Unsplash © Towfiqu Barbhuiya

Hiring a diverse workforce could help tackle data privacy issues

ISACA research has said organisations are dangerously exposed to cybersecurity problems because of a cyber skills gap. It reported 55% of firms are unable to fill technical privacy jobs and 46% are struggling with legal and compliance hires. It added the figures are expected to worsen in 2022 to 72% and 67%, respectively, and urged organisations to fully invest in privacy strategies.

Article originally published on Curation

ISACA also said 31% of organisations had open technical privacy jobs. Its report added that 41% of organisations blamed a shortage of competent resources for their difficulties in creating an overall privacy policy. (*Computer Weekly*)

Why does this matter?

Data has emerged as the world's most *valuable* resource. Training a workforce that can manage information effectively while adhering to regulatory guidelines is essential to ensure companies do not face financial penalties or

reputational damage.

Ongoing issue

A shortage in cybersecurity personnel is nothing new. Companies have previously been forced to *adopt* AI systems to replace a lack of cyber talent, while select firms began *crowdsourcing* “friendly” hackers to identify network vulnerabilities.

A lack of expertise, however, not only impacts how firms respond to a cyber event, but also causes problems for companies’ day-to-day managing of data.

Data misuse

Without trained employees, companies can be their own worst enemy when it comes to data management and sharing.

Crisis Text Line, for example, only recently *stopped* sharing sensitive user data with AI-enabled customer service platform Loris.ai after backlash from privacy experts. Despite the right decision being made, perhaps the issue would have been avoided if in-house personnel were aware of the implications of sharing personal data with third parties.

Diversifying talent

Prolonged shortages suggest a fresh approach to recruitment is needed to attract workers to cyber roles. The UK has already begun *retraining* service veterans for cybersecurity roles, however, diversity and inclusion initiatives could also be an answer.

Financial service companies have previously reported that the *hiring* of neurodiverse individuals has enabled them to outperform their competitors. This is just one example, and its likely similar benefits could be reaped by diversifying cybersecurity. Recruiters are now beginning to *prioritise* inclusion in their pursuit of talent as more teams recognise the positive impact it can have.

Mandy Andress, chief information security officer at solutions firm Elastic, *outlines* how diverse perspectives are crucial when considering the evolution of threats and risks on a daily basis, while different viewpoints could challenge data management practices.

Fred Fullerton is Senior Sustainability Specialist at *Curation* where this article was originally published

Sign up for Sustt

Article by FRED FULLERTON