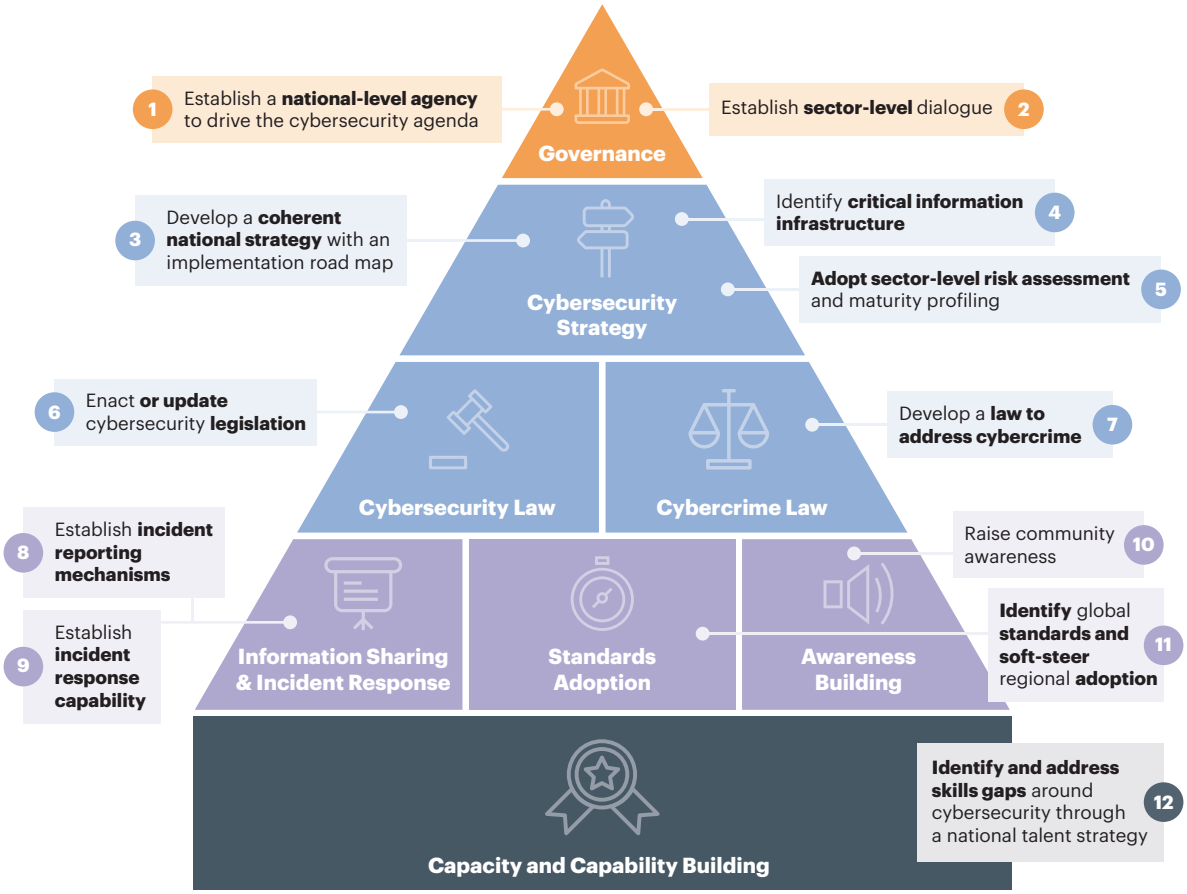
3.1.1 Steer the implementation of a Rapid Action Cybersecurity Framework

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

As discussed, several ASEAN countries have identified national agencies to drive their cybersecurity agenda. In others, the process is still ongoing, with CERTs serving as the de facto agency in charge of cybersecurity. It is important to define who within each country is responsible for managing and evaluating the cybersecurity strategy and ensure the v esting of sufficient authority to drive action across sectorial and government department boundaries. While centralized and decentralized models exist, establishing an **independent central national agency to define and supervise the security agenda** will foster a strong enforcement mindset.

An imperative of the Rapid Action Cybersecurity Framework is the definition of a **national cybersecurity strategy** by each country with a sharp vision, scope, objectives, and a practical road map for implementation (see sidebar: Australia's Cybersecurity Policy). In this context, an approach based on risk identification, risk analysis, and risk evaluation is crucial. **Risk assessments** should be carried out both at the national and sectorial level. **Defining and identifying critical sectors and critical information infrastructure** (CII) while engaging with CII owners at the outset is a vital part of the strategy. A clear set of sector specific risk mitigation mechanisms needs to be put in place. Assessing and prioritizing high-value assets and determining the probability of breach should be at the core of such risk assessments.

Enacting **pragmatic cybersecurity legislation or updating it** to current needs is the next step in the Rapid Action Cybersecurity Framework. While political issues could affect policy alignment at the regional level, the increasing integration of ASEAN requires a certain level of harmonization and coordination. Furthermore, because technology is rapidly advancing, the laws could quickly fall far behind. Adopting a careful approach in collaboration with the private sector, aimed at regulating human behavior and spreading a cybersecurity culture, is vital to ensure pragmatic legislation in each country.

To address **cybercrime**, each country must define cybercrime laws and strengthen local law enforcement. The only existing multilateral treaty addressing cybercrime is the Budapest

Australia's Cybersecurity Policy

The main themes of Australia's Cyber Security Strategy released in 2016 are co-leadership, strong cyber defenses, global responsibility and influence, and growth and innovation. A key tenet is the recognition of a national cybersecurity partnership that places the onus on government agencies and business leaders to set the national cybersecurity agenda. A cyber ambassador will identify opportunities for practical international cooperation and ensure Australia has a coordinated, consistent, and influential voice on international cyber issues.

The Australian Signals Directorate has developed strategies to help cybersecurity professionals mitigate cybersecurity incidents. This guidance addresses targeted cyber intrusions, ransomware, and external adversaries with destructive intent, malicious insiders, business email compromise, and industrial control systems. This policy has become standard practice for industry stakeholders as well. Areas such as escalated privilege management, 48-hour patch deployment, and application whitelisting are seen as the most effective tools for reducing cyber risk. Recent updates to this policy have added application hardening, blocking macros and daily backups. These controls were mandated via a critical review of incidents responded to by the national CERTs and were analyzed to be the most effective controls that would have prevented more than 85 percent of the breaches.

Convention on Cybercrime, proposed by the Council of Europe in 2001, which includes provisions for cross-border assistance between law enforcement agencies on cybercrime separate from the more cumbersome Mutual Legal Assistance Treaty arrangements. Despite the Philippines having committed to the Budapest Convention, none of the other ASEAN countries has signed. Adopting an ASEAN-initiated multilateral regime around cybercrime consistent with the Budapest Convention could bring about strategic and operational benefits to the region, particularly in the area of rapid law enforcement cooperation.

Information sharing among stakeholders is a powerful mechanism to better understand a constantly changing environment. Sharing views on emerging threats, risks and vulnerabilities together with aspects related to national security, provides powerful insight into how the threat landscape is evolving. In this context, it is important to properly define the information sharing mechanism and the underlying rules that govern it, including non-disclosure agreements, traffic-light protocol, antitrust rules, and law enforcement access. A sectorial approach to information sharing is a good start, but this should be extended to encourage cross-sector communication as there are many interdependencies between sectors, for example between the banking and telecom sector for mobile payments.

National cybersecurity agencies have a pivotal role to play in driving adoption and harmonization of **standards** across the region. A start could be made with standards such as ISO 27001 and the NIST Cybersecurity Framework. Collaboration at the sectorial level to share best practices around specific concerns such as IT-OT convergence and wider adoption of standard specifications for sharing threat intelligence such as STIX and TAXII can significantly benefit the region.

Raising awareness about threats and vulnerabilities and their impact on society has become vital. With greater awareness, individual and corporate users can learn how to behave in the online world and protect themselves from risks. Defining the target of awareness-raising campaigns and identifying mechanisms to address them is a joint responsibility of both the public and private sectors. Initiatives such as Safer Internet Day, International Youth Day, and ENISA's security month have helped tremendously to increase social awareness and modify online behavior.

Apart from the above, it is vital that the region adopts a forward-looking **talent strategy** aimed at addressing the capacity and capability gaps highlighted earlier. Cross-regional collaboration efforts at training together with industry can enable countries to tap into each other's strengths to quickly boost the talent level.