

Contents

- Executive Summary 1**
 - The ASEAN region is a prime target for cyberattacks 1
 - The situation will escalate over time 1
 - An urgent call to action 2
- 1 The ASEAN Region: A Prime Target for Cyberattacks 3**
 - 1.1 ASEAN countries have emerged as launchpads for cyberattacks 5
 - 1.2 Policy preparedness is still nascent with a lack of institutional oversight and limited funding to fortify digital economies 6
 - 1.3 A nascent local cybersecurity industry with shortages of home-grown capabilities and expertise 10
 - 1.4 Perception that cyber risk is an IT risk results in the absence of a holistic approach to cyber resilience 13
 - 1.5 Multiple vendor relationships and product deployments result in operational complexity 15
- 2 The Cybersecurity Challenge is Escalating 17**
 - 2.1 The cybersecurity challenge is likely to get more complex 18
 - 2.2 The exposure for ASEAN’s top companies is \$750 billion and is likely to increase 26
- 3 Call to Action: The Need for an Active Defense Mindset 27**
 - 3.1 Elevate cybersecurity on the regional policy agenda 27
 - 3.2 Secure a sustained commitment to cybersecurity 31
 - 3.3 Fortify the ecosystem 33
 - 3.4 Build the next wave of cybersecurity capability 40
- 4 Conclusion and Next Steps 46**
- Appendix A: Security Maturity Model 50**
- Appendix B: ASEAN Countries Cybersecurity Policy Developments 51**
- Appendix C: The Networking Academy’s Learning Portfolio 52**
- Table of Figures 53**