

Government & Higher Education 5x5 Cyber Change series:
A five-minute read to inspire new ways of thinking about cybersecurity

Re-imagining the future of cyber workforce



As the cybersecurity talent shortage continues, organizations should look at new ways to collaborate internally with HR and externally with stakeholders. Consider new dynamics in how government, higher education, and business can work together to build necessary talent. How can you leverage people differently and collaborative outside your organization to think about new incentives and alternative workforce dynamics?

5 insights you should know

Approximately 50% of IT security jobs go unfilled¹. By 2021 there will be an estimated 3.5 million unfilled cybersecurity jobs worldwide

New tech demands new skills. Artificial intelligence (AI) and robotic process automation (RPA) are among top digital priorities across government, yet even larger departments may not have those skills internally.

Legacy systems also make demands. Not only is it a challenge to find someone who still knows COBOL, it is equally hard to adopt modern infrastructure concepts while still operating a legacy environment, which can counterintuitively result in increased complexity and greater skills challenges for workers.

Talent is an ecosystem, too. Even the largest organizations cannot do everything in-house. Our survey found that 85% of IT executives rely on vendors or MSPs for cybersecurity.²

Organizational culture can undermine good security. One way to make the existing cybersecurity workforce more productive is to help the adjacent workforces—such as those with IT skills—to understand that they, too, have cybersecurity roles and responsibilities.

5 actions you can take



Build efficiency. Reexamine workflows and employ productivity tools to increase the efficiency of the existing IT workforce



Enhance humans with automation. Automate simple tasks with RPA to allow staff to focus on higher complexity issues, and thus boosting overall productivity.



Look for talent in new geographies. The rapid shift to remote work during COVID-19 has shown that many jobs—including cybersecurity—can be done from anywhere.



Consider new forms of talent. Consider alternate work arrangements, such as gig workers or shared resources from different agencies to fill talent gaps.



Invest in reskilling. Technology is dynamic, and so should be your workforce. Providing employees with opportunities to continue learning can not only make them more effective, it may also help with retention.

Connect with us

Tim Li

Principal
Government & Public Services
(GPS) Cyber & Strategic Risk Lead
Deloitte & Touche LLP
timli@deloitte.com

Jesse Goldhammer

Managing Director
Government & Public Services
(GPS) Cyber & Strategic Risk Lead
Deloitte & Touche LLP
jgoldhammer@deloitte.com