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.