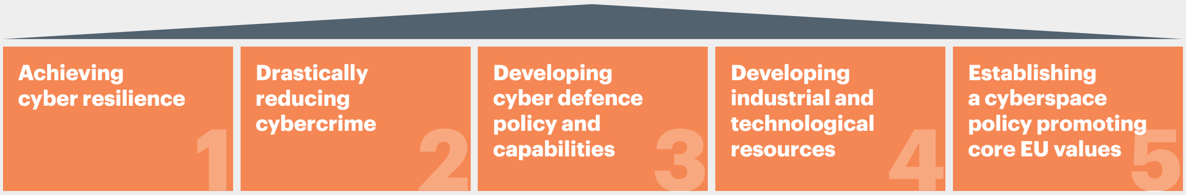
The EU Approach to Cybersecurity

The European Union (EU) developed a region-wide cybersecurity strategy in 2013 to "enhance the EU's overall performance" and to "safeguard an online environment providing the highest possible freedom and security for the benefit of everyone." This was augmented by the Cybersecurity Package announced in 2017. The figure below highlights the pillars of EU's cybersecurity strategy (see figure).

Facing similar complexities as ASEAN, such as fragmented regulation, the EU also saw the need for a unifying framework, giving rise to the Directive on Security of Network and Information Systems (NIS Directive) as part of its overall cybersecurity strategy, which entered into force in August 2016. Member states were given 21 months to adopt the directive into their national legislation. Some crucial elements of the directive include:

- **A requirement for member states to be appropriately equipped, such as having a national CSIRT and a national NIS body. The CSIRTs would form a collaborative CSIRT network that would cooperate on incidents and share risk-related information.**
- **A cooperation group involving all member states, allowing for strategic cooperation and information sharing**
- **Security measures across critical information infrastructure sectors and key digital service providers, such as the mandatory reporting of serious incidents by organizations to the national authorities**

Figure
Cybersecurity Strategy of the European Union


Achieving cyber resilience
1
Drastically reducing cybercrime
2
Developing cyber defence policy and capabilities
3
Developing industrial and technological resources
4
Establishing a cyberspace policy promoting core EU values
5

Sources: *Joint Communication to the European Parliament and The Council*, The European Economic and Social Committee, the Committee of the Regions, Cybersecurity Strategy of the European Union; A.T. Kearney analysis

Quantifying the value-at-risk from cybercrime is challenging, and organizations around the world lack competencies in this area. One of the biggest challenges is understanding the nature of the threat to high-value assets and appropriately prioritizing and focusing mitigating resources. No organization can afford to use every defense mechanism in its arsenal, nor is it practical. However, resources must be allocated according to the magnitude of the threat and the value-at-risk.

Based on a sector-wide perspective, most ASEAN countries are at risk of cyberattacks because of the significant contribution of information and communications technology (ICT) in the sectors that are most at risk. The IBM X-Force Threat Intelligence Index has cited the following as the most cyberattacked sectors in recent years: healthcare, manufacturing, financial services, government, transportation, and retail.[13] Across the ASEAN-6, these sectors account for the majority of GDP contribution (on average of 70 percent). In the case of Singapore, the share of these sectors is even higher at 94 percent of GDP.

[13] "Monitored security is superior security," *IBM X-Force Threat Intelligence Index 2017*