The United Kingdom's Malvern Cybersecurity Cluster

The United Kingdom has one of the most successful cybersecurity industries when measured in terms of economic growth. The sector alone contributed GBP 1.8 billion in exports to the UK economy in 2015 and grew from GBP 17.6 billion in 2014 to almost GBP 22 billion in 2015. Despite its relatively small size, the United Kingdom has 17 cybersecurity clusters.

In 2014, amid demand from small cybersecurity companies across the country, the UK Cyber Security Forum social enterprise was spun out of Key IQ and founded to help volunteers start cybersecurity clusters across the nation. The Forum acts as a focal point for organizations that want to engage with small, innovative companies and facilitates lobbying with the government about issues they face. The Malvern Cyber Security Cluster is now one of the clusters under the umbrella of the Forum.

The Malvern Cyber Security Cluster was founded in September 2011 by Key IQ Ltd. and today has a high concentration of active and innovative small cybersecurity companies. The area is now recognized as one of the primary locations in the United Kingdom for the research, development, and commercialization of cybersecurity products and services and is increasingly referred to as Cyber Valley.

4 Conclusion and Next Steps

The region's response to the cybersecurity challenge needs to be comprehensive and forward-looking, engaging an array of stakeholders to deal with the threat and support the region's leap into the vanguard of the digital economy. No country, company, or individual can surmount the cybersecurity challenge alone. Thus, every stakeholder has a role to play in creating a safe environment. The crucial shift from the failures of traditional cybersecurity to cyber resilience will require moving beyond protecting against attacks to building resilient assets and processes. The practices, procedures, and processes used to build and maintain technological systems will determine the success or failure of the next big attack.

In section 3, we highlighted that concerted actions will be required along a comprehensive four-point agenda to tackle the core of the problem:

1. Elevate cybersecurity on the regional policy agenda.
2. Secure a sustained commitment to cybersecurity.
3. Fortify the ecosystem.
4. Build the next wave of cybersecurity capability.

Immediate action is required. In figure 30 on page 47, we have outlined some of these actions. In the short term, national governments across ASEAN should speedily implement the 12-point agenda highlighted under the Rapid Action Cybersecurity Framework. The ASEAN secretary-general's annual report should be expanded to include a review of how each country's progress. This would increase awareness and raise the bar in terms of preparedness.

A sustained and committed approach to investing in cybersecurity is needed as the region becomes more digitally connected. From 2017 to 2025, ASEAN will need to spend $171 billion (0.35 to 0.61 percent of annual GDP) to align with international benchmarks. Given that the value-at-risk for ASEAN's top 1,000 listed companies is roughly $750 billion in terms of current