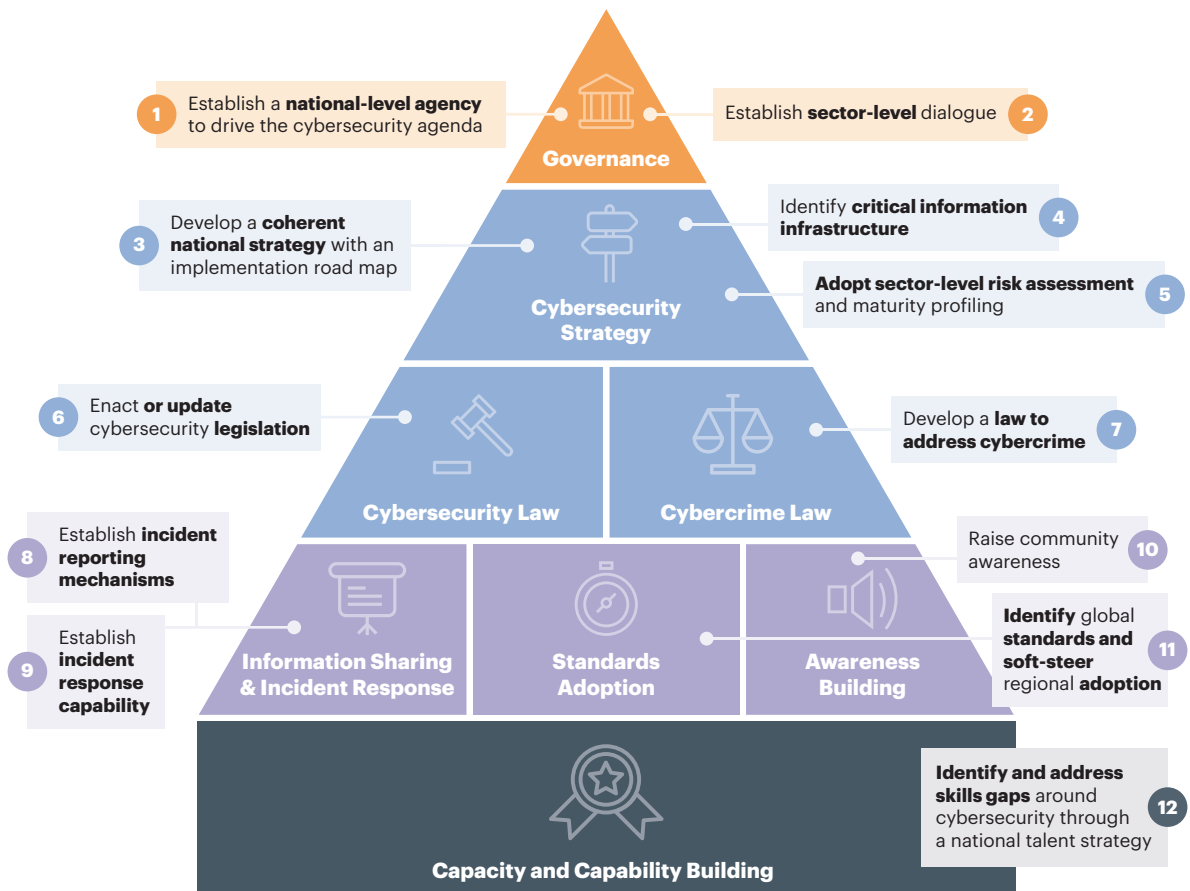


3.1.1 Steer the implementation of a Rapid Action Cybersecurity Framework

As highlighted earlier, a few ASEAN countries have already defined their national strategy around cybersecurity together with an implementation road map. However, the pace, urgency, and level of harmonization of policy thrusts around cybersecurity across the rest of the region remains too slow.

The AMCC has taken steps to extend collaboration on cybersecurity across the region. However, a system based on loose collaboration of national agencies and voluntary exchanges is unlikely to go far enough to make ASEAN safe. To be effective, a tighter coordination mechanism is needed. A Rapid Action Cybersecurity Framework focused on addressing current weaknesses in cyber resilience in each country across the region is the first step in establishing some degree of harmony in terms of readiness across the region (see figure 19). This is a threshold requirement for countries such as Laos, Cambodia, and Myanmar to speedily implement the institutional frameworks needed to govern cybersecurity and interface with the rest of the region. The Rapid Action Cybersecurity Framework envisages 12 strategic imperatives, aimed at fixing the basics related to cybersecurity across the region. National governments should take the lead in implementing the Framework with support and guidance from the AMCC.

Figure 19
Rapid Action Cybersecurity Framework



Source: A.T. Kearney analysis