BAB 1
PENDAHULUAN

Pada bab pendahuluan, akan dijelaskan terkait latar belakang penelitian ini dilakukan. Secara garis besar, penelitian ini akan mengevaluasi terkait ketahanan siber atau *cyber resilience* di Institut Teknologi Kalimantan. Setelah itu, akan dijelaskan juga terkait rumusan masalah, tujuan dan manfaat dari penelitian ini. Permasalahan yang ada pada Institut Teknologi Kalimantan akan disusun kedalam kerangka pemikiran penelitian yang juga disajikan pada bab ini.

1.1 Latar belakang

Pada era digital saat ini, masyarakat semakin bergantung pada sistem dan teknologi informasi yang kompleks dan saling berhubungan untuk melakukan aktivitas sehari-hari. Mulai dari pengelolaan keuangan pribadi, penggunaan aplikasi ojek sampai dengan pengautomasian proses bisnis yang telah terintegrasi di hampir semua tingkat aktivitas individu maupun kelompok. Integrasi semacam itu telah berhasil dalam mengefisiensikan penyampaian layanan kepada masyarakat. Namun, hal tersebut dapat meningkatkan kemungkinan penyerangan siber pada sebuah sistem di masyarakat, organisasi maupun perusahaan (Sep´ulveda-Estay, et al., 2020) seiring dengan kemajuan teknologi informasi (Arianto, 2017). Ancaman dunia maya tersebut telah bergeser dari waktu ke waktu untuk mempengaruhi berbagai fungsi dunia maya, seperti dengan *Direct Denial of Service* (DDoS), pencurian data, perubahan kode data, penyerangan melalui virus komputer dan lain-lain. Dilansir dari Laporan Tahunan Honeynet Project 2019 yang berkolaborasi dengan Badan Siber dan Sandi Negara, serangan siber di Indonesia pada tahun 2019 mencapai angka 98.243.896 serangan (Badan Siber dan Sandi Negara, 2019). Bahkan, Indonesia juga berada dalam situasi yang lemah terkait keamanan sibernya (Arianto & Anggraini, 2019).

Lonjakan serangan siber di masyarakat akan menimbulkan sebuah tantangan baru dalam menjaga ketersediaan, integritas, dan kerahasiaan informasi. Serangan terhadap siber yang parah dapat menimbulkan konsekuensi dalam hal

pengiriman layanan jika operasi sistem terhenti (Annarelli, et al., 2020). Beberapa jenis organisasi yang bergantung pada teknologi informasi akan menerima dampak yang sangat besar. Bahkan, sebuah serangan siber dapat menimbulkan ancaman bagi seluruh operasi bisnis. Sebagai contoh, serangan siber dengan memanfaatkan *Disrtributed Denial of Service* (DDOS) di Georgia (2008) berhasil melumpuhkan aktivitas negara dikarenakan banyak sektor kritis yang diserang (Rahmawati, 2017). Pada tingkat organisasi, serangan siber juga dapat terjadi seperti pada perusahaan SZ DJI Technology Co., Ltd tahun 2017. Serangan pada perusahaan DJI tahun 2017 berupa *cracking* yang memanfaatkan kode debug pengembangan *drone* untuk dapat mengendalikan hasil produksi *drone* melalui *backdoor* (Adianto, et al., 2020). Selain itu, terdapat juga kasus pencurian *username* dan *password* yang dialami oleh situs Tiket.com dengan kerugian hingga Rp4,1 miliar (Perdani, et al., 2018).

Dengan berbagai perlindungan terhadap teknologi informasi untuk melawan ancaman siber, para peneliti di seluruh dunia semakin mencari cara untuk merancang sebuah infrastruktur siber yang tangguh dan dapat bertahan, tidak hanya dari kegagalan stokastik tetapi juga serangan yang ditargetkan (Choudhury, et al., 2015). Ketahanan siber atau *cyber resilience* merupakan kemampuan sistem dalam mempersiapkan, menyerap, memulihkan, dan beradaptasi dengan efek yang dapat merugikan, terutama terkait dengan serangan siber (Linkov & Kott, 2019). Ketahanan siber memastikan bahwa sebuah sistem dan teknologi informasi dapat menerima respon setelah terjadi penyerangan dan mengembalikan keadaan seperti semula agar operasi layanan tetap berjalan. Dalam dunia luas, ketahanan siber juga dapat diartikan sebagai kemampuan dalan pertahanan dan pemulihan jika insiden dunia maya terjadi dan kembali ke keadaan layaknya fungsi normal (Williams & Manheke, 2010).

Organisasi telah mencegah teknologi informasi yang diterapkan tidak terlibat dalam aktivitas penyerangan siber, seperti menyebarkan spam dan email *phishing*. Namun, langkah pencegahan juga perlu diiringi dengan pengadaptasian, dimana organisasi bertindak seolah-olah ancaman akan menyerang sistem yang ada. Pada instansi yang bergerak pada bidang pendidikan, sistem TI berperan penting dalam kegiatan operasional perusahaan, seperti pengelolaan data

akademik. Oleh karena itu, ketahanan siber juga menjadi komponen yang penting dari misi perlindungan infrastruktur kritis, dan elemen kunci dari proposisi nilai untuk kemitraan dengan pemerintah karena mengedepankan kebutuhan akan keamanan dan keandalan operasi bisnis (NIAC, 2009). Dalam memastikan ketahanan siber dari infrastruktur kritis dan sistem lainnya, sistem perlu secara dinamis mengkonfigurasi ulang dirinya sendiri dalam menanggapi kejadian di dalam maupun di luar lingkungan sistem tersebut, termasuk pengaruh lingkungan yang tidak berbahaya dan insiden siber (Koelemeijer, 2018).

Beberapa peneliti telah melakukan penelitian terkait *cyber resilience*. Terdapat penelitian yang dilakukan untuk mendapatkan rekomendasi dalam peningkatan ketahanan siber, yaitu rekomendasi ketahanan siber pada sektor energi (Hagen, 2018), sektor pemerintah (Tonhauser & Ristvej, 2019) (Srinivas, et al., 2019) dan sektor pembangunan negara (Chang & Coppel, 2020). Sebuah sistem kontrol industri atau *Industrial Control System* (ICS) juga dilakukan penelitian terkait perumusan metriks ketahanan jaringan ICS secara keseluruhan (Haque, et al., 2018) dan alat untuk dapat menilai dan mengevaluasi ketahanan siber (Haque, et al., 2019). Penelitian terkait ketahanan siber juga dilakukan pada sektor infrastruktur kritis, yaitu evaluasi infrastruktur kritis berdasarkan kasus penjaminan (Koelemeijer, 2018) dan evaluasi melalui penilaian statistik (Rehak, et al., 2019). Terakhir, juga dilakukan penilaian ketahanan siber dengan berbagai metode, yaitu dengan kerangka kerja penilaian ketahanan siber (*Cyber Resilience Assessment Framework*) (Sep´ulveda-Estay, et al., 2020) dan *Data Flow Material Model* (DFMM) (Alghamdi & Rastogi, 2020).

Institut Teknologi Kalimantan (ITK) merupakan salah satu perguruan tinggi negeri di Indonesia. ITK dibentuk dengan tujuan untuk menyelenggarakan program pendidikan akademik pada sejumlah rumpun ilmu pengetahuan dan teknologi (IPTEK) tertentu, khususnya di Kalimantan. Saat ini, ITK memiliki 5 jurusan dan 17 program studi dan terus bertambah tiap tahunnya. Menurut data dari Pangkalan Data Pendidikan Tinggi (PDDikti), pada pelaporan periode 2019/2020 ganjil, mahasiswa ITK berjumlah 3247 orang. Proses pelaksanaan akademik menjadi penting dalam mendukung pencapaian tujuan perguruan tinggi. Kegiatan di perguruan tinggi dapat terlaksana dengan adanya aktivitas atau

proses, diantaranya adalah dapat berupa proses pelayanan akademik, proses kemahasiswaan, proses rencana studi dan proses lainnya yang berlaku untuk pemangku kepentingan ITK (APQC, 2014). Tentunya, menjalankan proses bisnis di ITK perlu didukung dengan teknologi informasi agar proses yang berjalan dapat dilakukan secara efektif dan efisien. Hal ini akan membutuhkan perencanaan yang matang dalam implementasi teknologi informasi kedepannya (Sihotang, 2015).

Dalam memastikan keselarasan antara proses bisnis dengan teknologi informasi, dibutuhkan sebuah tata kelola teknologi informasi yang baik. Tata kelola teknologi informasi merupakan bagian dari pengelolaan organisasi secara keseluruhan yang terdiri dari struktur dan proses untuk memastikan kelanjutan TI organisasi dan pengembangan strategi dari tujuan organisasi (Sihotang & Sagala, 2015). Pada perguruan tinggi, tata kelola teknologi informasi diatur olehn Peraturan Menteri Riset, Teknologi dan Pendidikan Tinggi Nomor 62 Tahun 2017. Peraturan ini mengharuskan setiap perguruan tinggi untuk mengimplementasikan tata kelola teknologi informasi berupa struktur tata kelola teknologi informasi, arsitektur organisasi, tata kelola pengembangan, tata kelola layanan dan tata kelola pengawasan. Tata kelola teknologi informasi menjadi penting karena dapat membantu organisasi dalam mengambil keputusan dengan cepat.

Pada penelitian terdahulu (Atrinawati, et al., 2020), ITK telah merancang sebuah tata kelola teknologi informasi di tahun 2020. Penelitian ini menggunakan *framework* COBIT 2019 dalam mengukur *design factor* ITK. Setelah dilakukan penilaian *design factor*, didapatkan proses tata kelola dan manajemen yang memiliki prioritas lebih dari 50 poin untuk ITK. Proses yang memiliki nilai paling tinggi yaitu proses manajemen keamanan di ITK dengan nilai 115 dan target level kapabilitas 4. Hal ini membuktikan bahwa manajemen keamanan khususnya data dan informasi di ITK sangat penting dan perlu mendapatkan perhatian yang khusus.

Manajemen keamanan dilakukan untuk meminimalisir ancaman siber yang dapat berdampak negatif pada kegiatan operasional ITK. Selain itu, hal ini juga dapat berdampak pada kecepatan pengiriman layanan, dimana layanan yang

dimaksud adalah layanan akademik. Jika terjadi ancaman siber yang tidak terduga, tentu akan berdampak dari berbagai sektor dan akan menghambat salah satu misi ITK yaitu menyelenggarakan proses pendidikan berbasis teknologi. Sebelumnya, ITK pernah mengalami serangan siber yaitu seseorang yang mencoba untuk meretas data akademik di ITK. Namun, UPT TIK di ITK telah menyadari dan memperbaiki sistem keamanan di ITK agar data-data akademik tetap terlindungi. Jika data-data berhasil diretas, maka akan sangat berdampak di berbagai unit organisasi. Tentunya, proses perbaikan dan peningkatan keamanan data membutuhkan waktu yang cukup lama dan akan berakibat pada proses pengiriman layanan akademik di ITK. Oleh karena itu, ITK perlu untuk meningkatkan ketahanan siber agar dapat bertahan dan beradaptasi jika terjadi ancaman siber. Tingkat kematangan dalam mempersiapkan ancaman siber merupakan kunci dari ketahanan siber. Namun, sampai saat ini ITK belum menerapkan sebuah kerangka kerja untuk mengimplementasikan praktik manajemen keamanan dan data untuk meningkatkan ketahanan siber. Jika ketahanan siber di ITK telah mencapai kematangan yang tinggi, proses untuk memulihkan kembali layanan akademik dapat lebih cepat dari sebelumnya. Sehingga, dapat dikatakan bahwa proses dalam pengamanan data dan informasi di ITK belum maksimal.

Berangkat dari permasalahan tersebut, dapat disimpulkan bahwa ITK membutuhkan langkah-langkah yang tepat untuk dapat meningkatkan ketahanan siber. Penelitian akan dilakukan terkait evaluasi ketahanan siber atau *cyber resilience* di ITK dengan *framework Cyber Resilience Review*. Penelitian dimulai dengan mengevaluasi melalui penilaian tingkat ketahanan siber yang telah diimplementasikan di ITK. Setelah itu, akan dilakukan analisis celah dan rekomendasi langkah-langkah dalam meningkatkan ketahanan siber di ITK. Penelitian ini akan menghasilkan sebuah rencana untuk pihak ITK agar dapat meningkatkan ketahanan siber dengan praktik-praktik yang terdokumentasi pada kerangka kerja *Cyber Resilience Review*. Dengan adanya rencana peningkatan ketahanan siber di ITK melalui kerangka kerja *Cyber Resilience Review*, pihak ITK dapat mempersiapkan teknologi informasi dan komunikasi di ITK dan merespon sebuah ancaman siber dengan baik. Hal ini bertujuan untuk

memperlancar kegiatan operasional perusahaan dan mencapai tujuan perusahaan, walaupun terjadi ancaman siber sewaktu-waktu.

1.2 Perumusan Masalah

Pada Institut Teknologi Kalimantan, memiliki permasalahan utama yaitu belum memaksimalkan praktik dalam peningkatan ketahanan siber melalui sebuah kerangka kerja. Oleh karena itu, dirumuskan pertanyaan penelitian sebagai berikut.

1. Bagaimana hasil dari proses evaluasi praktik-praktik ketahanan siber di ITK pada setiap *Cyber Resilience Domain*?
2. Apa saja *gaps* atau celah yang perlu ditingkatkan oleh ITK?
3. Bagaimana proses perencanaan dalam meningkatkan ketahanan siber pada setiap *Cyber Resilience Domain* di ITK?

1.3 Tujuan Penelitian

Penelitian ini dilakukan atas dasar beberapa tujuan, yaitu sebagai berikut.

1. Mendapatkan hasil dari proses evaluasi praktik-praktik ketahanan siber di ITK pada setiap *Cyber Resilience Domain*
2. Menentukan *gaps* atau celah yang perlu ditingkatkan oleh ITK
3. Menghasilkan rencana peningkatan ketahanan siber pada setiap *Cyber Resilience Domain* di ITK

1.4 Ruang Lingkup Penelitian

Dalam menentukan lingkup penelitian, disusun ruang lingkup penelitian yaitu penelitian ini berfokus pada evaluasi ketahanan siber di Institut Teknologi Kalimantan dengan kerangka kerja *Cyber Resilience Review*. Pada tahapan melakukan evaluasi, penelitian ini menggunakan metode *self-assessment*. Setelah itu, evaluasi 10 *Cyber Resilience Domain* melingkupi layanan akademik di ITK dengan menggunakan aplikasi Gerbang ITK, yaitu yang berisikan Sistem Informasi Akademik dan Kemahasiswaan.

Penelitian ini menggunakan metodologi sesuai dengan rekomendasi CRR, namun proses *implement plans* tidak dilakukan pada penelitian ini. Hal ini

dikarenakan proses *implement plans* merupakan sebuah proses untuk menyusun *timeline* implementasi rencana yang telah dibuat dengan mempertimbangkan sumberdaya, anggaran dan program kerja lainnya di ITK. Sehingga lebih tepatnya ITK yang menyusun implementasi rencana yang telah dibuat dari hasil penelitian ini.

1.5 Manfaat Penelitian

Manfaat yang didapatkan dengan penelitian ini sebagai berikut.

1. Mengurangi kerugian finansial dengan memberikan keamanan dan ketahanan keseluruhan pada sistem
2. Menjaga kelangsungan operasi layanan ITK jika terjadi serangan siber atau pembobolan keamanan
3. Memungkinkan ITK untuk mengembangkan proaktif yang lebih besar dalam menangani *risks*, *vulnerabilities*, dan *contingencies*
4. Menjaga reputasi ITK dengan menyediakan sistem keamanan data yang telah terdokumentasi
5. Menambah pengetahuan terkait praktik-praktik ketahanan sistem untuk mendukung keberlanjutan layanan ITK.

1.6 Kerangka Pemikiran Penelitian

Dalam menyusun kerangka pemikiran penelitian, dibuat diagram sebab akibat atau *fishbone diagram* sebagai berikut. Gambar 1.1 merupakan diagram sebab akibat yang menjelaskan kerangka berpikir penelitian ini dengan landasan kajian literatur dari peneliti. Diagram yang disajikan memiliki beberapa faktor, yaitu manusia, regulasi, lingkungan dan metode. Setelah itu, dilakukan analisis dan didapatkan sebuah usulan untuk penelitian.

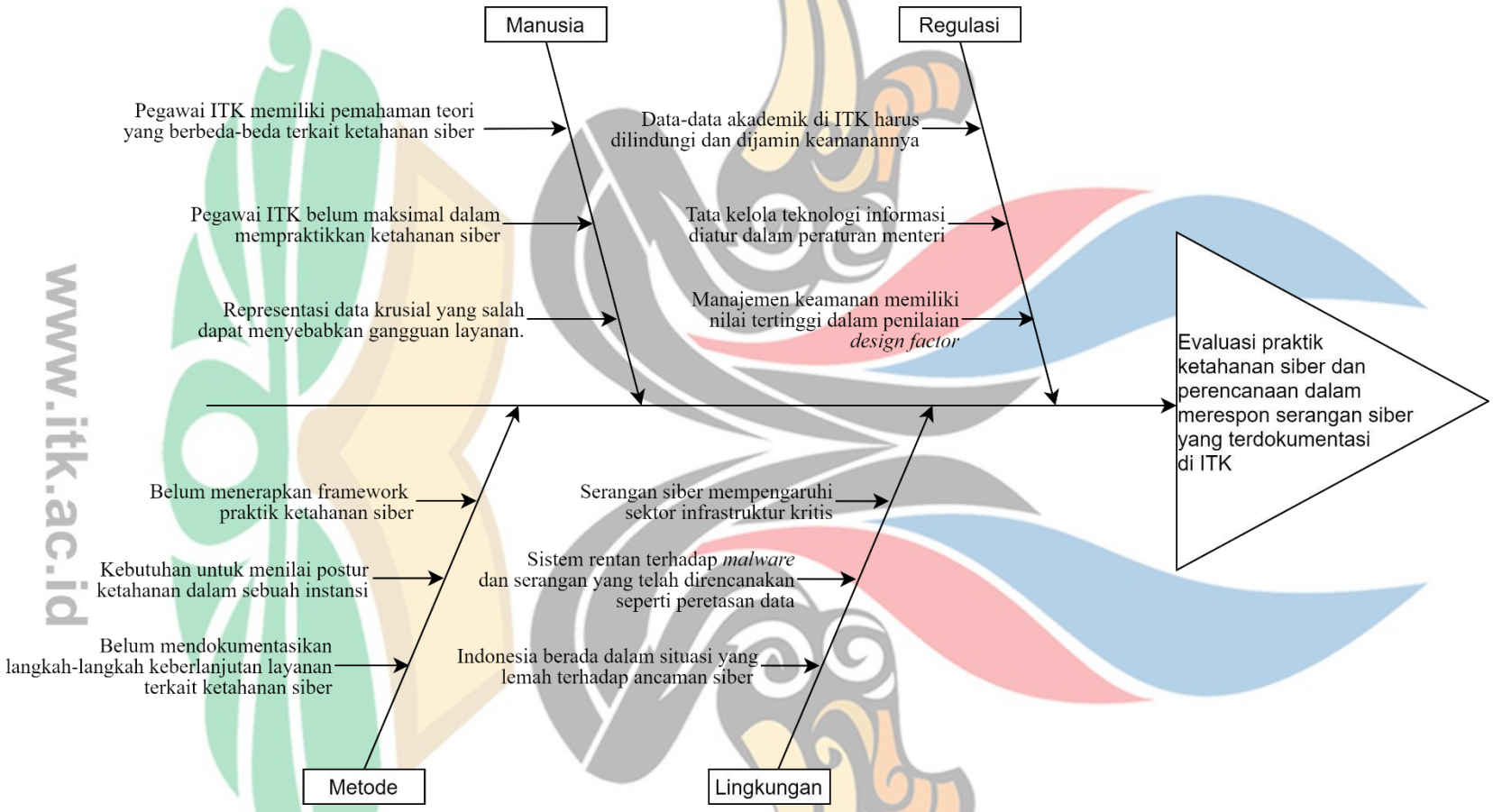
Pada faktor manusia, terdapat beberapa sebab yang didapatkan berdasarkan pengetahuan dan kesadaran dari sumber daya manusia. Adapun sebab pertama yaitu pegawai memiliki pemahaman yang berbeda-beda terkait ketahanan siber. Setelah itu, terdapat permasalahan yang didapatkan karena pegawai yang belum maksimal dalam mempraktikkan ketahanan siber. Terakhir, terdapat

permasalahanan dikarenakan representasi yang salah dari data krusial, sehingga dapat menyebabkan gangguan layanan.

Setelah itu, terdapat faktor regulasi yang didapatkan berdasarkan aturan dan standar yang berlaku. Penyebab pertama yaitu tata kelola teknologi informasi yang diatur oleh Peraturan Menteri Ristekdikti Nomor 62 Tahun 2017. Selanjutnya, manajemen keamanan memiliki nilai tertinggi pada penilaian *design factor* di ITK. Terakhir, data-data akademik di ITK juga perlu dilindungi dan dijamin keamananannya. Selanjutnya, terdapat faktor lingkungan yang didapatkan berdasarkan ancaman yang datang dari luar ITK. Adapun sebab pertama yaitu Indonesia dikatakan sangat lemah terhadap ancaman siber. Serangan siber mempengaruhi sektor infrastruktur kritis juga menjadi penyebab pada faktor lingkungan. Data-data yang ada di ITK juga harus dilindungi dan dijamin keamanannya. Sistem juga dapat dikatakan rentan terhadap *malware* dan serangan yang telah direncanakan.

Terakhir, terdapat faktor metode yang didapatkan berdasarkan kerangka kerja maupun metode yang digunakan pada ITK. Penyebab pertama didapatkan bahwa perusahaan belum menerapkan *framework* praktik ketahanan siber. Setelah itu, ITK juga belum mendokumentasikan langkah-langkah keberlanjutan layanan terkait ketahanan siber. Selain itu, juga dibutuhkan untuk menilai ketahanan postur dalam sebuah instansi.

Dari kerangka pemikiran yang disajikan, dapat disimpulkan bahwa sebuah ketahanan siber merupakan permasalahan yang umum, namun perlu dilirik oleh organisasi. Jika dilakukan sebuah penilaian ketahanan siber, tentu akan sangat membantu dalam keberlanjutan layanan perusahaan. Oleh karena itu, dapat diusulkan bahwa perlunya evaluasi ketahanan siber di suatu perusahaan agar dapat melihat kondisi saat ini dan di masa mendatang. Setelah itu, juga diperlukan perencanaan dalam merespon serangan siber yang terdokumentasi untuk meningkatkan ketahanan siber di perusahaan.



Gambar 1.1 Kerangka Pemikiran Penelitian