BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Produksi dan eksplorasi minyak dan gas adalah kegiatan utama Perusahaan X, sebuah perusahaan dunia. perusahaan X terdaftar sebagai perusahaan minyak dan gas terbesar ke-25 di dunia pada halaman online (Perusahaan Minyak dan Gas Terbesar berdasarkan Kapitalisasi Pasar, n.d.), namun di Indonesia, itu adalah salah satu dari sepuluh besar produsen minyak dan gas nasional (Verda Nano Setiawan, 2022).

Divisi ICT (information Commnication and Technology) merupakan bagian dalam perusahaan yang bekerja tidak hanya berfokuskan pada teknologi informasi. Tugasnya juga bertanggung jawab untuk meninjau semua sistem komputerisasi dan memastikan bahwa *system* berjalan lancar untuk user demi keberlangsungan pekerjaan.

Pegawai dalam perusahaan secara general mempunyai peranan yang sangat penting bagi perusahaan, bagaimana mereka diatur dan bertindak dapat mempengaruhi keberhasilan dan keunggulan bagi perusahaan (Gabčanová, 2011). Karyawan juga dapat menjadi sumber sejumlah besar kejadian dari keamanan informasi organisasi yang disebabkan secara langsung dan/atau tidak langsung yang menyebabkan sebagian besar insiden keamanan, menurut perspektif kesadaran keamanan. Dengan begitu, kesadaran keamanan informasi dari pegawai menjadi salah satu aspek penting dari perlindungan terhadap perilaku atau ancaman keamanan informasi yang tidak diinginkan (Khando et al., 2021).

Untuk penelitian ini, peneliti melakukan penyebaran kuesioner kepada 61 pegawai perusahaan X yang masuk ke dalam bagian divisi ICT. Pegawai tersebut terdiri dari berbagai posisi.

1.2 Latar Belakang Penelitian

Seriring berjalannya waktu, Perkembangan teknologi informasi semakin lama berkembang dengan sangat pesat. Perkembangan ini dapat memberikan dampak positif

bagi semua orang dan bidang pekerjaan. Kemajuan teknologi ini tentunya akan sangat membantu pekerjaan dan kehidupan masyarakat jika digunakan dengan baik dan benar, namun apabila ada kelebihan tentunya pasti juga ada kekurangan. Dampak yang harus diperhatikan dari penggunaan teknologi informasi untuk bisnis salah satunya ialah masalah keamanan (Yuliani, 2017)

Pada tahun 2021 dari bulan januari hingga bulan agustus, terdapat 888.711.736 terjadinya serangan siber ini di karenakan cepatnya pertumbuhan penggunaan teknologi informasi (Asih, 2021).

Manajemen keamanan informasi merupakan bagian penting dari keamanan *cyber*. Dalam kerangka COBIT, keamanan informasi sangat penting dalam menjaga privasi data yang tidak dapat dipublikasikan. Selain COBIT, *framework* ISO/IEC 27001 juga mengevaluasi komponen keamanan informasi dari sistem informasi yang digunakan oleh institusi. Perlu adanya tata kelola manajemen yang baik untuk mengklasifikasikan berbaga risiko yang berpotensi merugikan perusahaan. Pembahasan dalam penelitian ini akan dibahas mengenai menggambarkan perspektif dari karyawan salah satu perusahaan minyak yang ada di Indonesia untuk menjaga kelangsungan usaha dan melindungi data atau informasi yang bersifat rahasia (Singgalen et al., 2021).

Dilansir dari sumber *article* berita Bloomberg (Brambilla, 2022), perusahaan besar multinasional asal italia, mengalami percobaan *hack*. Telah dikonfirmasi bahwa *internal protection* telah mendeteksi percobaan akses oleh pikah yang tidak memiliki wewenang. Orang-orang yang mengetahui situasi tersebut mengatakan bahwa perusahaan tersebut telah terkena serangan *ransomware*. *Ransomware* merupakan sejenis *malware* yang mengunci komputer serta memblokir akses ke file sebagai pengganti pembayaran. Belum diketahui siapa yang bertanggung jawab atas pelanggaran tersebut. Namun, (IBM, 2014) menyatakan meskipun 45% serangan yang terjadi dilakukan dari pihak luar, akan tetapi 55% juga disebabkan dari pihak dalam yaitu mereka yang memiliki akses ke dalam suatu organisasi, atau karyawan yang kurang memiliki kesadaran keamanan informasi sehingga dapat menyebabkan insiden

pada keamanan informasi.

Dilansir dari *CyberEdge's 2018 Cyberthreat Defense Report*, ketertakutan terbesar dari sebuah organisasi adalah kurangnya kesadaran keamanan karyawan. Karyawan yang kurang menyadari kewajiban dan kepentingan keamanan siber cenderung mengabaikan kebijakan dan prosedur yang relevan, yang dapat menyebabkan pengungkapan data yang tidak disengaja atau mengundang serangan siber dari luar yang berhasil, seperti *phising* dan *ransomewere.* (Luke Irwin, n.d.)

Berita tersebut membuktikan bahwa kejahatan teknologi informasi tidak hanya serangan dari luar saja yang berbahaya, namun kesadaran keamanan *system* dari pegawai juga menjadi poin penting dalam keberlangsungan kemanan suatu organisasi atau perusahaan. Setiap pengguna dan karyawan dari sebuah organiasi atau perusahaan, wajib bertanggung jawab atas penggunaan sumber daya yang diberikan secara aman. Untuk itu, pengguna harus bertindak setiap saat dengan mematuhi kode etik dari perusahaan, dan harus menghindari semua penyalahgunaan layanan atau bertentangan dengan kode etik dari peraturan yang telah ditetapkan. Perlu adanya tindakan pengukuran tingkat kesadaran keamanan untuk mengetahui tingkat dari pegawai perusahaan. Untuk mengukur pemahaman karyawan tentang kesadaran keamanan informasi, peneliti berusaha menyelidiki tingkat kesadaran internal karyawan divisi ICT tentang keamanan informasi.

Penelitian ini akan membahas permasalahan mengenai hal-hal yang berkaitan dengan pengetahuan, sikap, dan perilaku pengguna sistem para pegawai Perusahaan X, khususnya pada divisi ICT. Penelitian ini menawarkan ide untuk menguraikan kesadaran keamanan siber dengan membatasi ruang lingkup diskusi pada kesadaran keamanan informasi. Secara kontekstual, pengguna sistem yang menjadi unit pengamatan penelitian ini terbatas pada pegawai divisi ICT pada Perusahaan X di Indonesia.

1.3 Perumusan Masalah

Berdasarkan dari pernyataan diatas, maka pertanyaan pada penulisan ini yaitu:

1. Bagaimana tingkat *security awareness* dari pegawai Perusahaan X berdasarkan *attitudenya?*
2. Bagaimana tingkat *security awareness* dari pegawai Perusahaan X berdasarkan *knowledgenya?*
3. Bagaimana tingkat *security awareness* dari pegawai Perusahaan X berdasarkan *behaviornya?*
4. Seberapa tinggi total tingkat *security awareness* dari pegawai Perusahaan X?

1.4 Tujuan Penelitian

Dari pemaparan yang sudah dijabarkan maka tujuan ingin dicapai pada tulisan iniyaitu:

1. Guna diketahuinya tingkat *security awareness* dari para pegawai divisi ICT Perusahaan X berdasarkan *attitude*.
2. Untuk mengetahui tingkat *security awareness* dari para pegawai divisi ICT Perusahaan X berdasarkan *knowledge*.
3. Untuk mengetahui tingkat *security awareness* dari para pegawai divisi ICT Perusahaan X berdasarkan *behavior*.
4. Untuk mengetahui tinggi total tingkat kesadaran *security awareness* dari pegawai divisi ICT perusahaan X

1.5 Manfaat Penelitian

1.5.1 Aspek Teoritis

Menginformasikan pengetahuan mengenai kesadaran dari manajemen keamanan informasi dari Perusahaan X.

1.5.2 Aspek Praktis

Dengan temuan ini ditujukan pada pegawai Perusahaan X agar lebih *aware* terhadap manajemen keamanan informasi dari bisnisnya.

1.6 Sistematika Penulisan Tugas Akhir

a. BAB I PENDAHULUAN

Bab ini memberikan informasi umum mengenai subjek penelitian, konteks penelitian, rumusan masalah, tujuan penelitian, keunggulan

penelitian, dan metodologi penulis proyek akhir.

b. BAB II TINJAUAN PUSTAKA

Teori sebelumnya, studi, kerangka kerja penelitian, dan hipotesis disertakan dalam bab ini.

c. BAB III METODE PENELITIAN

Bab ini menjelaskan strategi, taktik, dan prosedur yang digunakan untuk mengumpulkan dan memeriksa data yang dapat menyelesaikan masalah penelitian.

d. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pembingkaian masalah dan tujuan penelitian, yang disajikan dalam subjudul yang berbeda, diikuti dengan deskripsi metodis dari hasil penelitian dan diskusi.

e. BAB V KESIMPULAN DAN SARAN

Kesimpulan memberikan jawaban atas pertanyaan penelitian dan membuat rekomendasi tentang manfaat penelitian.