

Figure 13

A cyber-defense matrix can help optimize the cybersecurity portfolio

		NIST Framework				
		Identify	Protect	Detect	Respond	Recover
Asset classes	Devices	Device profiling	Identity and access management Antivirus and HIPS	Endpoint visibility and control, endpoint threat detection and response		
	Applications	Configuration and systems management	Application security			
	Networks	Net flow	Network security (firewalls, intrusion and prevention systems)	Distributed denial-of-service mitigation Intrusion detection system	Rapid threat containment	
	Data	Data labeling	Data encryption and data loss prevention	Deep web	Digital rights management	Backup
	Users	Phishing simulations	Phishing awareness	Insider threat and behavioral analytics		
	Degree of dependency	Technology			Process	

Note: HIPS is host-based intrusion prevention system. NIST is National Institute of Standards and Technology.
Sources: RSA, National Institute of Standards and Technology; A.T. Kearney analysis

2 The Cybersecurity Challenge is Escalating

In section 1, we highlighted that ASEAN countries are a prime target for cyberattacks, and a low level of preparedness makes the region particularly vulnerable. There is a need for urgency in addressing the problem as the threat landscape will escalate.

In the rapidly evolving cyber landscape, four issues must be addressed:

- The growing interconnectedness across the region and geographical dispersion of the physical supply chain will intensify systemic risk, making the region only as strong as its weakest link.
- Diverging national priorities and varying paces of digital evolution will continue to foster a sustained pattern of underinvestment.
- Limited sharing of threat intelligence, often because of mistrust and a lack of transparency, will lead to even more porous cyber defense mechanisms.