BAB IV

PENUTUP

4.1 Kesimpulan

Penulis menyimpulkan bahwa ancaman *cybercrime*, khususnya melalui penyebaran *spyware* dan *ransomware*, telah menjadi tantangan serius bagi keamanan informasi perusahaan-perusahaan di kawasan Asia Tenggara. Serangan tersebut tidak hanya menimbulkan kerugian finansial yang signifikan, tetapi juga menciptakan dampak reputasional dan operasional yang merugikan. Berdasarkan analisis kasus seperti serangan terhadap Bank Syariah Indonesia dan SingHealth Singapura, penulis menemukan bahwa pelaku kejahatan siber memanfaatkan kerentanan sistem digital dan rendahnya kesiapan perusahaan dalam menghadapi insiden siber secara teknis maupun strategis.

Selanjutnya, penulis menilai bahwa klasifikasi *cybercrime* sebagai kejahatan non-tradisional dan transnasional sangat relevan dalam konteks ini. *Spyware* dan *ransomware* dapat dikategorikan sebagai kejahatan dengan pendekatan *computer-as-tool* dan *computer-as-target*, yang menunjukkan kompleksitas metode yang digunakan pelaku untuk menyerang dan mengeksploitasi sistem digital. Di tengah lemahnya harmonisasi kebijakan siber di Asia Tenggara, ransomware bertransformasi menjadi alat ekonomi dan politik yang digunakan oleh aktor non-negara maupun negara, menuntut pendekatan keamanan yang lebih terkoordinasi lintas sektor dan lintas negara.

Penulis juga menegaskan bahwa strategi mitigasi yang paling efektif memerlukan kerja sama erat antara pemerintah, perusahaan swasta, dan organisasi regional seperti ASEAN. Pendekatan neoliberalisme dalam keamanan siber, yang menekankan kolaborasi publik-swasta dan insentif pasar, terbukti relevan dalam memperkuat respons terhadap ancaman *ransomware*. Namun, kerja sama ini harus ditunjang oleh regulasi yang adaptif, edukasi berkelanjutan, dan penguatan kapasitas teknis di tingkat nasional maupun regional. Penulis merekomendasikan bahwa keberlanjutan strategi keamanan siber di Asia Tenggara bergantung pada kemampuan negara dan sektor swasta dalam membangun ekosistem digital yang resilien dan inklusif.

4.2 Saran

Berdasarkan temuan dalam penelitian ini, penulis merekomendasikan agar peneliti selanjutnya dapat melakukan studi yang lebih mendalam mengenai strategi peningkatan kapasitas keamanan digital internal perusahaan-perusahaan di Asia Tenggara. Penelitian lanjutan dapat memfokuskan kajiannya pada efektivitas deteksi dini terhadap ancaman seperti *spyware* dan *ransomware*, dengan pendekatan studi kasus pada sektor industri tertentu seperti perbankan, kesehatan, atau UMKM. Peneliti juga dapat mengeksplorasi implementasi praktis dari protokol mitigasi seperti audit sistem berkala, penggunaan teknologi enkripsi, atau pelatihan keamanan siber bagi karyawan untuk mengetahui sejauh mana strategi tersebut mampu mencegah insiden siber.

Selain itu, penulis menyarankan agar penelitian selanjutnya dapat mengkaji peran pemerintah dalam memperkuat regulasi keamanan siber dan mendorong harmonisasi kebijakan antarnegara ASEAN. Studi lanjutan dapat meneliti efektivitas lembaga pengawasan yang ada, bentuk insentif fiskal yang paling relevan bagi sektor swasta, serta mekanisme kolaborasi hukum antarnegara dalam menghadapi kejahatan siber lintas batas. Penelitian ini dapat menggunakan pendekatan kualitatif melalui wawancara dengan pembuat kebijakan atau pendekatan kuantitatif dengan menganalisis tingkat kepatuhan perusahaan terhadap kebijakan nasional seperti UU PDP di Indonesia atau PDPA di Malaysia.

Terakhir, penulis menyarankan agar peneliti berikutnya fokus pada analisis mendalam mengenai dinamika kerja sama publik-swasta dalam keamanan siber. Penelitian ini dapat memanfaatkan studi kasus konkret seperti *ASEAN-Singapore Cybersecurity Centre of Excellence* atau proyek regional lainnya sebagai contoh kolaborasi yang berhasil. Fokus utama dapat diarahkan pada bagaimana model kemitraan strategis tersebut dibentuk, dikelola, dan direplikasi ke negara-negara lain di kawasan Asia Tenggara. Dengan pendekatan ini, penelitian selanjutnya diharapkan dapat memberikan kontribusi praktis dalam merancang kebijakan kolaboratif dan memperkuat ketahanan siber secara kolektif.