BAB 1 PENDAHULUAN

1.1 Latar belakang

Teknologi informasi (TI) berkembang pesat dan membawa banyak perubahan dalam berbagai aspek kehidupan. Di satu sisi, TI menawarkan berbagai peluang dan manfaat, seperti peningkatan efisiensi, akses informasi yang mudah, dan konektivitas global. Di sisi lain, perkembangan TI juga menghadirkan berbagai risiko yang perlu dikelola secara efektif. Manajemen risiko TI adalah bagian penting dari tata kelola TI yang baik. Dengan mengidentifikasi, menilai, dan mengendalikan risiko TI, organisasi dan individu dapat melindungi aset mereka, memastikan kelancaran operasi, dan memanfaatkan peluang yang ditawarkan oleh TI. Kejahatan siber dipengaruhi oleh pertumbuhan populasi. Jumlah orang yang menggunakan internet dan teknologi digital terus meningkat, yang meningkatkan persaingan di dunia digital, yang dapat menyebabkan tindakan kriminal seperti pencurian data pribadi dan serangan siber (Sen et al., 2022). Kejahatan siber juga dipengaruhi oleh kemajuan teknologi (Veronika Asri Tanderirung dan Riana T. Mangesa, 2023). Pelaku kejahatan dapat melakukan tindakan kriminal yang lebih kompleks dan sulit dideteksi berkat kemajuan teknologi seperti kecerdasan buatan, internet of things (IoT), dan blockchain. Misalnya, serangan siber yang menggunakan ransomware atau botnet dapat mengakibatkan kerugian yang signifikan bagi korban (Mikel Kelvin, 2016).[1] Penguatan kelembagaan keamanan siber, ketiadaan dasar hukum untuk keamanan siber, dan kurangnya tenaga profesional serta kerjasama dalam negeri dan internasional adalah tantangan terbesar saat ini. Oleh karena itu, pemerintah harus memperkuat keamanan siber dan mempersiapkan orang-orang yang dibutuhkan dalam dunia yang semakin digital.[7] Perlindungan data pribadi biasanya bergantung pada konteks keamanan negara terhadap warganya, tetapi tidak mempertimbangkan kapasitas warganya untuk melindungi data pribadinya di internet. [11] Studi keamanan di bidang hubungan internasional menjadi topik yang menarik. Menurut Barry Buzan (1989), pada awal Perang Dingin, studi keamanan terbatas pada politik dan militer. Namun, seiring waktu, studi keamanan mulai mempertimbangkan masalah sosial, ekonomi, dan lingkungan. [15] Dalam beberapa dekade terakhir, kemajuan dalam teknologi informasi dan komunikasi telah berkontribusi secara positif pada pertumbuhan ekonomi dunia sambil meningkatkan produktivitas, persaingan, dan keterlibatan masyarakat. [18]

Perusahaan teknologi informasi (TI) berperan penting dalam perekonomian modern, mendorong inovasi dan transformasi digital di berbagai sektor. Namun, di tengah pesatnya perkembangan teknologi, ancaman keamanan siber juga meningkat secara signifikan. Insiden seperti peretasan, malware, dan serangan ransomware tidak hanya dapat menyebabkan kerugian finansial yang besar tetapi juga dapat merusak reputasi perusahaan dan mengganggu operasional bisnis. Berdasarkan laporan yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN), jumlah kasus serangan cyber di Indonesia sejak awal tahun 2020 hingga 12 April 2020 adalah sebanyak 88 juta. Dari jumlah kasus tersebut, teridentifikasi aktivitas serangan trojan sebesar 56%, upaya pengumpulan informasi sebesar 43%, dan serangan web application sebesar 1%. Hasil monitoring total kasus serangan cyber di Indonesia pada akhir tahun 2020 menurun. [2] Dunia internet, juga dikenal sebagai "cyberspace", memungkinkan segala hal untuk dilakukan, termasuk mendorong kreativitas manusia, mempermudah akses informasi, dan menawarkan berbagai kemudahan dan keuntungan lainnya. Namun, jangan lupa bahwa setiap hal pasti memiliki sisi positif dan negatif. [3] Menurut BSSN (Badan Siber dan Sandi Negara), terdapat hampir 190 juta upaya serangan siber di Indonesia dari Januari hingga Agustus tahun 2020. Ini adalah peningkatan lebih dari empat kali lipat dibandingkan periode yang sama pada tahun 2019—sekitar 39 juta upaya serangan siber. [7] risiko cybernetic yang dapat merusak sistem teknologi organisasi. Faktor negatif tambahan adalah peningkatan peretasan atau hacking, termasuk pencurian data, akun

media sosial, akun bank, dan sebagainya.[12] Selain itu, pemerintah Indonesia belum memberikan pendidikan yang cukup tentang keamanan siber. Meskipun beberapa institusi pendidikan tinggi terkenal di Indonesia, seperti Universitas Nasional, menawarkan tingkat pengetahuan yang cukup tentang keamanan siber, tidak banyak sekolah tinggi yang menyediakan pendidikan yang memadai dan merata tentang subjek ini di berbagai wilayah di Indonesia.[15] Akan tetapi, karena pemerintah, pengusaha, dan masyarakat semakin terhubung di dunia maya, ada beberapa tantangan yang terkait dengan ancaman dunia maya yang memerlukan pengembangan keamanan dunia maya yang lebih kuat. [18]Versi pertama dari metode OCTAVE dilaksanakan melalui berbagai workshop dan difasilitasi oleh tim analisis yang dibentuk di organisasi atau departemen TI.[20] Penelitian terdahulu menunjukkan bahwa analisis risiko dan keamanan informasi dengan metode OCTAVE berfokus pada penilaian risiko aset informasi di bawah ruang lingkup yang dibutuhkan oleh perusahaan.[21] Panduan penelitian ini menggunakan metode Octave untuk manajemen risiko keamanan teknologi informasi. Metode ini digunakan untuk melakukan identifikasi aset dan penilaian risiko keamanan informasi. untuk memungkinkan pengurangan risiko dan rekomendasi pengurangan risiko.[23] Dalam penelitian ini, metode penilaian risiko OCTAVE digunakan karena mampu berfokus pada penilaian risiko aset informasi sesuai dengan cakupan yang dibutuhkan perusahaan.[22] OCTAVE adalah pendekatan yang komprehensif, sistematis, terarah, dan dilakukan sendiri untuk evaluasi risiko keamanan informasi.[25]

Pentingnya Manajemen Risiko

Di era digital ini, manajemen risiko menjadi aspek yang semakin krusial bagi perusahaan TI. Manajemen risiko yang efektif memungkinkan perusahaan untuk mengidentifikasi, menilai, dan mengendalikan risiko yang dapat mengancam pencapaian tujuan bisnis. Pendekatan yang sistematis dan proaktif terhadap manajemen risiko dapat membantu perusahaan meminimalkan dampak dari ancaman-ancaman ini dan meningkatkan kemampuan mereka dalam merespons dan pulih dari insiden keamanan siber. Manajemen Risiko adalah alat penting yang dapat membantu organisasi dan individu untuk mencapai tujuan mereka dengan lebih efektif dan efisien. Dengan mengidentifikasi, menganalisis, dan mengelola risiko, organisasi dan individu dapat meningkatkan kinerja mereka, melindungi aset mereka, dan meningkatkan reputasi mereka.

Tentu, risiko dalam industri IT dapat berasal dari berbagai sumber, mulai dari keamanan data hingga masalah infrastruktur teknologi. Berikut adalah latar belakang umum yang sering muncul dalam jurnal risiko yang terjadi pada perusahaan di bidang IT:

1.1.1 Keamanan Data dan Privasi: Ancaman keamanan data seperti serangan peretasan, malware, dan kebocoran informasi pribadi menjadi salah satu risiko utama bagi perusahaan IT. Jurnal dapat membahas strategi mitigasi, kebijakan keamanan, dan insiden keamanan yang terjadi.

1.1.2 Kerentanan Infrastruktur: Risiko terkait dengan kegagalan infrastruktur IT seperti pemadaman sistem, gangguan jaringan, atau kegagalan perangkat keras dapat menyebabkan gangguan operasional yang signifikan bagi perusahaan. Jurnal mungkin menyoroti praktik manajemen risiko dan pemulihan bencana.

1.1.3 Kepatuhan Regulasi: Perusahaan IT harus mematuhi berbagai peraturan dan regulasi, seperti GDPR (General Data Protection Regulation) di Uni Eropa atau HIPAA (Health Insurance Portability and Accountability Act) di Amerika Serikat. Jurnal dapat mengulas tantangan kepatuhan dan strategi untuk memenuhi persyaratan regulasi.

1.1.4 Inovasi Teknologi: Meskipun inovasi teknologi dapat memberikan keuntungan kompetitif, mereka juga dapat membawa risiko tertentu, seperti kegagalan produk

atau ketidakcocokan pasar. Jurnal mungkin membahas strategi manajemen risiko untuk pengembangan produk dan layanan baru.

1.1.5 Ketergantungan pada Pihak Ketiga: Banyak perusahaan IT mengandalkan vendor, penyedia layanan cloud, atau mitra eksternal lainnya. Risiko terkait dengan kegagalan pihak ketiga atau pelanggaran keamanan pada pihak ketiga dapat menjadi perhatian penting. Jurnal mungkin menyoroti praktik pengelolaan risiko vendor dan kontrak.

1.1.6 Krisis Reputasi: Insiden keamanan atau masalah layanan teknologi dapat merusak reputasi perusahaan secara signifikan. Jurnal mungkin membahas strategi komunikasi krisis dan pemulihan reputasi setelah insiden.

1.1.7 Risiko Sumber Daya Manusia: Risiko internal seperti kesalahan manusia, kehilangan karyawan kunci, atau kekurangan keahlian teknis dapat memengaruhi operasi perusahaan IT. Jurnal mungkin mengulas strategi pengelolaan risiko sumber daya manusia dan pengembangan karyawan.

Ini hanya beberapa contoh latar belakang yang dapat menjadi fokus dalam jurnal risiko perusahaan IT. Setiap perusahaan mungkin memiliki kebutuhan dan tantangan unik yang memerlukan pendekatan khusus dalam manajemen risiko IT.

1.2 Rumusan masalah

Dengan meningkatnya jumlah serangan siber yang memanfaatkan kerentanan faktor manusia, diperlukan peningkatan kemampuan di bidang keamanan siber. Selain itu, kemampuan digital sangat penting untuk menerapkan konsep pembangunan berkelanjutan.Sangat penting untuk meningkatkan pengetahuan dan keterampilan untuk meningkatkan keamanan cyber.[9] Pada dekade kedua abad kedua puluh satu, istilah seperti "cyberculture", "cybersex", dan "cyberwar" telah digunakan untuk menggambarkan topik seperti media digital, virtual reality, dan internet. Seperti halnya dengan gerakan sastra "cyberpunk", awalan dan imbuan berbagai kata dalam budaya populer tidak jelas. Demikian pula, sejak munculnya internet, kata "network" telah menjadi metafora yang menonjol dan telah menarik perhatian hampir setiap disiplin ilmu dan institusi besar kontemporer. Pada tahun 1948, kata "cyber" digunakan untuk menunjukkan "studi tentang pesan sebagai sarana yang mengendalikan mesin dan masyarakat."[8] Rumusan masalahnya Sehubungan dengan konteks di atas, pertanyaan, "Bagaimana upaya peningkatan keamanan siber di Indonesia" ? [13]

Keamanan data dari serangan siber :

- ✓ Bagaimana melindungi infrastruktur dari serangan siber?
- ✓ Bagaimana memastikan bahwa data organisasi aman dan terlindungi?
- ✓ Bagaimana merespon insiden keamanan serangan siber ?

Fakta Cyber Security	
66%	Selama Tahun 2023 ada 66% Organisasi/Perusahaan yang terdampak dari Ransomeware
44.7%	Data menunjukan 44.7% mengambil data Login dan Password (Dampak nya menjadi ID & Password menjadi tidak aman)
	Source : Delloite annual cyber threat trends 2024 and check point, Cyber Security trends 2024

Tabel 1 - Cyber Security trends 2024

1.3 Batasan masalah

Dengan memahami batasan-batasan ini, perusahaan dapat mengambil langkah-langkah yang tepat dalam merencanakan, mengimplementasikan, dan memelihara sistem keamanan mereka untuk melindungi diri dari ancaman siber. Manajemen risiko adalah alat penting yang dapat membantu organisasi dan individu untuk mencapai tujuan mereka dengan lebih efektif dan efisien. Dengan mengidentifikasi, menganalisis, dan mengelola risiko, organisasi dan individu dapat meningkatkan kinerja mereka, melindungi aset mereka, dan meningkatkan reputasi mereka. Sistem ini berkomitmen untuk menerapkan manajemen risiko yang efektif untuk mencapai tujuannya dan memberikan nilai terbaik bagi para pemangku kepentingan. Dengan mengidentifikasi, menganalisis, dan mengelola risiko, Perusahaan di bidang Teknologi Informasi dapat meningkatkan kinerja dan reputasinya, serta meningkatkan kepercayaan investor dan pemangku kepentingan lainnya. Menurut Buzan (1998), ada tiga model keamanan yang mempelajari bidang siber: hypersecurity, everyday security practice, dan tech notification yang digunakan oleh ahli siber untuk melakukan hypersecurity (Hansen & Nissenbaum, 2009, hal. 1171). Konsep keamanan siber atau cyber security sendiri merupakan implementasi dari ketiga model sekuritisasi (Hansen & Nissenbaum, 2009, hal. 1171). [13] Untuk mengukur risiko bisnis e-commerce, ada berbagai pendekatan yang dapat digunakan, yang bervariasi tergantung pada standar, spesifikasi, karakteristik bisnis, dan reorganisasi organisasi. Pengukuran risiko cybercrime dalam e-commerce adalah proses yang dilakukan untuk mengidentifikasi, menganalisis, serta mengevaluasi kemungkinan kerugian finansial dan reputasi yang dapat ditimbulkan oleh serangan cyber. [14]

1.4 Tujuan Penelitian

1.4.1 Meningkatkan Ketahanan Terhadap Serangan Siber mengembangkan sistem dan infrastruktur yang kuat untuk mengidentifikasi, mencegah, dan merespons serangan siber secara efektif. Hasil yang Diharapkan: Mengurangi frekuensi dan dampak serangan siber, serta mempercepat pemulihan setelah insiden.

1.4.2 Memperkuat Keamanan Infrastruktur Teknologi mengimplementasikan praktik terbaik dalam pengelolaan dan pengamanan infrastruktur TI, termasuk perangkat, jaringan, dan sistem yang terintegrasi. Hasil yang Diharapkan: Mengurangi kerentanan terhadap eksploitasi dan meningkatkan keamanan keseluruhan jaringan perusahaan.

1.5 Manfaat

Membuat sistem keamanan untuk mengatasi ancaman dari siber membawa berbagai manfaat bagi perusahaan teknologi informasi. Berikut adalah beberapa manfaat utama:

1.5.1 Perlindungan Data Sensitif: Sistem keamanan yang kuat membantu melindungi data sensitif perusahaan dari akses yang tidak sah, pencurian, atau manipulasi oleh pihak yang tidak berwenang. Ini termasuk data pelanggan, informasi keuangan, dan rahasia dagang.

1.5.2 Melindungi Reputasi Perusahaan: Insiden keamanan siber dapat merusak reputasi perusahaan dan mengurangi kepercayaan pelanggan. Dengan mencegah serangan siber dan menjaga data pelanggan tetap aman, perusahaan dapat mempertahankan reputasi yang baik dalam industri.

1.5.3 Ketahanan Terhadap Ancaman Masa Depan: Dengan membangun sistem keamanan yang adaptif dan fleksibel, perusahaan dapat lebih mudah beradaptasi dengan ancaman baru yang muncul di masa depan. Ini

memungkinkan perusahaan untuk tetap bersaing dan berkembang di lingkungan yang berubah dengan cepat.

Dengan demikian, membuat sistem keamanan untuk menghadapi ancaman dari siber bukan hanya investasi untuk melindungi perusahaan dari risiko, tetapi juga merupakan strategi bisnis yang cerdas untuk memastikan kelangsungan dan pertumbuhan jangka panjang. Penelitian ini meningkatkan pengetahuan tentang jenis serangan cyber, teknik yang digunakan oleh penyerang, dan kerentanan sistem yang ada. Ini meningkatkan kesadaran dan kewaspadaan terhadap ancaman cyber di kalangan individu, kelompok, dan masyarakat umumnya. [19]

1.6 Sistematika pembahasan

Dalam pembahasan mengenai pembuatan sistem keamanan untuk menghadapi ancaman siber, sistematika yang tepat dapat membantu memandu pembahasan agar terstruktur dan mudah dipahami. Sistematika pembahasan adalah kerangka atau urutan logis yang digunakan untuk membahas suatu topik. Sistematika yang baik akan membantu pembahasan menjadi lebih terstruktur, sistematis, dan mudah dipahami.

BAB 1 Pendahuluan

BAB 2 Tinjauan Pustaka

BAB 3 Metode Penelitian

BAB 4 Hasil

BAB 5 Pembahasan

BAB 6 Kesimpulan dan Saran