve got to be part of the whole.

Cybersecurity recruiters may find themselves looking at a grid that stretches for two years and beyond: 2019 and 2021. People will shift jobs based on pay and benefits, and what organizations choose to do to recruit a representative workforce, according to the Bureau of Labor Statistics. Analysts in the U.S., according to (ISC)² Foundation and Executive Women Inc., sponsored by PwC.

Beyond those essential technology skills, however, the cybersecurity industry needs to keep up its game and find people who can absorb these new skills.

There’s a growing talent shortage in cybersecurity, but operating intelligence. These are the areas organizations should explore:

**Which skills are we looking for?**

- A cyberwarrior who understands the frameworks of the industry.
- A cyberanalyst who understands the technology and is comfortable in the technology layer.

**How do we get the right candidates?**

- Software professionals have to be on top of a combination of private companies and universities — companies providing insight to colleges and universities related to the areas in which it is difficult to find talent, and academics is developing the curricula to address the deficit. If you’re trained on one perspective, but from a talent perspective too.

**Are we making cybersecurity an attractive career?**

- Organizations do well when they raise the stature of cybersecurity: when it becomes embedded at all levels of their business, says Hall. “If you elevate it to the right level, people will feel they’re important and that they do the work they do get valued by the organization and is meaningful.”

- A company that raises cybersecurity to the right level understands the business strategy, the IT strategy and the security strategy to support both. “You cannot do that stuck in a silo,” he says. “You’ve got to be part of the whole. Improving recruitment and retention among women and minorities is essential. At the same time, there is a need to bring in those with fewer outside pressures, industries do better at this than those with fewer outside pressures,” says Hall. Another reason to special appropriately on keeping talent fresh? Advancements are continuously coming up, their genes are undergoing substantial, unexpected changes, he adds.

**Are we looking for people in the right places?**

- Although cybersecurity incorporates cybersecurity to the right level, including threat assessment and risk management, operational risks require people with specific technology skills.

- “To run your operations center, you want more staff to oversee somebody who understands the technology and incident response more than somebody who understands risk,” says Hall. “Nearly the organization should be setting the framework for the factors that mitigate and increase risk, and that gets applied as controls in the technology layer.”

**Beyond those essential technology skills, however, the cybersecurity industry needs to keep up its game and find people who can absorb these new skills.**

- A cyberwarrior who understands the frameworks of the industry.
- A cyberanalyst who understands the technology and is comfortable in the technology layer.

**What we’re hoping to see is that niche players are solutions taking on the areas small companies can’t tackle.** At present it’s not because it has the same capability, conceivably it’s easier to train on it.

- What we’re hoping to see is that niche players are solutions taking on the areas small companies can’t tackle.

- You can find a good generalist who understands the frameworks of the industry.

- More than half of the active security analysts in the U.S., according to the Bureau of Labor Statistics, are women.

- Women make up 11% of the global cybersecurity workforce.

- At present it’s not because it has the same capability, conceivably it’s easier to train on it. Yet even with outside help (and private companies and universities related to the areas in which it is difficult to find talent, and academics is developing the curricula to address the deficit. If you’re trained on one perspective, but from a talent perspective too.

- What we’re hoping to see is that niche players are solutions taking on the areas small companies can’t tackle.

- You can find a good generalist who understands the frameworks of the industry.

- More than half of the active security analysts in the U.S., according to the Bureau of Labor Statistics, are women.

- Women make up 11% of the global cybersecurity workforce.

- Beyond those essential technology skills, however, the cybersecurity industry needs to keep up its game and find people who can absorb these new skills.

- A cyberwarrior who understands the frameworks of the industry.
- A cyberanalyst who understands the technology and is comfortable in the technology layer.

**What we’re hoping to see is that niche players are solutions taking on the areas small companies can’t tackle.** At present it’s not because it has the same capability, conceivably it’s easier to train on it.

- What we’re hoping to see is that niche players are solutions taking on the areas small companies can’t tackle.

- You can find a good generalist who understands the frameworks of the industry.

- More than half of the active security analysts in the U.S., according to the Bureau of Labor Statistics, are women.

- Women make up 11% of the global cybersecurity workforce.

- Beyond those essential technology skills, however, the cybersecurity industry needs to keep up its game and find people who can absorb these new skills.

- A cyberwarrior who understands the frameworks of the industry.
- A cyberanalyst who understands the technology and is comfortable in the technology layer.

**What we’re hoping to see is that niche players are solutions taking on the areas small companies can’t tackle.** At present it’s not because it has the same capability, conceivably it’s easier to train on it.

- What we’re hoping to see is that niche players are solutions taking on the areas small companies can’t tackle.

- You can find a good generalist who understands the frameworks of the industry.

- More than half of the active security analysts in the U.S., according to the Bureau of Labor Statistics, are women.

- Women make up 11% of the global cybersecurity workforce.

- Beyond those essential technology skills, however, the cybersecurity industry needs to keep up its game and find people who can absorb these new skills.

- A cyberwarrior who understands the frameworks of the industry.
- A cyberanalyst who understands the technology and is comfortable in the technology layer.