BAB 5
SIMPULAN DAN SARAN

5.1 Simpulan

Secara umum keamanan siber di Indonesia masih sangat rendah, jika tidak mau dikatakan parah. Data yang tersimpan di *server* pribadi ataupun penyimpanan *cloud* masih sangat rentan diretas oleh pihak atau oknum yang tidak bertanggung jawab, demi kepentingan ekonomi yaitu memperoleh *ransom* ataupun data tersebut dijual. Secara spesifik, kelompok akademisi menyebut kondisi keamanan siber Indonesia sangat rentan, sementara narasumber Pemerintah mengatakan alasan kondisi tersebut disebabkan oleh karena sangat kurang/ terbatasnya jumlah sumber daya manusia yang mumpuni dan bersertifikat keahlian keamanan siber dibandingkan dengan kebutuhan, walaupun sudah ada beberapa usaha dan pelatihan yang dilakukan untuk berproses ke arah kemajuan. Sedangkan kalangan dunia usaha / pelaku bisnis mengatakan bahwa baik dalam hal regulasi untuk menegakkan keamanan siber maupun dalam pengembangan industri keamanan siber, Indonesia masih terbelakang jika dibandingkan dengan negara lainnya. Perlu dibangun keterampilan digital, termasuk keterampilan untuk mendapatkan pengalaman online yang aman dan bebas dari serangan siber. Fakta mengenai belum adanya penyusunan dan pengesahan Undang Undang Keamanan Siber oleh DPR mencerminkan kondisi keamanan siber yang sebenarnya di masyarakat, yaitu kamsiber belum menjadi prioritas.

Pengumpulan data kuantitatif melalui distribusi survei singkat kepada 50 responden dilakukan untuk mengkonfirmasi data kualitatif yang dilakukan melalui wawancara kepada 10 narasumber yang terdiri dari perwakilan institusi pemerintah pusat dan daerah, pelaku bisnis, akademisi pakar keamanan siber, dan asosiasi kemasyarakatan (Indonesia Cyber Security Forum). Ringkasan data kuantitatif sebagai berikut: 78% responden menyatakan tingkat kesadaran publik mengenai pentingnya keamanan siber masih rendah, 75% menyatakan kepatuhan terhadap ISO/IEC 27001 tentang Sistem Manajemen Keamanan Informasi tidak dilakukan secara konsisten, 70% menyarankan penggunaan *software antivirus/firewall* dalam pencegahan dan mitigasi serangan siber; 68% merekomendasikan penerapan prinsip *zero trust*, 54% responden cenderung untuk menggunakan pusat data lokal, 70% menyarankan penggunaan penyedia penyimpanan *cloud* terpercaya, dan 88%

merekomendasikan pembaruan sistem secara berkala. Sementara pengamanan data geospasial dapat dilakukan melalui enkripsi data dan tanda tangan digital 76% dan image coding 70%.

Hasil penelitian kualitatif diringkaskan di bawah ini sesuai dengan rumusan masalah dan tujuan penelitian.

1. Penelitian tugas akhir ini telah mendeteksi penyebab utama penyerangan siber terhadap data geospasial:
   (a) Titik terlemah dalam keamanan siber di Indonesia adalah ketidaksiapan sumber daya manusia (SDM) di dalam lembaga/ institusi/ perusahaan terhadap serangan siber. SDM khususnya di bidang keamanan siber baik secara kuantitatif maupun kualitatif (bersertifikat) masih sangat kurang jika dibandingkan dengan kebutuhan.
   (b) Tingkat kesadaran digital dan literasi keamanan siber, budaya keamanan data masih rendah dan perlu dibangun.
   (c) Peraturan perundangan yang khusus mengatur tentang keamanan siber dan penanganan insiden peretasan data dan ancaman siber belum selesai disusun dan disahkan.
2. Tugas akhir ini telah mengidentifikasi dan mengkompilasi teknik/metodologi pencegahan dan mitigasi terhadap serangan siber pada data geospasial yaitu:
   (a) Menerapkan kebijakan dan SOP keamanan siber yang komprehensif.
   (b) Menyimpan data geospasial di *cloud service provider* yang terpercaya.
   (c) Meng-update *patch* keamanan data, access dengan IP admin secara tertib.
   (d) Membubuhkan *digital signature*, menerapkan *image encoding* di dalam data geospasial, antara lain dengan cara *watermark* dan steganografi.
3. Akhirnya, beberapa cara untuk meningkatkan pengamanan akses dan data geospasial telah didiskusikan antara lain:
   (a) Meningkatkan kesadaran akan keamanan siber dan literasi digital melalui program pelatihan yang formal, komprehensif, dan berkelanjutan sehingga lingkungan kerja memungkinkan untuk mendukung terciptanya budaya keamanan siber dalam pengelolaan data.

(b) Secara konsisten, terus menerus mendukung upaya peningkatan program pelatihan sertifikasi keamanan siber untuk pengelolaan data dan mencetak lebih banyak SDM yang ahli keamanan siber sehingga semakin mencukupi kebutuhan.

(c) Menerapkan level perizinan untuk akses ke sistem.

(d) Menyusun *Standard Operational Procedures* (SOP) Budaya Keamanan Data, idealnya mengikuti praktik terbaik ISO/IEC 27001.

(e) Menyusun peraturan, perundang-undangan keamanan siber, penanganan peretasan, penata layanan data termasuk data geospasial.

(f) Melakukan audit secara konsisten untuk memelihara kepatuhan (IT governance), mengevaluasi dan meng-*update* SOP secara berkala.

(g) Meningkatkan prioritas terhadap keamanan siber yang tercermin melalui peningkatan alokasi anggaran untuk memperkuat sistem keamanan siber, lebih baik proaktif dan preventif daripada menangani *ran*som.

(h) Se*cara teknologi informasi: menggunakan* software antivirus/ firewall, menerapkan *Zero Trust Framework*, meng-*update* sistem secara berkala, menggunakan enkripsi data dan perimeter keamanan aplikasi dan jaringan.

(i) Melakukan *multi-stakeholder approach* dalam kerjasama keamanan siber.

5.2 Saran

(a) Menggalang Kemitraan Pemerintah/Publik dan Swasta/industri:
Seperti contoh di Inggris Raya dan Australia antara lain melalui *"Online Fraud Charter"* melingkupi 12 perusahaan TI terbesar di dunia; atau *"Telecommunications Fraud Sector Charter"* dengan delapan perusahaan telekomunikasi; juga melalui penyusunan kode etik yang mengatur platform komunikasi digital, telekomunikasi, dan transaksi perbankan *"Scams Code Framework"*.[16]. Hal yang serupa dapat dilakukan pada perlindungan data Geospasial, misalnya kemitraan antara Badan Informasi Geospasial (BIG) dengan penyedia layanan data geospasial seperti ESRI.

(b) Menggalang kerja sama lintas sektor dan pemangku kepentingan:
DPR dan seluruh pemangku kepentingan keamanan siber dari unsur pemerintah, pelaku bisnis, pakar kamsiber dan akademisi perlu memulai kembali proses penyusunan Undang Undang Keamanan Siber, serta bersepakat perihal pembentukan dan pengesahan Badan Otoritas Keamanan Siber. Serupa dengan hal di atas, dengan sudah adanya pengesahan Undang-Undang Perlindungan Data Pribadi, pemerintahan Indonesia perlu segera membentuk Lembaga Penyelenggaraan Perlindungan Data Pribadi (LPPDP) yang dapat juga mencakup data geospasial.

(c) Memperkuat kemitraan internasional:
Kemitraan lintas negara, kawasan regional dan internasional ini akan sangat bermanfaat untuk forum berbagi pengalaman mengenai ancaman siber yang terjadi dan cara-cara sukses untuk menanganinya, pengetahuan terapan dan praktik terbaik tentang keamanan siber misalnya melalui kerja sama di Perserikatan Bangsa-Bangsa, *Global Cyber Cabinet*/GCC (Kabinet Siber Global), *Counter Syber Initiatives*/CRI (Inisiatif Kontra Siber). dan menjalin kemitraan dengan perusahaan global ternama, contohnya AWS, Google, Amazon, Microsoft, Oracle, ESRI, dan lain sebagainya.

(d) Berperan serta proaktif dalam perjanjian keamanan siber internasional:
Proaktif ikut serta dalam perjanjian internasional ini berguna untuk mengatasi ancaman siber yang seringkali lintas atau melampaui batas-batas negara. Berkolaborasi adalah kuncinya, Indonesia perlu terlibat proaktif dengan asosiasi dan organisasi siber internasional, dan mengadopsi Perjanjian Keamanan Siber internasional. Hal ini termasuk juga keaktifan untuk turut serta dalam latihan dan simulasi/*role play* keamanan siber demi meningkatkan kesiapsiagaan dan kemampuan tanggap.

Dalam masa mendatang yang tidak lama lagi, Indonesia akan menyadari kebutuhan akan data geospasial yang detail dan menyeluruh meliputi permukaan tanah dan kandungan di dalamnya, perairan lautan yang besar proporsinya, dan membuktikan fakta kekayaan sumber daya alam Indonesia. Ini semua memerlukan budaya keamanan siber demi pencapaian pembangunan berkelanjutan, pengembangan kota cerdas,

dan layanan berbasis lokasi dari platform *e-commerce*.

Data geospasial sesungguhnya sangat strategis baik dari segi politik (batas kedaulatan negara); perencanaan kota dan kawasan; ekonomi dan bisnis (kandungan sumber daya alam dan mineral), serta transportasi dan konektifitas.