PENERAPAN MANAJEMEN RISIKO PADA KEAMANAN INFORMASI DAN TEKNOLOGI PADA PERUSAHAAN FINTECH BERDASARKAN STANDARD ISO/IEC 27001:2013 (STUDI KASUS PERUSAHAAN FINTECH X)

TESIS

Oleh:

Kevin Bastian Sirait

2017811012

Pembimbing:

Dr. Ir. Batara Maju Simatupang, MT., MPhil., CIMBA®

PROGRAM MAGISTER MANAJEMEN

FAKULTAS EKONOMI

UNIVERSITAS KATOLIK PARAHYANGAN

BANDUNG

JULI 2019

PENERAPAN MANAJEMEN RISIKO PADA KEAMANAN INFORMASI DAN TEKNOLOGI PADA PERUSAHAAN FINTECH BERDASARKAN STANDARD ISO/IEC 27001:2013 (STUDI KASUS PERUSAHAAN FINTECH X)

TESIS

Oleh:

Kevin Bastian Sirait

2017811012

Pembimbing:

Dr. Ir. Batara Maju Simatupang, MT., MPhil., CIMBA®

PROGRAM MAGISTER MANAJEMEN

FAKULTAS EKONOMI

UNIVERSITAS KATOLIK PARAHYANGAN

BANDUNG

JULI 2019

HALAMAN PENGESAHAN

PENERAPAN MANAJEMEN RISIKO PADA KEAMANAN INFORMASI DAN TEKNOLOGI PADA PERUSAHAAN FINTECH BERDASARKAN STANDARD ISO/IEC 27001:2013 (STUDI KASUS PERUSAHAAN FINTECH X)

Oleh:

Kevin Bastian Sirait

2017811012

Persetujuan untuk Sidang Tesis pada Hari/Tanggal:

Sabtu, 27 Juli 2019

Pembimbing:

Dr. Ir. Batara Maju Simatupang, MT., MPhil., CIMBA®

PROGRAM MAGISTER MANAJEMEN

FAKULTAS EKONOMI

UNIVERSITAS KATOLIK PARAHYANGAN

BANDUNG

JULI 2019

PERNYATAAN

Yang bertandatangan di bawah ini, saya dengan data diri sebagai berikut:

Nama	:	Kevin Bastian Sirait
Nomor Pokok Mahasiswa	:	2017811012
Program Studi	:	Magister Manajemen
		Fakultas Ekonomi
		Universitas Katolik Parahyangan

Menyatakan bahwa Tesis dengan judul:

Penerapan Manajemen Risiko Pada Keamanan Informasi dan Teknologi Pada Perusahaan Fintech Berdasarkan Standard ISO/IEC 27001:2013 (Studi Kasus Perusahaan Fintech X)

adalah benar-benar karya saya sendiri di bawah bimbingan Pembimbing, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non formal dari pihak lain berkaitan dengan keaslian karya saya ini, saya siap menanggung segala resiko, akibat, dan/atau sanksi yang dijatuhkan kepada saya, termasuk pembatalan gelar akademik yang saya peroleh dari Universitas Katolik Parahyangan.

Dinyatakan : di Bandung
Tanggal : 27 Juli 2019

Kevin Bastian Sirait

PENERAPAN MANAJEMEN RISIKO PADA KEAMANAN INFORMASI DAN TEKNOLOGI PADA PERUSAHAAN FINTECH BERDASARKAN STANDARD ISO/IEC 27001:2013 (STUDI KASUS PERUSAHAAN FINTECH X)

Kevin Bastian Sirait (NPM: 2017811012)
PEMBIMBING: Dr. Ir. Batara Maju Simatupang, MT., MPhil., CIMBA®
Magister Manajemen
Bandung
Juli 2019

ABSTRAK

Tujuan utama dari penelitian ini ialah untuk menemukan sumber-sumber serangan *cyber* dan dampak yang ditimbulkannya pada perusahaan *financial technology* (fintech) X pada periode 2014-2019. Objek penelitian adalah perusahaan fintech X yang bergerak dibidang *micro-payment gateway*. Metodologi yang digunakan adalah metode *fault tree analysis* untuk menemukan sumber-sumber yang dapat memicu terjadinya serangan *cyber*. Sedangkan untuk estimasi kerugian finansial yang timbul akibat kejadian risiko dari sumber tersebut, digunakan metode *single loss expectancy*, dan untuk menemukan estimasi kerugian dalam kurun waktu tahunan digunakan metode *annualized loss expectancy*. Hasil riset mengungkapkan, bahwa sumber ketidaktahuan pengguna dan penggunaan identitas personel perusahaan sebagai pemicu terjadinya insiden penipuan, dimana modus penipuan termasuk pada jenis *social engineering*. Untuk insiden penyalahgunaan akun, terjadi akibat ketiadaan sistem yang dapat membaca perilaku para pengguna. Untuk estimasi kerugian finansial, ditemukan bahwa pada modus penipuan dengan jenis *social engineering* memiliki estimasi kerugian yang lebih besar untuk setiap insiden daripada rata-rata estimasi kerugian tahunan pada periode penelitian. Sedangkan untuk insiden penyalahgunaan akun, ditemukan bahwa estimasi kerugian finansial dalam kurun waktu tahunan lebih besar daripada estimasi kerugian untuk setiap insiden yang terjadi pada periode penelitian. Adapun untuk mitigasi serangan *cyber* jenis *social engineering*, diterapkan konsep *customer due diligence*, dan penerapan sistem *big data* digunakan untuk mendeteksi perilaku yang mencurigakan dari penggunaan aplikasi. Terkait temuan yang terdapat pada perusahaan fintech X, ditemukan bahwa perusahaan fintech X tidak memenuhi tujuan bagian 16.1 pada bagian annex A pada standard ISO/IEC 27001:2013 terkait pencatatan atau dokumentasi terhadap insiden yang berorientasi terhadap keamanan informasi dan teknologi.

Kata Kunci: Identifikasi Sumber, Fintech, Serangan *Cyber*, *Fault Tree Analysis*

THE RISK MANAGEMENT IMPLEMENTATION ON INFORMATION AND TECHNOLOGY SECURITY IN THE FINTECH FIRM BASED ON ISO/IEC 27001:2013 STANDARD (FINTECH FIRM X CASE STUDY)

Kevin Bastian Sirait (NPM: 2017811012)
SUPERVISOR: Dr. Ir. Batara Maju Simatupang, MT., MPhil., CIMBA®
Master of Management
Bandung
July 2019

ABSTRACT

The primary objectives of this research are to find the sources that trigger the incident of cyber attacks and the impact it causes to the financial technology (fintech) firm X in the period of 2014 to 2019. Regarding the object of this research, fintech firm X is operating in the area of the micro-payment gateway. The methodologies used in this research are the fault tree analysis to find the sources that can trigger the incident of the cyber attack. Meanwhile, the single loss expectancy and annualized approach are used to estimating the financial losses; to be precise, in finding the financial losses estimations per-incident and annually, respectively. Based on the research conducted in the fintech firm X, it is uncovered that the lack of information on its users and the use of the company personnel triggers the incident of fraudulent activities; in which, these fraudulent activities are classified as social engineering attacks. On the other hand, the incident of application misuse was triggered by the lack of systems that has the capability to analyze its user behaviors. In terms of the financial losses estimation from the identified sources, it is found that the incident of fraudulent activity has higher financial losses estimation per-incident than its yearly losses estimation. Meanwhile, the incident misuse of the application has higher financial losses estimation annually compared to the financial losses estimation per-incident. In regards to the solution that can be applied by the fintech firm X to mitigate cyber-attacks in the form of fraudulent activities that are classified into social engineering attacks and the misuse of application, the concept of customer due diligence can be applied to mitigate the risk of fraudulent activities, and the implementation of big-data based system to detect any suspicious activities on its to mitigate the risk of the application of fintech firm X are misused by its users. Finally, in regards to the finding from the fintech firm X, it is found that the fintech firm X is not fulfilling the objectives of Annex A section 16.1 of ISO/IEC 27001:2013 standard in regards to the documentation of incident or findings which are oriented in the area of information and technology security; the objective of section 16.1 in the Annex A of ISO/IEC 27001:2013 is not fulfilled in terms of the documentation and reporting mechanism of incidents in the area of information and technology security.

***Keywords**: Source Identification, Fintech, Cyber Attacks, Fault Tree Analysis*

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya yang telah diberikan kepada penulis dalam penyusunan tesis ini. Tesis ini disusun dalam rangka memenuhi salah satu syarat akademik dalam memperoleh gelar Magister Manajemen pada Universitas Katolik Parahyangan di Bandung. Dalam pembuatan tesis ini, penulis mendapat bantuan dan dukungan dari berbagai pihak. Dikarenakan hal tersebut, dalam kesempatan ini penulis ingin menyampaikan rasa hormat dan terima kasih yang sebesar-besarnya kepada:

- Dosen pembimbing, Dr. Ir. Batara Maju Simatupang, MT., MPhil., CIMBA® atas saran, masukan, arahan, kesabaran dan ilmu yang diberikan kepada penulis. Dimana, hal tersebut membantu saya dalam memperoleh kesempatan untuk mengikuti konferensi internasional, lomba dan terutama, memberikan saya kesempatan dalam menyelesaikan tesis ini.

- Dosen penguji, Dr. Franciskus Antonius Alijoyo, Drs., MM. dan Dr. Franciscus Haryanto, S.E., M.M. yang telah memberikan saya masukan, rekomendasi, sudut pandang baru dan ilmu terkait konsep manajemen risiko dalam menyelesaikan tesis ini.

- Kepada orang tua penulis, Ir. Rudy Yanto Sirait dan Helen Carolina Sembiring dan adik penulis, Daniel Tanta Christopher Sirait yang telah memberikan dukungan moril, doa, materil dan perhatian kepada penulis. Terutama terhadap proses penyelesaian program studi dan pengerjaan tesis.

- Kepada pihak perusahaan Fintech X, yang telah memberikan kesempatan, data dan informasi yang dibutuhkan dalam menjalankan kegiatan tesis terkait tema penerapan manajemen risiko dibidang keamanan informasi dan teknologi.

- Kolega penulisan jurnal internasional dan artikel untuk lomba manajemen risiko, Handy Andriyas yang telah membantu penulis dalam menghasilkan salah satu karya akademik yang akan dipresententasikan di Bali pada bulan Agustus tahun 2019.

- Kepada Beby Prilly, Hans Gerald, Mikael Abraham dan Ivonne Bonita sebagai kolega pengerjaan tesis dan disaat yang sama menjadi penghibur kepada penulis dalam menghadapi tantangan, proses pengerjaan dan suka duka dalam menyelesaikan tesis dan pembuatan jurnal untuk konferensi internasional.

- Kepada sesama rekan kelas program studi magister manajemen dan seperjuangan tesis, Ignatius Bryan, Fernando Sijabat, Anita Puteri, Steffi Priani, Yohannes Billy, Sandy Suryajaya, Muhammad Sri Sadono, Uchenna Collins, Edgar Ngao, Demetrius Kunto, Livia Natasha, Felina Kusnakhin, Setiadi Aloysius, Widra Kristian, Bernardi Avriadi, Felix Indrawan dan Adi Pamungkas yang telah memberikan semangat, dukungan dan terutama, menjadi teman dalam pendewasaan diri baik secara keilmuan dan karakter selama studi di progam magister manajemen Universitas Katolik Parahyangan.

- Semua pihak yang tidak dapat disebutkan satu persatu yang telah membantu penulis dalam menyelesaikan tesis ini.

Akhir kata, penulis menyadari bahwa tesis ini masih jauh dari sempurna. Dikarenakan hal tersebut, penulis dengan senang hati menerima setiap saran dan kritik yang membangun untuk dapat melengkapi dan menyempurnakan tesis ini. Setiap saran dan kritik yang diterima diharapkan dapat membantu para pembaca dalam memperdalam ilmu manajemen risiko maupun menggunakan tesis ini sebagai referensi dalam menghasilkan karya akademik atau non-akademik terkait implementasi manajemen risiko dibidang informasi dan teknologi. Terima kasih.

Bandung, 27 Juli 2019

Penulis

Kevin Bastian Sirait

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi pada era revolusi industri 4,0 telah berdampak pada setiap kegiatan ekonomi di masyarakat. Bahkan aplikasi digitalisasi pada *financial technology* (fintech) sudah merasuki setiap aspek kehidupan masyarakat. Perkembangan tersebut ditandai dengan munculnya perusahaan-perusahaan perintis (*startup companies*) yang menawarkan berbagai kemudahan yang dapat diakses secara digital (*online*) dengan menggunakan perangkat yang berbasis *web-based* atau *mobile*. Didalam konteks perusahaan fintech, Financial Stability Board (2017) membagi kegiatan finansial yang dilakukan oleh perusahaan fintech kedalam lima kategori, yaitu: (1) *payment, clearing* dan *settlement*; (2) *deposits, lending* dan *capital raising*; (3) *insurance*; (4) *invesment management* dan (5) *market support*. Kelima kategori dari segmen bisnis fintech ini telah turut meningkatkan volume transaksi ekonomi digital Indonesia.

Menurut Anandan et al. (2018), ekonomi digital Indonesia dapat mengalami pertumbuhan dengan nilai sebesar US$ 100 miliar atau setara dengan Rp. 1.411 triliun pada tahun 2025. Bahkan kini, perusahaan startup di Indonesia telah mampu menembus valuasi dengan kategori *unicorn* atau setara dengan US$ 1 miliar, perusahaan-perusahaan tersebut merupakan Tokopedia, Bukalapak, Traveloka dan Go-jek (Tanuwidjaja & Quan, 2018). Serta, Anandan et al. (2018) menambahkan bahwa salah satu perusahaan *startup* di Asia tenggara yang memiliki status *decacorn* atau perusahaan yang memiliki nilai valuasi setara dengan US$ 10 miliar ialah Grab Holding Inc yang bergerak dibidang jasa transportasi. Pollari & Ruddenklau (2019) menambahkan bahwa dengan adanya perkembangan teknologi yang cepat, hal tersebut mendukung adanya kolaborasi antara perusahaan

tradisional dengan perusahaan fintech dan mendorong perusahaan tradisional untuk melakukan transformasi digital. Proses transformasi digital dan kolaborasi dengan perusahaan berbasis teknologi dapat mendorong perusahaan tradisional untuk meningkatkan kualitas dari penerapan kebijakan *know your customer* (KYC), pendeteksian aktivitas pencucian uang dan manajemen identitas digital. Dengan tambahan, hal tersebut memberikan kesempatan kepada perushaan berbasis teknologi untuk menyediakan jasa yang sebelumnya sudah disediakan oleh institusi tradisional dan memberikan kesempatan kepada perusahaan tersebut untuk melakukan ekspansi secara global. Secara spesifik, hal tersebut memberikan persaingan kepada institusi perbankan tradisional yang dihasilkan dari kehadiran perusahaan fintech yang menghasilkan jasa yang sama; dimana, perusahaan fintech tersebut berfokus kepada penggunaan teknologi untuk memenuhi kebutuhan para pengguna daripada perusahaan tradisional (Pollari & Ruddenklau, 2019).

Dari perkembangan volume dan nilai dari transaksi yang meningkat secara signifikan terhadap pertumbuhan ekonomi digital dan meningkatnya partisipasi perusahaan berbasi teknologi dalam menyediakan jasa yang sebelumnya ditawarkan oleh insititusi tradisional, hal tersebut membutuhkan pengawasan kinerja perusahaan secara *real-time* dan perusahaan tersebut dituntut untuk mampu mengidentifikasi kebutuhan dari pasar, pola transaksi pengguna atau *end-user* serta mencegah adanya penyimpangan yang dilakukan oleh individu atau kelompok yang berasal dari sisi internal maupun eksternal perusahaan dalam rupa serangan *cyber* (*cyber attack*). Wroblewska et al. (2016) menjelaskan bahwa dengan perkembangan dari teknologi tersebut, terdapat sistem yang dapat menemukan pola dari transaksi dari para pengguna dan sistem tersebut mempunyai kapabilitas untuk memberikan rekomendasi produk kepada pengguna dalam melakukan transaksi digital, terutama didalam transaksi digital yang terjadi di pasar elektronik. Dengan data transaksi dan pola aktivitas pengguna yang tercatat pada sistem tersebut, serangan *cyber* berpotensi untuk membuat data pengguna maupun perusahaan terekspos untuk dicuri maupun dimanipulasi bahkan sistem tersebut berpotensi untuk dinon-aktifkan secara digital oleh para pelaku serangan *cyber*.

Serangan *cyber* mempunyai potensi untuk terjadi dalam skala global dan dapat

mempengaruhi setiap industri dan perusahaan yang mempunyai sistem informasi dan teknologi (IT). Salah satu serangan *cyber* yang mempunyai skala dan dampak global adalah *Wanna Decryptor* (WannaCry). WannaCry merupakan serangan *cyber* dengan jenis *ransomware* yang terjadi pada bulan Mei tahun 2017 yang telah mempengaruhi 99 negara dan telah mempengaruhi 57.000 pengguna sistem IT (Fritzvold, 2017). Karakteristik dari serangan tersebut adalah mengenkripsi setiap data yang dimiliki oleh para *user* dan data tersebut dapat diakses kembali dengan cara membayar nominal yang telah ditentukan oleh para *hacker* atau *attacker*. Fritzvold (2017) menambahkan bahwa serangan WannaCry terjadi dikarenakan adanya peningkatan terhadap *cybercrime* dan hal tersebut membuat serangan *cyber* menjadi risiko yang harus dihadapi oleh perusahaan menggunakan sistem IT, terutama terhadap perusahaan yang menggunakan teknologi sebagai fondasi kegiatan operasional.

Serangan *cyber* dengan jenis *ransomware* merupakan salah satu jenis dari serangan *cyber*; serangan *cyber* mempunyai kapabilitas untuk melakukan pencurian, manipulasi data dan pembajakan sistem informasi yang dimiliki oleh perusahaan maupun individu. Freund & Jones (2015) menambahkan bahwa serangan *cyber* yang terjadi tidak hanya berfokus kepada perusahaan yang menggunakan sistem IT, melainkan kepada para pengguna jasa atau aplikasi dari perusahaan tersebut. Hal tersebut dilakukan dengan cara penipuan (*fraud*) terhadap pengguna jasa atau aplikasi tersebut. Peningkatan terhadap serangan *cyber* dan *cyber crime* disebabkan oleh peningkatan konektifitas atas perangkat lunak dan perangkat keras kepada jaringan digital atau *internet*.

Serangan *cyber* yang telah terjadi berorientasi terhadap informasi dan infrastruktur yang dimiliki oleh setiap pengguna sistem IT. Pengguna IT tersebut dapat berupa penduduk sipil, perusahaan bahkan instansi pemerintahan. Dalam menanggapi serangan *cyber* yang terjadi kepada para pengguna sistem IT ialah dengan menerapkan sistem keamanan terhadap sistem IT yagng dimiliki atau *cybersecurity*. Penerapan dari *cybersecurity* dapat membantu perusahaan dalam melindungi informasi, infrastruktur dan pengguna dari jasa atau aplikasi yang digunakan oleh perusahaan tersebut.

Berdasarkan uraian diatas, setiap perusahaan, instansi pemerintah dan para regulator harus mengetahui kerentanan dan kelemahan yang terkandung didalam sistem IT yang dimiliki. Situasi tersebut mendorong setiap perusahaan yang berbasis teknologi untuk mempunyai sistem keamanan yang dapat melindungi data, infrastruktur dan pengguna dari serangan *cyber*. Callen-Naviglia & James (2018) menyatakan bahwa apabila perusahaan tidak mempunyai sistem keamanan IT yang tidak memadai maka perusahaan tersebut berpotensi untuk mengalami intrusi terhadap sistem IT yang dimiliki dan dapat menghasilkan masalah bahkan bencana bagi perusahaan tersebut.

Sistem IT yang dimiliki oleh perusahaan maupun instansi pemerintahan yang mempunyai konektifitas dengan internet mempunyai potensi untuk mengalami serangan dari para hacker, dimana serangan tersebut dapat mempengaruhi pengguna IT dalam jumlah besar. Bendovschi (2015) menyatakan bahwa pada tahun 2015 serangan *cyber* telah mencapai 117.000 serangan per hari dan Cisco (2018a) melaporkan bahwa kerugian finansial yang disebabkan oleh serangan *cyber* pada tahun 2018 mencapai US$ 500.000. Sebagai gambaran, pada Tabel 1.1 ditampilkan beberapa kasus serangan *cyber* yang terjadi pada tahun 2017 terkait pembajakan sistem IT, pencurian dan penghapusan data. Dengan tambahan, 1.1 menunjukkan bahwa dampak dari serangan *cyber* dapat terjadi kepada perusahaan yang memiliki kerjasama dengan perusahaan lainnya dan serangan *cyber* tidak hanya terjadi kepada suatu industri spesifik melainkan terhadap berbagai industri yang menggunakan sistem informasi dan teknologi.

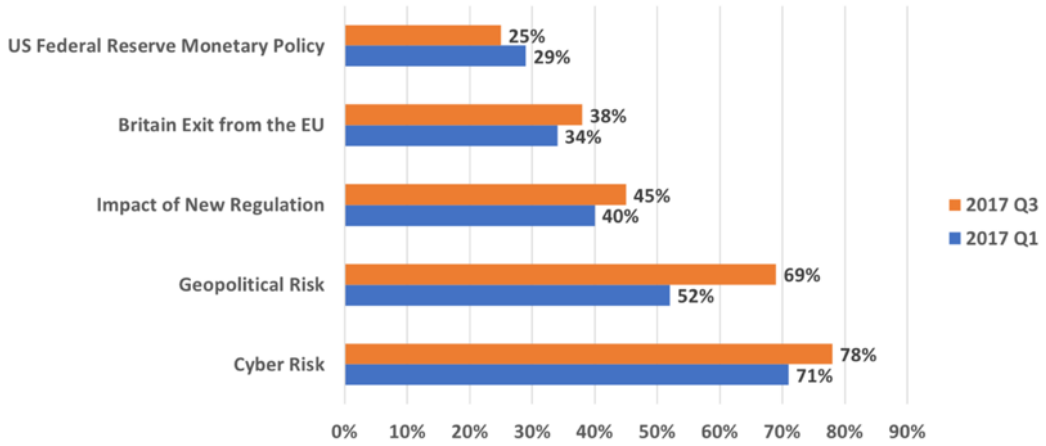
Tabel 1.1. Kasus Serangan *Cyber*, 2017

Perusahaan / Instansi	Bulan	Dampak
Princeton University	Januari	Data studi 27.000 mahasiswa dihapus dikarenakan kerentanan yang terkandung didalam *database* universitas.
PlayStation	Februari	2,5 juta data pengguna Xbox dan PlayStation dibocorkan.

Perusahaan / Instansi	Bulan	Dampak
New York Post	April	*Mobile app* dari New York Post direntas oleh para *hacker* dan memberikan notifikasi berantai terhadap berita palsu kepada seluruh pengguna aplikasi tersebut.
Equifax	September	143 juta data telah dicuri, data yang dicuri termasuk informasi kredit.
Uber	November	57 juta data pengguna dicuri dari akun Amazon Web Services (AWS) yang telah dibajak.

Sumber: Check Point Research (2018)

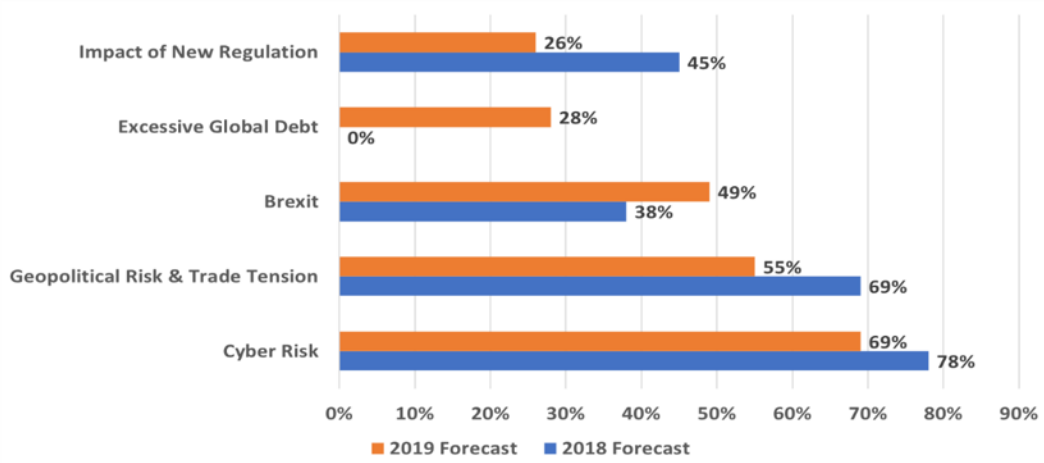
Berdasarkan penelitian yang dilakukan oleh Bouveret (2018), ditemukan bahwa *cyber risk* merupakan risiko yang dikhawatikan oleh partisipan dipasar global berdasarkan pengukuran yang dilakukan oleh Depository Trust & Clearing Corporation (DTCC). Pada Gambar 1.1 ditampilkan berbagai risiko yang terdapat pada sektor finansial dan *cyber risk* merupakan risiko dengan persentase tertinggi dengan nilai 71% pada tahun 2017Q1 dan 78% pada tahun 2017Q3.



Gambar 1.1. Risiko Pada Sektor Finansial (Global), 2017
Sumber: Depository Trust & Clearing Corporation (2017)

Bouveret (2018) menjelaskan bahwa serangan *cyber* mempunyai dampak yang dapat mempengaruhi berbagai pihak yang menggunakan sistem IT (perusahaan dan pengguna dari jasa atau aplikasi) dan serangan *cyber* tersebut mempunyai potensi untuk memberikan kerugian yang masif. Pada sudut pandang perusahaan fintech, terdapat beberapa risiko yang terdapat pada serangan *cyber* yang mempunyai karakteristik untuk memperkuat dan memperbesar kerugian (Lukonga, 2018). Potensi kerugian yang terjadi dapat mempengaruhi sistem IT yang digunakan, bahkan terhadap jasa atau produk yang ditawarkan kepada para pengguna. Peningkatan terhadap serangan *cyber* berbanding lurus dengan peningkatan konektifitas antar perangkat lunak dan perangkat keras yang digunakna oleh perusahaan. Dengan kata lain, semakin besar skala konektifitas yang dimiliki oleh perusahaan maka akan terjadi peningkatan terhadap *entry point* yang dapat digunakan oleh para *hacker* dalam merealisasikan serangan *cyber*.

Cyber risk merupakan salah satu risiko yang mempunyai potensi dalam mempengaruhi aktivitas pasar didalam sektor finansial (Depository Trust & Clearing Corporation, 2018). Hal tersebut mengindikasikan bahwa setiap perusahaan yang menggunakan sistem IT sebagai fondasi utama dalam menjalankan kegiatan operasional maupun menggunakan sistem IT sebagai pelengkap kegiatan perusahaan memiliki potensi untuk mengalami serangan *cyber*,terutama terhadap perusahaan yang tergolong kedalam perusahaan fintech. Pada Gambar 1.2 ditampilkan nilai prediksi terhadap risiko yang terdapat pada sektor finansial dan *cyber risk* diprediksikan menjadi risiko utama yang diantisipasi pada tahun 2019 pada sektor finansial. Berdasarkan gambar tersebut, dapat diindikasikan bahwa setiap perusahaan atau instansi yang memiliki dan menggunakan teknologi terekspos terhadap potensi dan dampak dari serangan *cyber*. Secara spesifik, setiap serangan tersebut berpotensi untuk mempengaruhi data atau informasi yang dimiliki oleh perusahaan fintech dan data para pengguna yang terdaftar pada pada sistem IT; serta, serangan *cyber* tersebut berpotensi untuk mempengaruhi profitabilitas dan performa perusahaan fintech secara signifikan; Dengan tambahan, hal tersebut berpotensi untuk mempengaruhi para pengguna pada saat yang bersamaan.



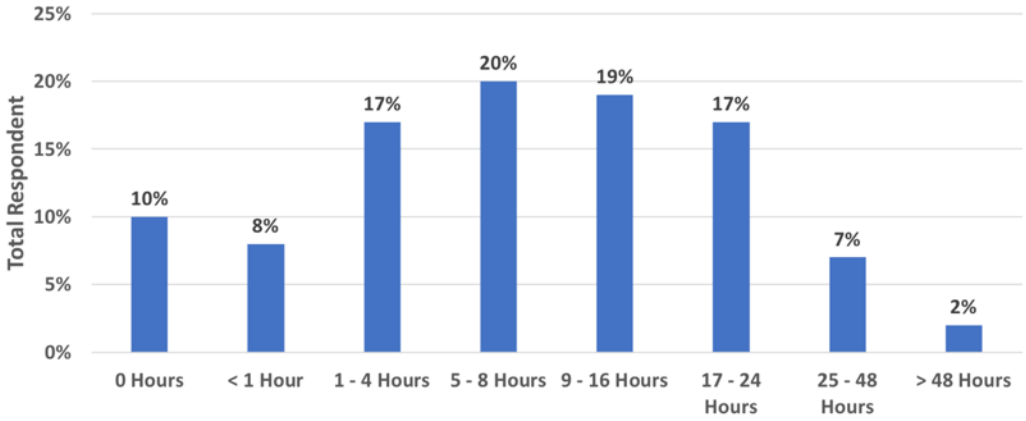
Gambar 1.2. Prediksi Risiko di Sektor Finansial
Sumber: Depository Trust & Clearing Corporation (2018)

Berdasarkan laporan Cisco (2018b) terkait serangan *cyber* di region *Asia Pacific Japan China* (APJC), ditemukan bahwa serangan *cyber* yang terjadi setiap enam menit dan hanya 50% dari peringatan serangan *cyber* yang telah diterima sedang dalam proses investigasi. Cisco (2018b) menambahkan bahwa mayoritas perusahaan yang beroperasi diregion APJC, mengalami serangan *cyber* yang menyebabkan sistem IT yang dimiliki menjadi non-aktif dalam kurun waktu kurang dari 24 jam dan setengah dari responden tersebut melaporkan bahwa sistem IT dapat diaktifkan kembali dalam waktu delapan jam. Uraian terkait sistem informasi yang non-aktif yang disebabkan oleh serangan *cyber* disertakan pada Gambar 1.3. Berdasarkan laporan tersebut, terdapat indikasi bahwa setiap perusahaan yang beroperasi pada region APJC mempunyai tingkat keamanan informasi dan teknolgi yang berbeda, sehingga waktu yang dibutuhkan untuk mengaktifkan kembali sistem IT dari serangan *cyber* bervariasi antar setiap perusahaan. Dengan tambahan, perusahaan tersebut harus memastikan bahwa tingkat keamanan IT yang dimiliki memadai untuk mereduksi dan memitigasi risiko dari serangan *cyber*, terutama terhadap serangan *cyber* yang memiliki frekuensi yang relatif singkat.

Partisipan yang mengikuti survey yang diselanggarakan oleh Cisco (2018b) sebanyak 2,000 responden dan meliputi 11 negara di region APJC[1] dan data tersebut dibandingkan dengan data global yang meliputi 26 negara dengan jumlah

[1] 11 negara di region APJC merupakan Jepang, China, Korea, Singapura, Thailand, Filipina, Indonesia, Malaysia, Vietnam, Australia dan India.

responden sebanyak 3,600 responden.



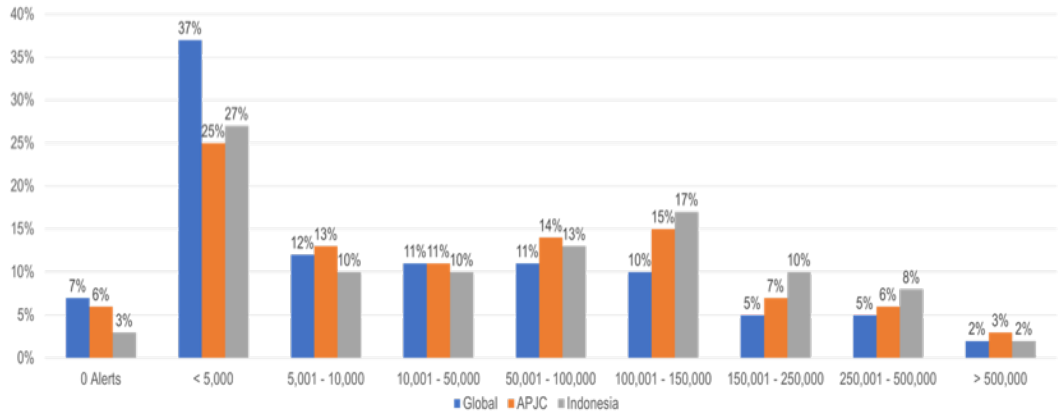
Gambar 1.3. Sistem Non-Aktif di Karenakan Serangan *Cyber* (APJC)
Sumber: Cisco (2018b)

Fritzvold (2017) menjelaskan bahwa aspek yang dapat menjaga dan menjamin informasi dan infrastruktur IT yang digunakan berorientasi terhadap manajemen sumber daya manusia, pengembangan teknologi, analisis kerentanan sistem, operasional dan pemeliharaan sistem. Aspek tersebut dapat mempunyai peran krusial dalam memberikan keamanan yang memadai terhadap informasi yang dimiliki, dikarenakan setiap perangkat lunak dan perangkat keras saling terhubung. Akan tetapi, apabila perusahaan tidak mempunyai tingkat keamanan yang memadai maka perusahaan tersebut berpotensi untuk mengalami kerugian dalam bentuk finansial dan non-finansial yang dapat disebabkan oleh serangan *cyber*.

Cisco (2018b) menemukan bahwa 37% responden global, 25% responden dari region APJC dan 27% responden dari Indonesia[2] mengalami serangan *cyber* sebanyak 5,000 serangan per hari. Cisco (2018b) menambahkan bahwa terdapat beberapa responden yang mengalami serangan *cyber* dalam rentang 100,001 sampai dengan 150,001 serangan per hari. Secara sederhana, perusahaan atau organisasi yang beroperasi di Indonesia maupun di region APJC memiliki intensitas peringatan serangan *cyber* yang berbeda. Dengan tambahan, insiden serangan *cyber* yang terjadi di Indonesia lebih rendah daripada insiden yang terjadi di region APJC; namum insiden serangan *cyber* yang telah terjadi pada perusahaan atau organisasi

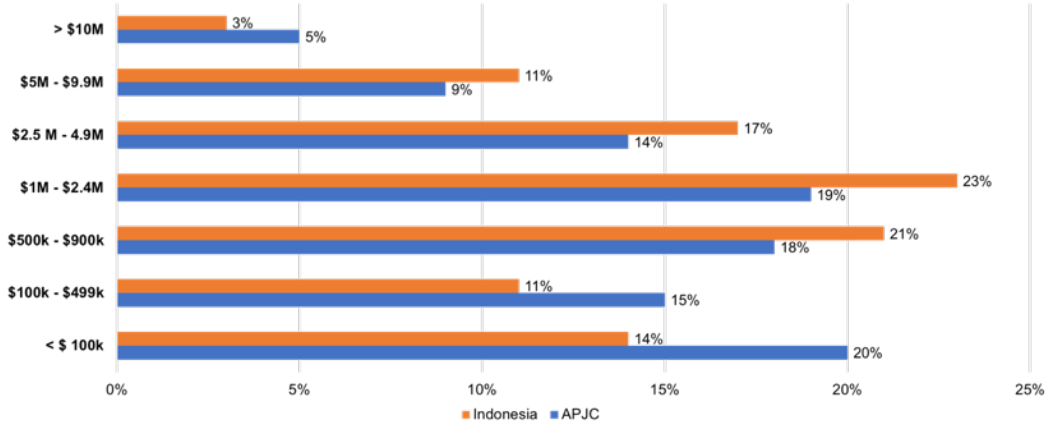
[2] Proses wawancara yang dilakukan oleh Cisco (2018b) terhadap perusahaan atau organisasi yang beroperasi di Indonesia, Thailand dan Singapura dilakukan pada bulan Juni 2018.

yang beroperasi di Indonesia lebih tinggi dari pada insiden yang terjadi di Australia dan Jepang (Cisco, 2018b). Sebagai gambaran, jumlah serangan yang dialami oleh respoden global, APJC dan Indonesia yang berpartisipasi pada survey Cisco (2018b) disertakan pada Gambar 1.4.



Gambar 1.4. Jumlah Serangan *Cyber* per Hari
Sumber: Cisco (2018b)

Serangan *cyber* yang terjadi diregion APJC dan di Indonesia telah memberikan kerugian finansial dan kerugian tersebut disebabkan oleh penetrasi atau intrusi yang dilakukan oleh para *hacker* terhadap perusahaan yang memiliki sistem IT (Cisco, 2018b). Cisco (2018b) melaporkan bahwa 19% responden dari region APJC dan 23% responden dari Indonsia mengalami kerugian finansial direntang US$ 1 juta sampai dengan US$ 2.4 juta. Berdasarkan kerugian finansial yang disebabkan oleh serangan *cyber* tersebut. Cisco (2018b) menjelaskan bahwa 13% dari partisipan yang mengikuti survey tersebut tidak mempunyai tenaga profesional didalam bidang *cybersecurity* dan serangan *cyber* yang telah terjadi tidak hanya berfokus kepada inftrastruktur IT yang digunakan oleh perusahaan melainkan kepada teknologi yang digunakan. Dengan tambahan, terdapat 3% dari organisasi yang beroperasi di Indonesia yang mengalami kerugian finansial diatas US$ 10 juta, dimana kerugian tersebut setara dengan standard kerugian finansial yang terjadi dalam skala global (Cisco, 2018b). Sebagai gambaran, Gambar 1.5 merupakan rentang kerugian finansial yang dialami oleh responden dari region APJC dan Indonesia.



Gambar 1.5. Kerugian Dikarenakan Serangan *Cyber*
Sumber: Cisco (2018b)

Berdasarkan penjelasan terkait kondisi dan dampak yang dihasilkan oleh serangan *cyber* pada region APJC dan di Indonesia, dapat dinyatakan bahwa dampak dari suatu serangan *cyber* dapat memberikan kerugian dalam rupa finansial dan non-finansial. Meskipun serangan *cyber* yang telah terjadi ditujukan kepada perangkat keras dan perangkat lunak yang dimiliki oleh perusahaan, Freund & Jones (2015) menambahkan bahwa serangan *cyber* dapat terjadi dalam bentuk penipuan dan target dari serangan tersebut bukan kepada perusahaan yang menggunakan sistem IT melainkan kepada para pengguna dari jasa yang ditawarkan oleh perusahaan tersebut. Modus penipuan tersebut dilakukan oleh para *attacker* dalam rangka untuk mendapatkan informasi secara langsung dari para pengguna tanpa harus melakukan penyerangan terhadap sistem IT yang dimiliki oleh perusahaan. Salah satu jenis dari modus penipuan yang ditujukan kepada para pengguna aplikasi atau jasa digital merupakan *social engineering*. Serangan dengan jenis *social engineering* merupakan serangan yang berfokus dalam persuasi dan mempengaruhi para pengguna sistem atau aplikasi untuk memberikan informasi sensitif yang dimiliki. Serta, serangan dengan jenis *social engineering* berpotensi menimbulkan kerugian signifikan terhadap perusahaan swasta dan instansi pemerintahan (Krombholz et al., 2015). Hal tersebut mengindikasikan bahwa para *hacker* mempunyai opsi dalam melakukan serangan *cyber* dengan jenis social engineering kepada individu tertentu maupun secara massal.

Terkait serangan *cyber* pada industri fintech, Bouveret (2018) melaporkan bahwa serangan *cyber* telah memberikan kerugian finansial kepada perusahaan fintech dari tahun 2013. Perusahaan fintech telah mengalami serangan *cyber* dan estimasi kerugian yang dihasilkan dari serangan *cyber* tersebut disertakan pada Tabel 1.2. Perusahaan fintech yang terdapat pada Tabel 1.2 merupakan perusahaan yang memiliki fitur pembayaran atau transaksi secara digital dan penyimpanan dana secara digital atau *e-wallet*. Kerugian finansial yang disebabkan oleh serangan *cyber* telah mencapai nilai US$ 1.450 juta dari tahun 2013.

Tabel 1.2. Serangan *Cyber* Pada Perusahaan Fintech

Institusi	Bulan	Estimasi Kerugian (Juta US$)
Inputs.io	Oktober 2013	1.3
GBL	Oktober 2013	5
Bitcoin Internet Payment Services	November 13	1
MT Gox	Januari 2014	470
BitPay	Desember 2014	1.9
EgoPay	Desember 2014	1.1
Bitstamp	Januari 2015	5.3
Bitfinex	Mei 2015	0.3
Gatecoin	Mei 2016	2
DAO Smart Contract	Juni 2016	50
Bitfinex	Agustus 2016	72.2
CoinDash	Juli 2017	7
Tether	November 17	31
NiceHash	Desember 2017	64
Coincheck	Januari 2018	534
BitGrail	Februari 2018	170
Coinsecure	April 18	33

Sumber: Bouveret (2018)

Serangan tersebut berpotensi untuk melakukan pencurian, manipulasi data dan menghentikan kegiatan operasional dari suatu perusahaan yang menggunkan sistem IT sehingga berpotensi untuk menurunkan performa dan efisiensi bahkan mempengaruhi tingkat profitabilitas dari perusahaan tersebut. Meskipun serangan *cyber* dapat ditujukan kepada sistem IT, serangan tersebut dapat ditujukan kepada para pengguna dari jasa atau aplikasi yang dihasilkan oleh perusahaan tersebut dalam rangka memperoleh informasi secara langsung dari para pengguna. Berdasarkan hal tersebut, terdapat indikasi bahwa terdapat sumber yang mempunyai potensi untuk merealisasikan serangan *cyber*.

Secara sederhana, konsep dari manajemen risiko harus diterapkan terhadap penanggulangan dari serangan *cyber* yang ditujukan kepada perusahaan dan para pengguna dari aplikasi. Hal tersebut diperlukan untuk menemukan sumber penyebab terjadinya serangan *cyber* disuatu perusahaan dan menghasilkan tindakan untuk memitigasi *cyber risk*. Penerapan konsep manajemen risiko di *cybersecurity* dapat membantu perusahaan dalam meningkatkan performa sistem keamanan IT untuk mencegah, memitigasi, meminimalisir dampak dan melindungi para pengguna dari serangan *cyber*.

Apabila perusahaan yang tergolong kedalam perusahaan fintech tidak dapat melakukan identifikasi dari sumber terjadinya serangan *cyber*, maka perusahaan tersebut berpotensi untuk meningkatkan kerentanan yang terdapat didalam sistem IT yang dimiliki dan meningkatkan potensi para pengguna dari jasa atau aplikasi tersebut untuk mengalami serangan *cyber* secara langsung. Berdasarkan hal tersebut, penelitian ini dilakukan terhadap perusahaan fintech X terkait implementasi konsep manajemen risiko terhadap keamanan sistem IT yang dimiliki serta menemukan sumber yang dapat merealisasikan serangan *cyber* terhadap perusahaan fintech X.

1.2 Rumusan Masalah

Dalam ruang lingkup perusahaan yang menggunakan sistem IT (terutama perusahaan fintech), berpotensi untuk mengalami serangan *cyber* yang mempunyai kapabilitas untuk memanipulasi data atau mengambil alih data tersebut oleh pihak

yang tidak memiliki otoritas atas data tersebut; hal tersebut dapat memberikan rasa tidak percaya kepada para pengguna dari sistem IT dalam melindungi data atau informasi para penggunanya apabila serangan *cyber* tersebut terjadi (Affia, 2018, hal. 9).

Peran *cybersecurity* dalam sistem IT yang digunakan dapat memberikan kapabilitas kepada perusahaan dalam menjaga informasi atau data sensitif terkait data perusahaan dan pengguna; serta *cybersecurity* mempunyai kapabilitas dalam melindungi para pengguna dari para *hacker*. Secara sederhana, aset dari sistem IT yang digunakan membutuhkan keamanan terhadap berbagai kejadian yang terdapat dilingkungan suatu perusahaan. Serangan *cyber* tersebut berpotensi untuk memberikan kerugian maupun bencana terhadap instansi tersebut dan setiap serangan yang terjadi kepada sistem IT dapat memberikan kerugian finansial yang disebabkan oleh pencurian atau penghilangan informasi (Henriques de Gusmão et al., 2018). Meskipun serangan *cyber* secara umun ditujukan kepada sistem IT yang dimiliki oleh perusahaan, Freund & Jones (2015) menyatakan bahwa serangan *cyber* dengan jenis penipuan juga dilakukan oleh para hacker yang secara langsung menargetkan pengguna untuk motif menarik keuntungan secara ilegal.

Sebagaimana dijelaskan di atas, perusahaan fintech yang mengalami serangan *cyber* tersebut mayoritas beroperasi dibagian jasa transaksi, pertukaran *bitcoin* dan penyimpanan dana secara digital (*e-wallet*).

Pada penelitian Patil et al. (2012), dijelaskan bahwa kerentanan terhadap sistem informasi yang digunakan dapat berasal dari sisi internal perusahaan. Secara spesifik, sumber internal tersebut disebabkan oleh para pegawai dari perusahaan tersebut dan hal tersebut dapat dilakukan secara sengaja maupun dikarenakan ketidaksengajaan. Apabila kerentanan terhadap sistem informasi yang terjadi dkarenakan ketidaksengajaan maka dibutuhkan metode kuantitatif yang dapat mengukur frekuensi dan probabilitas terhadap kejadian yang berpotensi untuk melemahkan keamanan sistem IT. Patil et al. (2012) menambahkan bahwa dampak dari ketidaksengajaan berpotensi untuk tidak dapat dideteksi oleh kerangka atau model yang dibangun dengan dasar kesengajaan.

Dari uraian diatas, terdapat indikasi bahwa serangan *cyber* dapat terjadi dari

sisi internal maupun eksternal perusahaan serta setiap perusahaan mempunyai tingkat dan performa yang berbeda dalam mengamankan sistem *informaton and communication* (ICT) yang dimiliki. Dengan berkembangnya teknologi dan meluasnya skala konektivitas dari perangkat keras dan perangkat lunak secara global, maka perusahaan yang menggunakan sistem IT sebagai fondasi utama dalam menjalankan kegiatan operasional disarankan untuk memiliki model identifikasi risiko yang dihadapi dan, hal tersebut dapat digunakan untuk menghasilkan kabijakan yang dapat memperkuat aspek *cybersecurity* terhadap sistem IT yang dimiliki dan mereduksi kerugian yang dihasilkan dari serangan *cyber*.

Didalam sudut pandang identifikasi sumber yang dapat merealisasikan suatu kejadian atau risiko, terdapat masalah yang harus dihadapi dalam rangka mengidentifikasi sumber tersebut secara akurat terhadap suatu kejadian atau risiko tertentu. Secara fundamental, proses identifikasi sumber dari suatu risiko dapat dilakukan dengan menggunakan pendekatan kualitatif atau kuantitatif, dimana kedua pendekatan tersebut mempunyai kelebihan dan kekurangan tersendiri. Wangen (2017) menjelaskan bahwa penelitian yang menggunakan pendekatan kualitatif memiliki kencenderungan unsur bias dan pendekatan secara kuantitatif memiliki batasan atau kondisi terhadap data yang digunakan pada suatu penelitian.

Terkait hal tersebut di atas, Fritzvold (2017) dan Henriques de Gusmão et al. (2018) menegaskan bahwa dalam konteks penerapan manajemen risiko didalam ruang lingkup IT dan *cybersecurity*, metode *fault tree analysis* dapat digunakan untuk mengidentifikasi sumber atau penyebab terjadinya suatu kejadian atau risiko dan dampak yang dapat ditimbulkan secara finansial dan non-finansial. Penggunaaan dari metode *fault tree analysis* dapat membantu perusahaan dalam menghasilkan tindakan atau kebijakan yang dapat memitigasi dan mereduksi dampak yang disebabkan oleh serangan *cyber*.Wangen (2017) dan Henriques de Gusmão et al. (2018) menambahkan bahwa metode *fault tree analysis* menggunakan model probabilistik untuk mengukur potensi terjadinya suatu kejadian berdasarkan sumber atau penyebab yang telah teridentifikasi dan direpresentasikan dalam bentuk *tree*.

Berdasarkan uraian diatas, permasalahan yang terdapat pada fenomena dan latar belakang di penelitian ini diuraikan sebagai berikut:

a. Terdapat potensi terjadinya serangan *cyber* terhadap informasi atau data perusahaan fintech dan pengguna, baik secara internal maupun eksternal.

b. Para *hacker* dapat secara langsung menargetkan pengguna jasa atau aplikasi perusahaan fintech untuk memperoleh profit. Hal tersebut membuat para pengguna aplikasi terekspos terhadap risiko modus penipuan secara digital yang dilakukan oleh para *hacker* dalam rangka memperoleh informasi sensitif dan uang elektronik yang dimiliki.

c. Risiko internal perusahaan fintech berpotensi untuk tidak terdeteksi oleh sistem, seperti terjadinya kebocoran informasi perusahaan akibat *human error*.

d. Penggunaan data yang bersifat kualitatif berpotensi untuk memberikan nilai estimasi yang tidak akurat terkait kerugian dan pola dari suatu insiden serangan *cyber* dikarenakan unsur *bias* yang terkandung pada data tersebut. Sehingga, data yang bersifat kuantitatif merupakan data utama yang dapat digunakan untuk memetakan pola dan karakteristik dari serangan *cyber* dikarenakan tren serangan *cyber* yang dapat terjadi dalam jumlah besar dan intesitas yang berbeda disetiap waktu terjadinnya serangan *cyber*.

e. Dibutuhkan teknik penyaringan data dan pengumpulan informasi terhadap data yang digunakan dalam mengidentifikasi pemicu terjadinya serangan *cyber*. Hal tersebut dikarenakan pola beserta kerugian finansial dan non-finansial dari serangan *cyber* berpotensi untuk tidak tereskpos pada data data yang digunakan.

f. Protokol keamanan dan kebijakan terkait penanganan serangan *cyber* yang tidak memadai, sehingga berpotensi meningkatkan kerugian finansial dan non-finansial.

1.3 Tujuan Penelitian

Tujuan utama dilakukannya penelitian ini ialah untuk menemukan sumber yang dapat merealisasikan risiko dari serangan *cyber* pada perusahaan fintech X. Dari tujuan tersebut, setiap sumber yang telah teridentifikasi digunakan untuk menemukan nilai probabilitas, frekuensi, estimasi kerugian finansial yang dapat ditimbulkan dari insiden yang dipicu oleh suatu sumber, dan menghasilkan saran terkait tindakan yang dapat diterapkan oleh perusahaan dalam memitigiasi suatu risiko serangan *cyber* yang dipicu dari suatu sumber. Berdasarkan hal tersebut, berikut merupakan tujuan dari penelitian ini:

a. Mengidentifikasi sumber yang dapat merealisasikan serangan *cyber* dari sisi internal maupun eksternal perusahaan.

b. Mengukur potensi kerugian yang dapat dialami oleh perusahaan fintech X.

c. Mengukur probabilitas dan frekuensi dari serangan *cyber* yang telah dialami oleh perusahaan fintech X berdasarkan sumber yang telah teridentifikasi. Nilai probabilitas yang telah terukur direpresentasikan kedalam bentuk *risk matrix* dalam rangka memetakan dampak dan probabiltias dari insiden yang telah dialami oleh perusahaan fintech X.

d. Memberikan rekomendasi atau kebijakan yang dapat diterapkan oleh perusahaan fintech X dalam memitigasi *cyber risk* berdasarkan sumber yang telah teridentifikasi berdasarkan sudut pandang dari konsep manajemen risiko.

e. Mengukur performa dari implementasi manajemen risiko yang dapat diterapkan oleh perusahaan fintech X dalam memitigasi dan mereduksi dampak dari serangan *cyber*.

f. Menilai apakah implementasi manajemen risiko perusahaan fintech X sudah menerapkan standard ISO/IEC 27001:2013.

Dalam rangka melakukan analisa terhadap penerapan manajemen risiko terhadap keamanan informasi dan teknologi, penelitian ini bertujuan untuk

melakukan proses analisa dari konsep implementasi manajemen risiko dari suatu perusahaan berdasarkan standard ISO/IEC 27001. Hal tersebut dilakukan untuk mengukur performa perusahaan dalam menghadapi risiko dari serangan *cyber*. Serta, setiap temuan yang diperoleh dari proses analisa diharapkan untuk meningkatkan kesadaran perusahaan terhadap keamanan informasi dan teknologi, serta menghasilkan tindakan untuk memitigasi risiko serangan *cyber* yang dapat terjadi.

1.4 Pertanyaan Penelitian

Dalam rangka memenuhi tujuan dari penelitian ini berdasarkan rumusan masalah yang telah dijelaskan, tujuan penelitian dan rumusan masalah yang telah dijelaskan direpresentasikan kedalam bentuk pertanyaan penelitian. Pertanyaan penelitian yang terdapat pada penelitian ini terdiri atas dua jenis pertanyaan, yaitu pertanyaan mayor dan pertanyaan minor. Berdasarkan hal tersebut, pertanyaan mayor pada penelitian ini yang harus dapat dijelaskan dan dijawab merupakan:

> "Apakah sumber pemicu yang dapat menghasilkan serangan *cyber* pada perusahaan fintech X"

Berdasarkan pertanyaan mayor tersebut, setiap sumber yang telah teridentifikasi dan menjawab pertanyaan mayor yang telah ditentukan maka terdapat lima pertanyaan minor yang harus dijawab terkait jawaban dari pertanyaan mayor tersebut. Pertanyaan minor yang harus dijawab dari pertanyaan mayor yang telah terpenuhi diberikan sebagai berikut:

a. Berapakah kerugian finansial yang disebabkan oleh setiap sumber pemicu yang telah teridentifikasi.

b. Berapakah tingkat frekuensi dan probabilitas dari setiap sumber pemicu yang dapat merealisasikan kejadian serangan *cyber*.

c. Apakah kebijakan atau tindakan yang dapat diterapkan oleh perusahaan fintech X untuk memitigasi dan meminimalisir dampak dari serangan *cyber* berdasarkan sumber pemicu yang telah teridentifikasi.

d. Bagaimana performa dari perusahaan fintech X dalam mengimplementasi konsep dari manajemen risiko dalam menghadapi serangan *cyber* terhadap sistem keamanan IT yang dimiliki.

e. Bagaimana protokol keamanan atas serangan *cyber* pada perusahaan fintech X dikembangkan sebagai tindak lanjut dari mitigasi risiko.

Berdasarkan kedua tipe dari pertanyaan tersebut, dalam menghasilkan jawaban yang dapat memenuhi tujuan penelitian berdasarkan rumusan yang telah dijelaskan, pertanyaan tersebut diformulasikan untuk mengetahui sumber yang dapat merealisasikan serangan *cyber* pada perusahaan fintech X. Serta, dari setiap sumber yang telah teridentifikasi dilakukan analisa untuk menemukan nilai frekuensi, probabilitas dan tindakan yang dapat membantu perusahaan fintech X dalam memitigasi risiko dari serangan *cyber*.

1.5 Manfaat Penelitian

Berdasarkan rumusan masalah dan tujuan penelitian yang telah diuraikan, berikut merupakan manfaat dari penelitian ini terkait analisa implementasi konsep manajemen risiko terhadap sistem IT pada perusahaan fintech X:

a. Manfaat teoritis:

   Penelitian ini memberikan pengetahuan dan tata cara proses identifikasi sumber yang dapat merealisasikan serangan *cyber* terhadap perusahaan yang memiliki fitur keamanan terhadap sistem IT yang dimiliki.

b. Manfaat praktis:

   Penelitian ini dapat digunakan sebagai acuan terkait proses identifikasi sumber-sumber yang dapat mengakibatkan serangan *cyber* terhadap perusahaan pemilik fitur keamanan sistem IT, dan sebagai pedoman perusahaan maupun individu dalam merancang kebijakan mitigasi *cyber risk* demi meminimalisir dampak dari serangan *cyber*.

1.6 Kerangka Pemikiran

Keamanan terhadap sistem IT yang dimiliki oleh perusahaan mempunyai peran dalam menjaga privasi dan aksesbilitas informasi terhadap pelanggaran yang dilakukan oleh para *hacker*. Serangan *cyber* yang ditujukan kepada perusahaan dapat memberikan kerugian finansial dalam jumlah besar serta dapat mempengaruhi kegiatan yang dilakukan oleh perusahaan tersebut (Bouveret, 2018). Kerugian finansial yang dihasilkan oleh serangan *cyber* dapat berupa pelanggaran privasi dari data yang dimiliki dan serangan tersebut berpotensi untuk menghasilkan risiko reputasi (Lukonga, 2018). Stallings (2011) menjelaskan bahwa serangan *cyber* berorientasi terhadap tiga faktor utama dari konsep *cybersecurity* yang diterapkan pada sistem IT yang digunakan, yaitu: (1) *confidentiality*, (2) *integrity* dan (3) *availability*. Ketiga faktor tersebut berfokus dalam menjaga kerahasian dan keutuhan data serta memastikan data tersebut dapat diakses disetiap waktu. Peran *cybersecurity* dapat membantu perusahaan yang menggunakan sistem IT dalam menjaga informasi perusahaan dan pengguna serta memastikan sistem tersebut berada dalam kondisi aktif di setiap waktu.

Suatu serangan *cyber* dapat terealisasi dari sumber yang berasal dari sisi internal dan eksternal perusahaan. Dari sisi internal, Patil et al. (2012) menyatakan bahwa serangan *cyber* dapat terjadi apabila pegawai dari suatu perusahaan melakukan kesalahan baik secara disengaja maupun dikarenakan ketidaksengajaan, maka kesalahan tersebut berpotensi untuk melemahkan tingkat keamanan dari sistem IT yang dimiliki sehingga meningkatkan potensi terjadinya serangan *cyber*. Disisi lain, apabila perusahaan menggunakan model atau kerangka yang didisain berlandaskan kesengajaan maka kerangka tersebut mempunyai potensi untuk tidak dapat mendeteksi suatu kesalahan yang dihasilkan dari suatu ketidaksengajaan.

Dari sisi eksternal, Marinos et al. (2016) menjelaskan bahwa serangan *cyber* dilakukan oleh pihak yang mempunyai tujuan atau motivasi yang bervariasi untuk melakukan pencurian data atau mengnonaktifkan sistem IT yang dimiliki; beberapa motivasi tersebut ialah untuk memperoleh profit atau reputasi. Nagaraju et al. (2017) menambahkan perkembangan dari serangan *cyber* mengalami

perkembangan dari sisi intensitas serangan dan teknik yang digunakan untuk mengeksekusi serangan tersebut. Serangan *cyber* yang dilakukan oleh para individu atau grup tersebut berpotensi untuk menimbulkan kerugian secara finansial dan berpotensi untuk mempengaruhi kegiatan operasional perusahaan.

Terkait konteks identifikasi sumber yang dapat merealisasikan serangan *cyber*, Henriques de Gusmão et al. (2018) menggunakan metode *fault tree analysis* dalam rangka menemukan sumber yang dapat merealisasikan serangan *cyber* terhadap sistem IT yang dimiliki oleh perusahaan. Sedangkan Patil et al. (2012) menggunakan metode *fault tree analysis* untuk menemukan sumber yang dapat merealisasikan serangan *cyber* dan kebocoran data dari sisi internal perusahaan. Berdasarkan penelitian yang dilakukan oleh Patil et al. (2012) dan Henriques de Gusmão et al. (2018) dapat diindikasikan bahwa sumber yang dapat merealisasikan serangan *cyber* dapat berasal dari sisi internal dan eksternal perusahaan serta penurunan terhadap tingkat keamanan di sistem IT meningkatkan probabilitas terjadinya serangan *cyber*.

Serangan *cyber* berpotensi untuk memberikan kerugian dan kerugian tersebut dapat dikonversi kedalam bentuk nominal dalam rangka membantu perusahaan dalam mengestimasi kerugian finansial yang dapat dialami. Kesswani & Kumar (2015) menjelaskan bahwa metode yang dapat digunakan untuk mengukur estimasi kerugian finansial yang ditimbulkan oleh serangan *cyber* menggunakan *single loss expectancy* dan *annualized loss expectancy*. Adapun metode *single loss expectancy* digunakan untuk mengukur estimasi kerugian finansial yang timbul dari satu kejadian, dan *annualized loss expectancy* digunakan untuk mengukur estimasi kerugian finansial yang terjadi dalam kurun waktu satu tahun. Sistem IT berfokus kepada pencegahan atau mereduksi potensi kerugian finansial akibat serangan *cyber*, bukan terhadap profit atau kerugian perusahaan.

Berdasarkan kerangka pemikiran diatas, disertakan model kerangka pemikiran yang direpresentasikan pada Gambar 1.6. Kerangka pemikiran tersebut diterapkan untuk menghasilkan kebijakan atau tindakan yang dapat diimplementasikan oleh perusahaan fintech dalam menghadapi serangan *cyber* berdasarkan konsep manajemen risiko terhadap keamanan informasi dan teknologi.

Gambar 1.6. Model Kerangka Pemikiran Tesis

1.7 Sistematika Penulisan

Struktur penulisan pada tesis ini terdiri atas lima bagian utama dalam rangka melakukan analisis terhadap penerapan manajemen risiko pada keamanan informasi dan teknologi pada perusahaan fintech X. berdasarkan hal tersebut, berikut merupakan penjelasan dari lima bagian dari struktur tesis ini:

a. Bab 1 pendahuluan: bab 1 terdiri atas latar belakang terhadap penjelasan terkait fenomena serangan *cyber* yang terjadi dalam skala global, region APJC dan di Indonesia terhadap perusahaan fintech, rumusan masalah, tujuan penelitian, pertanyaan penelitian dan manfaat penelitian terhadap analisa dan proses identifikasi sumber yang dapat merealisasikan serangan *cyber*.

b. Bab 2 landasan teori: bab 2 terdiri atas teori yang digunakan dalam membangun kerangka penelitian terhadap analisis serangan *cyber* dan *cyber risk* berdasarkan sudut pandang dari manajemen risiko dan penelitian terdahulu. Teori dan penelitian terdahulu digunakan untuk menjelaskan perkembangan dan dampak dari serangan *cyber*, peran *cybersecurity* terhadap keamanan sistem IT dan pengaruh dari serangan *cyber* dan kegunaan *cybersecurity* terhadap industri fintech.

c. Bab 3 metode penelitian: bab 3 terdiri atas metode yang digunakan untuk

mengidentifikasi sumber yang dapat merealisasikan serangan *cyber* pada perusahaan fintech X dan estimasi kerugian finansial yang ditimbulkan dari insiden yang dipicu oleh sumber tersebut. Metode yang digunakan untuk menemukan sumber dari serangan *cyber* ialah dengan menerapkan *fault tree analysis* (FTA), dan metode tersebut digunakan untuk menemukan nilai frekuensi dan probabilitas yang terkandung dari sumber yang telah teridentifikasi. Dengan tambahan, metode *data mining* digunakan untuk melakukan penyaringan data dan menemukan pola dari sumber yang memicu terjadinya insiden serangan *cyber*, serta metode tersebut digunakan untuk menemukan kerugian secara finansial yang sebelumnya tidak terekspos pada data yang digunakan, dan metode tersebut digunakan untuk memberikan kapabilitas untuk menganalisa data atau informasi dalam jumlah besar. Terkait estimasi kerugian finansial yang ditimbulkan dari serangan *cyber*, metode *single loss expectancy* (SLE) digunakan untuk menemukan nilai estimasi kerugian yang dapat ditimbulkan untuk setiap insiden yang dapat terjadi; dan, metode *annualized loss expectancy* (ALE) digunakan untuk menemukan nilai estimasi kerugian finansial dari insiden serangan *cyber* dalam kurun waktu tahunan.

d. Bab 4 analisis dan pembahasan: bab 4 terdiri atas temuan yang diperoleh pada pada saat menganalisis perusahaan fintech X terkait penerapan manajemen risiko terhadap keamanan informasi dan teknologi. Pada bab 4 terdiri atas proses identfikasi sumber penyebab terjadinya serangan *cyber* berdasarkan insiden yang telah terjadi pada perusahaan fintech X dengan menggunakan metoda FTA. Serta, pada bab ini disertakan estimasi terhadap kerugian finansial yang dapat ditimbulkan dari insiden serangan *cyber* dengan menggunakan metoda SLE dan ALE. Dengan tambahan, pada bab 4 disertakan pembahasan dan tindakan yang dapat diterapkan oleh perusahaan fintech X dalam memitigasi risiko dan mereduksi dampak yang dapat ditimbulkan dari seraangan *cyber* beserta pengembangan dari tindakan atau kebijakan yang telah diterapkan oleh perusahaan terhadap insiden yang telah terjadi.

e. Bab 5 kesimpulan dan saran: bab 5 merupakan bagian yang berisikan kesimpulan dari penelitian terhadap penerapan manajemen risiko terhadap keamanan informasi dan teknologi pada perusahaan fintech X. Serta, pada bab ini terdapat saran yang dapat membantu perusahaan fintech X dalam memitigasi risiko dan mereduksi dampak yang dapat ditimbulkan dari serangan *cyber* dalam rangka menjaga informasi dan teknologi yang dimiliki dan digunakan.