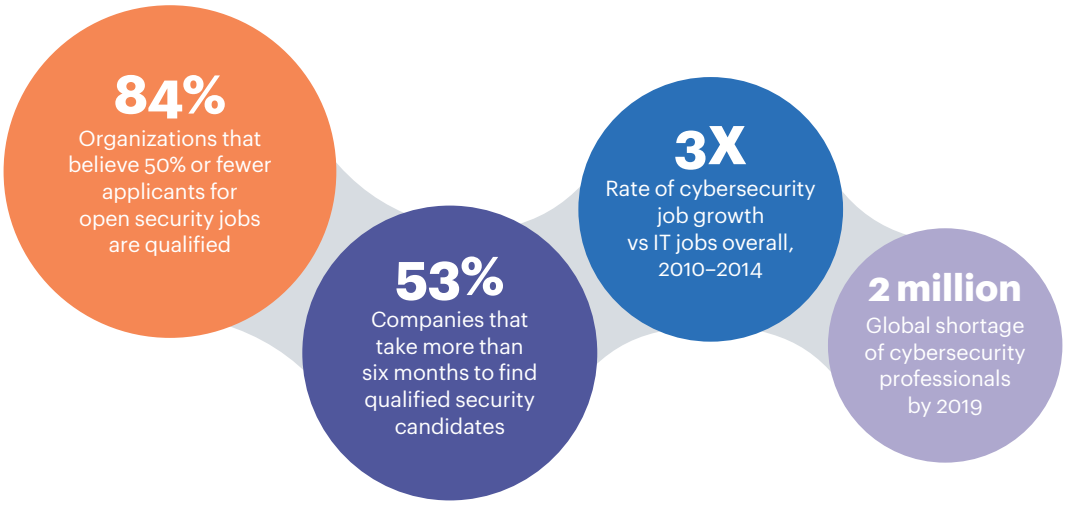
Figure 9
State of global cybersecurity talent



Source: A.T. Kearney analysis

cybersecurity training programs for ASEAN. Efforts are currently under way across other markets, largely driven by the private sector and with a focus on addressing short-term skills gaps.

Earlier this year, Singapore announced plans to set up a new cyber defense vocation that will create a force of approximately 2,600 cyber defenders, consisting of mostly civilians but also leveraging National Service personnel. The vocation will fall under the Singapore Armed Forces, adding military support to the capacity-building efforts.

Building capacity is a long-term effort. With the majority of ASEAN member states lacking a structured and long-term approach to developing competent cybersecurity professionals, the emerging member states must rapidly adopt best practices from countries that have implemented capacity-building frameworks.

Companies across the region are also looking at other avenues to address the challenge. Select corporations in the telecom, manufacturing, and oil and gas industries have been considering strategic moves into the cybersecurity domain, either organically or through acquisitions. These companies have been actively scouting for innovative cybersecurity companies to strengthen their in-house capabilities. Because of the experience built over the years, cybersecurity is seen as part of a wider growth agenda, potentially driving new revenue streams while securing critical infrastructure. Efficiency can be gained by placing inexperienced personnel in event and incident management and leaving experienced, highly trained cyber personnel focused on the system use case engineering, tuning, and review.

1.4 Perception that cyber risk is an IT risk results in the absence of a holistic approach to cyber resilience

Corporate stakeholders often have a myopic view of cyber risk, seeing it as an IT issue and not a business risk. As a result, technology investment is perceived as the key to mitigating cyber risk. Systems architecture, people, processes, and organizational culture are the greatest assets organizations can employ to shrink the attack surface. Many organizations either underestimate