With economic interconnectedness, the region faces more systemic risk, a concept traditionally applied to financial services. Systemic risk is defined as the risk that a cyber event cascades into related ecosystem components, creating adverse effects in public health, safety, the economy, or national security.[21] Recent cyber heists are game changing in their implications on regional systemic risk, demonstrating that threat actors need not attack a core system to exploit its weaknesses. Systemic risk took center stage with the hacking of banks in Bangladesh, Vietnam, and Ecuador—exposing the entire SWIFT network of more than 11,000 banks (see sidebar: Systemic Attack on SWIFT).

Further, as discussed, supply chain partners have the potential to be the weak links in any company's business operation. Even if companies can ensure the robustness of their own cybersecurity operations, there is often limited visibility into the business partner ecosystem, creating blind spots in data security. The challenges are twofold in the region: First, supply chain partners are at varying levels of IT and security readiness, requiring significant foundation-setting and training. Second, the adoption of security standards is as yet nascent, and companies with a regional footprint as well as market entrants face the risk of differing regulations by country, leading to inefficiencies in intraregional trade.

2.1.2 Diverging national priorities because of varying paces of digital evolution will foster a pattern of sustained underinvestment

Despite the region's interconnectedness, the networked readiness and pace of digital evolution across ASEAN countries has been and is likely to continue to be much different (see figure 15 on page 20).

As the region becomes increasingly digital, there will be a greater need to spend more on cybersecurity. There is a strong correlation between the share of the digital economy and spend

Systemic Attack on SWIFT

Systemic cyber risk recently came under scrutiny with the discovery of three separate hacking incidents against member institutions connected to the SWIFT network at banks in Bangladesh, Vietnam, and Ecuador, accounting for more than $90 million in stolen funds. The attacks demonstrated that the applications that enable the financial messaging traffic between member banks can be manipulated and misused when member institutions do not strictly adhere to the security standards. Previously, accessing the SWIFT network required being physically present at a dedicated terminal.

However, as banking requirements and technologies have changed, the ability for financial institutions to connect to this network has changed as well. Banks now leverage multiple applications, resident on various user endpoints, to interface with the SWIFT network. Each connected endpoint presents an avenue of attack for threat actors to fraudulently create and send financial messages. The Bangladesh Central Bank hack is a prime example of this situation; a threat actor infiltrated a poorly secured network and used an unsecured endpoint to carry out one of the largest bank heists in history. Approximately 11,000 institutions enjoy access to SWIFT, and the ability of the network to withstand a cyberattack is only as good as the weakest link in the network.

[21] *Understanding Systemic Cyber Risk*, World Economic Forum