

Table of Figures

- Figure 1: Regional cybersecurity defense playbook 2
- Figure 2: A digital revolution will transform the ASEAN region by 2025 4
- Figure 3: Blocked suspicious web activity, by country of origin (expected ratio = 1.0) 5
- Figure 4: Four step approach to national cybersecurity strategy development 6
- Figure 5: ASEAN Countries - National cyber policy landscape 7
- Figure 6: ASEAN cybersecurity spending is expected to show double digit growth up to 2025 10
- Figure 7: Benchmarking cybersecurity spend as percent of GDP (2017e) 11
- Figure 8: Vendors’ product and service positioning across the value chain (non-exhaustive). . . 11
- Figure 9: State of global cybersecurity talent.13
- Figure 10: NIST Framework for Improving Critical Infrastructure cybersecurity14
- Figure 11: Number of security vendors and products used by organizations.15
- Figure 12: Costs escalate the longer a cyberattack remains uncontained16
- Figure 13: A cyber defense matrix can help optimize the cybersecurity portfolio.17
- Figure 14: Regional footprint of ASEAN businesses and member states’ share of intra-regional trade.18
- Figure 15: The ASEAN region has a significant digital divide 20
- Figure 16: Correlation between digital evolution and cybersecurity spend.21
- Figure 17: Virtual currency increasingly a target for cyberattacks 25
- Figure 18: Regional cybersecurity defense playbook. 27
- Figure 19: Rapid Action Cybersecurity Framework 28
- Figure 20: A tighter regional cybersecurity governance framework is needed.31
- Figure 21: Target cumulative cybersecurity spend – 2017 to 2025 32
- Figure 22: Focus the cybersecurity agenda on relevant metrics (illustrative) 33
- Figure 23: Deploy a cyber-hygiene dashboard. 34
- Figure 24: Define a cybersecurity strategy with a focus on four areas 34
- Figure 25: Adopt a risk-centric approach to cybersecurity 35
- Figure 26: Security as a digital enabler 36
- Figure 27: Address gaps in cybersecurity capacity and capabilities41
- Figure 28: MDEC’s 3-tier capacity building program 43
- Figure 29: Identifying user patterns to recognize true threats with automation 44
- Figure 30: Stakeholder view of Call to Action. 47
- Figure 31: Action agenda for Board and CISO stakeholders 48