BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi meberikan dampak baik serta buruk bagi para penggunanya, semakin canggih sebuah teknologi maka akan semakin tinggi resiko serangan yang diterima [1]. Kejahatan dunia maya, atau yang dikenal dengan istilah *cyber crime* adalah salah satu dampak negatif dari penyalahgunaan kecanggihan teknologi. Terdapat tiga hal yang menjadi komponen utama sistem keamanan informasi, yaitu: proses, teknologi, dan manusia. Ketiga komponen tersebut merupakan satu kesatuan dalam membangun sistem keamanan informasi yang kuat [2]. Terkadang kita hanya mengetahui bahwa *hacker* melakukan peretasan pada teknologi, namun pada kenyataannya sistem paling lemah dan paling rentan terhadap serangan ada pada sisi manusia. Serangan seperti itu disebut dengan *Social Engineering* atau Rekayasa Sosial. Serangan Rekayasa Sosial dapat dilakukan dengan dua metode, yaitu berbasis Komputer dan berbasis Manusia [3]. Salah satu cara untuk menanggulangi serangan Rekayasa Sosial adalah dengan memahami setiap serangan yang terjadi dengan memperhatikan keadaan dan pengetahuan mengenai serangan yang sering terjadi. Kesadaran keamanan informasi menjadi hal utama dan paling penting bagi setiap individu, organisasi, ataupun perusahaan. Dengan menerapkan kesadaran keamanan informasi, maka penerapan *Work From Home (WFH)* dapat terlaksana dengan baik, serta dengan menerapkan kesadaran keamanan informasi dapat mengurangi tingkat resiko kegagalan sistem ataupun pencurian data karena kesalahan pengguna.

Dengan adanya pandemi covid 19 mengakibatkan peningkatan kejahatan dunia maya, menurut laporan *Phishing Activity Trends Report Analisys,* pada bulan April – Juni 2020 telah terdeteksi website yang digunakan untuk kejahatan *Phising* sebanyak 146,994 [4]. *Webmail* yang menargetkan phishing dan *Software-as-a-Service (SaaS)* bertahan sebagai kategori phishing terbesar, dengan 31,4% dari semua serangan. Perusahaan merupakan tempat favorit bagi penyerang dalam melakukan kejahatan dunia maya dikarenakan perusahaan merupakan

sumber data serta memiliki keuntungan lebih ketika penyerang berhasil melakukan eksploitasi. *Phishing* terhadap perusahaan media sosial naik dari 10,8 menjadi 12,6 persen, kata Stefanie Wood Ellis, Manajer Produk & Pemasaran Anti-Penipuan di salah satu pendiri APWG, OpSec Online [5]. Kesadaran tentang kemanan informasi menjadi hal utama bagi seorang *customer services* dalam melakukan pekerjaannya, kesalahan kecil yang dilakukan dapat mengakibatkan efek yang besar bagi perusahaan. Dalam menghadapi serangan rekayasa sosial ataupun segala serangan yang memungkinkan, perusahaan diwajibkan memiliki sebuah standar keamanan [6]. Standar ISO/IEC 27001:2013 adalah standar keamanan internasional dalam upaya menerapkan sistem manajemen keamanan informasi atau yang dikenal dengan *Information Security Management System* (ISMS) [7]. Dengan menerapkan standar keamanan yang sesuai dan mengimplementasikan dengan baik, perusahana mampu meminimalisir kegagalan sistem ataupun pencurian data karena kesalahan user. Security awareness adalah hal yang perlu diperhatikan bagi setiap perusahan terhadap para pegawainya dalam menerapkan *Work From Home (WFH)*. Analisa kesadaran keamanan informasi sangat dibutuhkan oleh pegawai dan sesuai dengan pengendalian ISO 27001: 2013 A.7.2.2 yang mensyaratkan bahwa "Semua karyawan organisasi dan, jika relevan, kontraktor harus menerima pendidikan dan pelatihan kesadaran yang sesuai dan pembaruan rutin dalam kebijakan dan prosedur organisasi, yang relevan dengan fungsi pekerjaan mereka".

Penelitian ini akan menganalisa tingkat kesadaran keamanan informasi dengan menggunakan metode *Failure Mode and Effect Analysis (FMEA)* sesuai standar keamanan ISO/IEC 27001:2013. Penelitian ini juga bertujuan untuk menganalisa keefektifan metode *Failure Mode and Effect Analysis (FMEA)* dalam penilaian tingkat kesadaran keamanan informasi berbasis manusia dimasa pandemi Covid-19

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka didapatkan sebuah permasalahan yaitu, bagaimana analisa kesadaran keamanan informasi menggunakan metode *Failure Mode And Effect Analysis* dengan *framework* ISO/IEC 27001:2013.

1.3 Batasan Masalah

Permasalahan dalam penelitian ini akan dibatasi dengan beberapa hal berikut:

a. Penelitian ini dilakukan untuk mengetahui tingkat kesadaran keamanan informasi dengan framework ISO/IEC 27001:2013.
b. Dalam melakukan penilaian tingkat kesadaran kemanan informasi, Penelitian ini menggunakan metode *Failure Mode Effect and Analysis (FMEA).*
c. Objek pada penelitian mengunakan PT CEBONG TOKO IJO INDONESIA sebagai objek dalam penilaian menggunakan metode *Failure Mode Effect and Analysis (FMEA)..*
d. Alat ukur yang digunakan untuk mengukur standar keamanan adalah ISO/IEC 27001:2013 pada penelitian ini menggunakan metode kualitatif dengan mengajukan kuesioner.
e. Metode yang digunakan dalam penelitian ini adalah metode kuantitatif dengan mengajukan kuesioner serta beberapa wawancara juga dilakukan untuk mendapatkan informasi secara lebih akurat dan ditambah dengan observasi pada objek penelitian.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menganalisa kesiapan perusahaan dalam menghadapi serangan rekayasa sosial pada masa pandemi, serta beberapa manfaat sebagai berikut:

a. Melakukan analisa kesadaran keamanan informasi pada *customer services* dimasa pandemi dengan menggunakan metode *Failure Mode Effect and Analysis (FMEA)* dengan standar yang digunakan adalah ISO

27001:2013 dalam menghadapi serangan rekayasa sosial pada masa pandemi.

b. Menganalisa Keefektifan metode FMEA dalam proses analisa kesadaran keamanan informasi berbasis manusia.

1.5 Sistematika Penulisan

Pada dasarnya penyusunan sistematika penulisan bertujuan untuk memudahkan pembaca dalam mengikuti apa yang dipaparkan dalam laporan skripsi ini. Sistematika penulisan skripsi ini adalah sebagai berikut ::

Bab I Pendahuluan, berisi: latar belakang, rumusan masalah dan hipotesis, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori, berisi: hasil penelitian sejenis yang sudah pernah dilakukan sebelumnya, teori penunjang, dan referensi berupa buku, jurnal, dan laporan skripsi/tesis.

Bab III Metodologi Penelitian, berisi: penjelasan mengenai metode penelitian yang digunakan untuk memahami dan mengexplorasi obyek penelitian, hasil observasi / pengumpulan data, masalah yang terdapat pada obyek, dan gambaran umum proyek atau obyek penelitian, hingga Rencana Alur Penelitian.

Bab IV Pembahasan, berisi: tahapan yang dilakukan adalah implementasi dari metodologi. Data hasil akhir pengujian dapat berupa grafik, table, data monitoring, dan lain-lain, dengan pembahasan.

Bab V Penutup, berisi kesimpulan dari hasil akhir penilaian proyek, dan saran.