HELP
SOURCE
Q&A

Q As the CISO of my organization, I am facing a problem I have not encountered before. We are finding it difficult to hire security staff with appropriate skills. How can we resolve this problem?

A It is not a unique problem, but a universal one. Many organizations have encountered this, and there is data to confirm it. ISACA's *State of Cybersecurity 2018* report supports this finding:

> *The skills gap continues unabated. Enterprises still have open security positions, and the time to fill them appears to have decreased slightly. Demand is greatest for skilled technical resources at the individual-contributor level, rather than the management or executive level. For job seekers, technical skills are a strong differentiator.*[1]

In addition to this report, many other surveys have pointed out that getting properly skilled people for managing cybersecurity is a challenge today, as the unemployment rate for security professionals is zero.

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

Many experts have drawn on their experience to suggest ways to address this problem. Some of these suggestions are summarized here:

- Outsourcing is an easy solution that is likely to give access to appropriately skilled resources. When implementing a security operations center (SOC), I used this method. Ours had been an organization that believed in hiring its own personnel, but when we took into account the market demand and a faster attrition rate for SOC-related skills, we decided to hire management-level personnel and outsource other skills required. In that way, we achieved both availability of skilled persons and oversight of their performance. Nowadays, there are many business establishments that provide managed security services (MSS).
- Adapting short-term skills management practices by outsourcing security and providing training to existing staff may make those employees suited to be moved into jobs for which needed skills and competencies are not currently available internally. This is essential for all organizations as new threats are emerging and organizations may not have the required skills to respond to them.
- Cross-functional training within the organization enables functional users to understand technology and security-related basic skills and informs IT staff on functional and security

> "WHEN ALL IS SAID AND DONE, ORGANIZATIONS NEED TO UNDERSTAND THAT INFORMATION SECURITY REQUIRES AN INVESTMENT IN PEOPLE AND TECHNOLOGY."

aspects. This sharing of knowledge helps strengthen the first line of defense, providing enough bandwidth for skilled resources to address complex security issues.

- Optimizing the cybersecurity workforce in collaboration with local education systems and trainers is a useful approach. However, it requires collaboration and may need time to get the right skilled resources. It is necessary to develop a framework by considering future staffing needs.

When all is said and done, organizations need to understand that information security requires an investment in people and technology. It also requires an investment on the part of stakeholders—an investment of their time to be on top of the information security agenda.

Endnotes

1 ISACA, *State of Cybersecurity 2018*, USA, 2018, *https://cybersecurity.isaca.org/state-of cybersecurity*