BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

PT Telkom Indonesia, Tbk merupakan Badan Usaha Milik Negara (BUMN) yang bergerak dibidang jasa layanan teknologi informasi dan komunikasi serta jaringan telekomunikasi di Indonesia. PT Telkom Indonesia, Tbk memiliki perusahaan pusat resmi di Bandung dan berperusahaan pusat operasional di Jakarta. Perusahaan pusat resmi di Bandung beralamat di Jalan Japati no.1, Sadang Serang, Kecamatan Cicendo, Kota Bandung. Telah hadir dari tahun 1965 hingga sekarang. Dengan riset terpadu dan didukung oleh tenaga ahli dalam bidangnya, PT Telkom Indonesia, Tbk mampu menghasilkan produk yang berkualitas dan bermutu. PT Telkom sendiri telah menjadi distributor layanan jaringan dan telekomunikasi, termasuk layanan telekomunikasi domestik maupun internasional yang tersebar.

Dalam upaya bertransformasi menjadi *digital telecommunication company*, Telkom Group mengimplementasikan strategi bisnis dan operasional perusahaan yang berorientasi kepada pelanggan. Kegiatan usaha Telkom Group bertumbuh dan berubah seiring dengan perkembangan teknologi, informasi dan digitalisasi, namun masih dalam koridor industri telekomunikasi dan informasi. Telkom mulai saat ini membagi bisnisnya menjadi 3 *Digital Business* yaitu *Digital Connectivity, Digital Platform, dan Digital Services.*

Divisi *Information Technology* (IT) di PT Telkom Indonesia menjadi peran utama dalam menggerakkan perusahaan telekomunikasi terbesar di Indonesia. Dengan fokus pada pengelolaan infrastruktur jaringan, pengembangan layanan inovatif, serta keamanan informasi, divisi IT PT Telkom menjaga agar jaringan telekomunikasi tetap beroperasi dengan lancar dan efisien. Divisi IT juga memiliki tanggung jawab untuk menjaga keamanan data pelanggan, mengidentifikasi dan mengatasi ancaman siber, serta mematuhi regulasi yang ketat dalam menerapkan teknologi terbaru. Divisi IT PT Telkom adalah pendorong utama bagi kemajuan perusahaan ini dalam industri yang sangat kompetitif.

Gambar 1. Logo PT Telkom Indonesia, Tbk
Sumber: www.telkom.co.id (2023)

1.1.2 Visi dan Misi PT Telkom Indonesia, Tbk

Adapun Visi dari PT Telkom Indonesia, Tbk adalah sebagai berikut:
Menjadi *digital telco* pilihan utama untuk memajukan masyarakat

Sedangkan Misi dari PT Telkom Indonesia, Tbk sebagai berikut:

1. Mempercepat pembangunan Infrastruktur dan *platform digital* cerdas yang berkelanjutan, ekonomis, dan dapat diakses oleh seluruh masyarakat.
2. Mengembangkan talenta *digital* unggulan yang membantu mendorong kemampuan *digital* dan tingkat adopsi *digital* bangsa.
3. Mengorkestrasi ekosistem *digital* untuk memberikan pengalaman *digital* pelanggan terbaik

1.1.3 Aspek Organisasi Divisi IT

Divisi *Information Technology* memiliki peran penting dalam mendukung operasional dan tujuan perusahaan. Aspek-aspek utama dalam menjalankan divisi IT yang sukses dan efisien meliputi manajemen infrastruktur IT, yang mencakup perencanaan, pengadaan, instalasi, dan pemeliharaan perangkat keras, perangkat lunak, jaringan, dan sistem komputer yang diperlukan. Selain pengembangan perangkat seperti mencakup perencanaan, desain, pengembangan, pengujian, dan pemeliharaan aplikasi dan sistem yang menjadi bagian integral dari perusahaan, divisi IT juga bertanggung jawab atas keamanan informasi, mengidentifikasi, dan mencegah ancaman keamanan seperti *malware*, peretasan, dan serangan siber.

Manajemen proyek IT diperlukan untuk memastikan proyek-proyek seperti implementasi sistem baru, peningkatan infrastruktur, atau perubahan perangkat lunak berjalan sesuai rencana, anggaran, dan jadwal. Selain itu, pengelolaan data, termasuk penyimpanan, pengambilan, dan analisis data, sangat penting untuk mendukung pengambilan keputusan dan operasi organisasi. Divisi IT juga harus mematuhi peraturan dan regulasi yang berlaku dalam industri mereka, termasuk perlindungan data pribadi, privasi, dan peraturan keamanan.

Terakhir, divisi IT juga harus berperan dalam inovasi teknologi, aktif mengidentifikasi dan mengeksplorasi inovasi yang dapat membantu organisasi menjadi lebih efisien, kompetitif, dan adaptif dalam era perkembangan teknologi yang terus berlanjut. Dalam menghadapi dinamika teknologi yang terus berkembang, divisi IT harus terus beradaptasi dan berinovasi untuk memenuhi kebutuhan organisasi.

1.2 Latar Belakang Penelitian

Tidak dipungkiri bahwa keamanan informasi telah menjadi faktor kunci dalam keberhasilan berbagai organisasi maupun individu di era digital yang semakin berkembang ini. Perkembangan teknologi informasi dan komunikasi telah memungkinkan kita untuk menyimpan, mengakses, serta berbagi data dengan lebih mudah. Akan tetapi, ancaman terhadap keamanan informasi juga semakin meningkat seperti peretasan, kebocoran data hingga pencurian identitas. Serangan terhadap keamanan informasi memiliki dampak serius yang mengakibatkan kerugian finansial hingga terjadi kerusakan reputasi perusahaan.

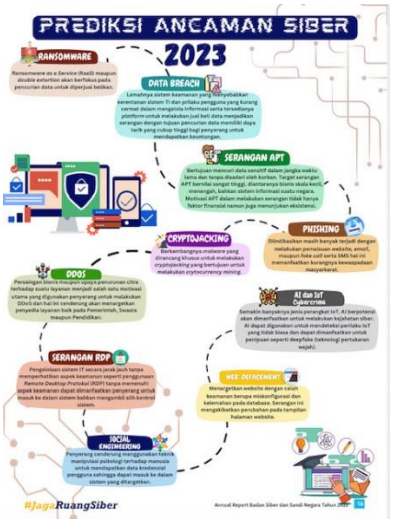
Menurut perkiraan dari Laporan Keamanan *Siber Statista National Cyber Security Organization* pada November 2022 menyatakan bahwa biaya keseluruhan pengeluaran terkait kejahatan siber diseluruh dunia diperkirakan akan meningkat dalam lima tahun mendatang. Kejahatan siber didefinisikan oleh *cybercrime magazine* sebagai kerusakan dan penghancuran data, hilangnya produktivitas, pencurian data pribadi, penghapusan data dan sistem yang diretas, serta kerusakan reputasi (Fleck, 2022).

Gambar 2. Cybercrime Expected in the Coming Years
Sumber: Statista Technology Market Outlook (2022)

Sementara itu dilansir dari situs web BSSN Indonesia sendiri, dalam sebuah konferensi pers yang diadakan di Perusahaan Badan Siber dan Sandi Negara (BSSN) di Jakarta Selatan pada tanggal 20 Februari 2023, Kepala BSSN, Hinsa Siburian, melakukan transparansi Laporan Tahunan BSSN 2022. Hinsa juga memberikan gambaran umum tentang kondisi *cyber*

security di Indonesia pada tahun 2022 dan tren *threat security* yang diperkirakan akan terjadi pada tahun 2023.

Tren *Threat Security* akan menjadi sumber informasi yang berguna untuk meningkatkan pemahaman tentang budaya keamanan siber di kalangan berbagai instansi dan organisasi yang berkepentingan dalam keamanan siber. Dalam dokumen laporan tahunan pada halaman 16 terlampir beberapa prediksi ancaman siber di Indonesia tahun 2023. *Data Breach* dan *Ransomware* merupakan ancaman yang perlu diperhatikan lebih lanjut kepada seluruh masyarakat maupun organisasi dalam melindungi keutuhan keamanan security. Hasil dari laporan tahunan BSSN tahun 2022, menyatakan bahwa insiden yang paling sering terjadi pada individu, instansi, maupun organisasi yaitu *data breach* sebesar 26%, lalu diikuti oleh insiden *web defacement* 26%, dan *Ransomware* sebesar 24%. Sehingga dapat dikatakan bahwa *ransomware* dan *data breach* merupakan permasalahan yang harus awasi karena akan menjadi sorotan utama dalam prediksi ancaman siber 2023.



Gambar 3. Prediksi ancaman siber
Sumber: bssn.go.id (2023)

Gambar 4. Top 3 insiden siber
Sumber: bssn.go.id (2023)

Pernyataan ini diperkuat oleh insiden yang dikutip dari situs kompas.com pada tanggal 7 Juli 2023, mengenai dugaan kebocoran data di layanan Indihome milik PT Telkom, dalam berita tersebut dijelaskan bahwa terdapat 35 juta data histori pelanggan IndiHome bocor, termasuk email, No handphone, No indihome, NIK, Alamat IP, *password* dan data lainnya. Pelaku yang dikenal dengan sebutan bjorka, mengakui ada 35 juta data pelanggan Indihome yang dijual dengan harga 5.000 dollar Amerika Serikat. Kebocoran data ini terungkap dan menjadi topik perbincangan utama dalam masyarakat secara luas.

PT Telkom langsung segera mengambil tindakan dengan memberikan informasi yang transparan kepada para pelanggan mengenai berita insiden tersebut. Ahmad Reza, *SVP Corporate Communication & Investor Relation* Telkom, dalam kegiatan konferensi pers bersama *VP Network/IT Strategy, Technology & Architecture* Telkom Rizal Akbar, *dan EGM Divisi Information Technology* Telkom Sihmirmo Adi di Telkom Landmark Tower menegaskan tidak ada kebocoran data pelanggan. Setelah dilakukan penelusuran dan investigasi menyeluruh, PT Telkom memastikan data yang bocor merupakan data yang difabrikasi dan disalah gunakan oleh pihak yang tidak bertanggung jawab.

Meskipun berita tersebut tidak benar, tetapi insiden tersebut cukup membuktikan bahwa *threat data breach* sangat rentan terjadi karena *awareness* terhadap *security* tidak maksimal, sehingga menjadi peringatan untuk seluruh karyawan bahwa betapa pentingnya perusahaan menjaga keamanan data dan privasi pelanggan serta bagaimana perusahaan dapat memperkuat perlindungan terhadap keamanan data. (Darmawi, 2019), mengatakan bahwa manajemen risiko adalah usaha dalam mencegah dan mengelola risiko pada semua aspek operasional perusahaan untuk meningkatkan efektivitas dan efisiensi suatu perusahaan. Dalam konteks manajemen risiko, kesadaran keamanan adalah fondasi penting dalam mendorong usaha manajemen risiko yang efektif. Menurut (Whitman & Mattord, 2018) dari jurnalnya (Putra & Sari, 2016) *Security Awareness* merupakan kontrol/peraturan yang diciptakan dengan tujuan mengurangi insiden pelanggaran terhadap keamanan informasi yang disebabkan oleh kelalaian maupun tindakan perencanaan.

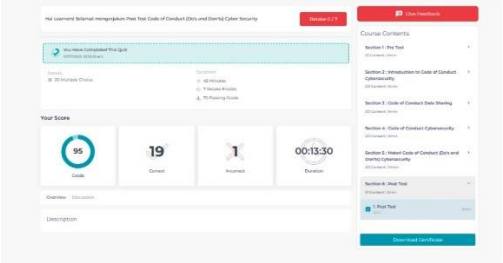
Menurut (Alshaikh et al., 2021) Program *Security Education, Training, and Awareness* (SETA) merupakan salah satu strategi yang digunakan untuk mengendalikan ancaman keamanan informasi dan melindungi aset informasi dengan melibatkan pemahaman karyawan dan anggota organisasi terhadap berbagai aspek keamanan informasi unntuk melindungi informasi dan aset organisasi. Program *Security Education Training and Awareness* (SETA) dapat membantu karyawan memahami pentingnya *cybersecurity* dan melatih pemahaman

mereka dalam mengidentifikasi potensi ancaman dan bagaimana mereka dapat merespons dengan cepat. Sehingga membantu melindungi organisasi dari ancaman *cyber* seta dapat membantu melindungi aset informasi perusahaan dari potensi kerugian atau kerusakan.

Sistem informasi perusahaan merupakan aset penting yang harus dilindungi dari *threat security*, seperti serangan siber, *data breach*, dan penyalahgunaan data. Divisi IT bertanggung jawab untuk mengelola dan mengamankan sistem informasi perusahaan. Divisi IT memiliki pemahaman yang mendalam tentang teknologi informasi, akses ke data dan sumber daya yang dibutuhkan, serta tanggung jawab untuk memastikan keamanan sistem informasi perusahaan. Dengan peran penting yang dimiliki oleh divisi IT, PT Telkom dapat memanfaatkan teknologi informasi secara efektif untuk meningkatkan efisiensi, efektivitas, dan daya saing. Selain karena keterbatasan sampel penelitian, sumber daya manusia yang terdapat di Divisi IT diharuskan untuk lebih memahami dan aware terhadap *threat security* dibandingkan karyawan dari Divisi lain. Oleh karena itu penulis akan lebih memfokuskan penelitian ini dibagian Divisi *Information Technology*.

Berdasarkan hasil wawancara dengan Bapak Bimo Sulistyo selaku *Manager IT General Control* Divisi IT PT Telkom Indonesia, Tbk dalam upaya melindungi pemahaman, pengetahuan dan perilaku individu terkait dengan keamanan informasi, PT Telkom melakukan *campaign training security awareness* berbentuk *e-learning*, webinar serta *campaign* sosialisasi mengenai *security awareness* melalui *email* dan *whatsapp.*

Gambar 5. Cyber Security campaign
Sumber: Narasumber Peneliti (2023)



Gambar 6. Training e-learning
Sumber: Narasumber Peneliti (2023)

Gambar 7. Webinar
Sumber: Narasumber Peneliti (2023)

Halo BIMO SULISTYO

Tahukah Telkomers?
Kasus **kebocoran data dan serangan siber** lainnya kian meningkat tiap tahunnya. Menurut laporan Cybersecurity Ventures tahun 2022, **kerugian** akibat serangan siber diprediksi akan mencapai **lebih dari $8 triliun** pada tahun **2023**, dan diperkirakan akan **mencapai $10,5 triliun** pada tahun **2025**.

Oleh karena itu, penting bagi Telkomers untuk memiliki **kesadaran keamanan data** yang baik demi melindungi informasi perusahaan. Simak beberapa **Do's dan Don'ts** yang perlu diperhatikan terkait **data** berdasarkan **PR 210.02 tentang Standar Perilaku Karyawan untuk Mendukung Keamanan Informasi dan PR 210.03 tentang Fasilitas Kerja.**

Ketuk tombol "Yuk!" untuk artikel selengkapnya ya!

We Care, We Secure
Salam #SecurityAwareness
#SelaluBerintegritas #ProtekSIBERsama

Gambar 8. Campaign melalui Whatsapp
Sumber: Narasumber Peneliti (2023)

Gambar 9. Campaign Melalui Whatsapp
Sumber: Narasumber Peneliti (2023)

Dapat kita lihat dalam bukti diatas, PT Telkom telah berupaya menjaga keamanan sistem informasi dengan berbagai bentuk campaign. Namun pada saat dilakukan program training, PT Telkom belum pernah melakukan pengukuran terhadap tingkat *security awareness*. Tidak dipungkiri bahwa sumber daya manusia merupakan faktor pemelihara yang penting, mengingat bahwa pendayagunaan faktor pemeliharaan keamanan informasi dilakukan oleh manusia. Oleh karena itu Kesadaran keamanan sumber daya manusia terkait Pengetahuan, Sikap, dan Perilaku perlu diperhatikan dan dikelola dengan baik agar dapat meminimalisir ancaman *security* dalam mencapai tujuan perusahaan yang telah ditetapkan.

Berdasarkan penelitian (Mahardika et al., 2020) yang berjudul "*Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial Commission Republic of* Indonesia" dilakukan untuk mengukur kesadaran keamanan informasi di kalangan karyawan yang bekerja di Pusat Analisis dan Layanan Informasi (Palinfo) Komisi Yudisial Republik Indonesia. Dalam penelitian tersebut, *Human Aspects of Information Security Questionnaire* (HAIS-Q) digunakan sebagai instrumen untuk mengukur tingkat kesadaran keamanan informasi karyawan di Pusat Analisis dan Layanan Informasi. HAIS-Q mencakup tiga dimensi, yaitu *Knowledge, Attitude,* dan *Behavior*. Hasil dari penelitian sebelumnya menunjukkan bahwa pemanfaatan HAIS-Q dalam penelitian tersebut memberikan rekomendasi untuk meningkatkan kesadaran keamanan informasi di Palinfo, Pusat Analisis dan Layanan Informasi. Dengan demikian, penggunaan HAIS-Q dalam

penelitian sebelumnya terbukti efektif dalam mengukur tingkat kesadaran keamanan informasi karyawan dan memberikan panduan untuk meningkatkan kesadaran keamanan informasi di lingkungan kerja.

Mengingat *security awareness* merupakan faktor penting dalam mencapai kematangan keamanan yang tinggi, oleh karena itu Penelitian tentang pengukuran *Security Awareness* menggunakan sebuah metode dilakukan untuk mengidentifikasi apakah pengukuran awareness sudah terpenuhi atau belum terpenuhi setelah dilakukan program *Security Education Training Awareness*. Berdasarkan uraian diatas, Peneliti akan mengangkat judul "**Efektivitas program *Security Education Training Awareness* terhadap tingkat *Information Security Awareness* pegawai (Studi kasus Divisi *Information Technology* PT Telkom Indonesia, Tbk)".** Dalam penelitian ini *Human Aspects of Information Security Questionnaire* (HAIS-Q) digunakan sebagai instrumen kuesioner untuk mengukur tingkat kesadaran keamanan informasi mencakup tiga dimensi yaitu *Knowledge, Attitude,* dan *Behavior*. Dengan adanya Penelitian ini, diharapkan dapat meningkatkan kesadaran akan pentingnya keamanan informasi di berbagai sektor, serta membantu organisasi dalam melindungi aset informasi mereka.

1.3 Rumusan Masalah

Ada pula rumusan masalah dari Penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat *Information Security Awareness* di kalangan karyawan PT Telkom Indonesia, Tbk pada Divisi IT pada aspek *Knowledge, Attitude, Behavior* berdasarkan HAIS-Q?
2. Bagaimana tingkat *Information Security Awareness* di kalangan karyawan PT Telkom Indonesia, Tbk pada Divisi IT secara keseluruhan dengan menggunakan HAIS-Q?
3. Bagaimana pengaruh SETA *effectiveness* terhadap tingkat *Information Security Awareness* berdasarkan aspek *Knowledge, Attitude,* dan *Behavior*?

1.4 Tujuan Penelitian

Tujuan kegiatan ini adalah:

1. Untuk mengetahui tingkat *Information Security Awareness* pada karyawan Divisi IT di PT Telkom Indonesia, Tbk pada Divisi IT pada aspek *Knowledge, Attitude, Behavior* berdasarkan HAIS-Q
2. Untuk mengetahui tingkat *Information Security Awareness* pada karyawan Divisi IT di PT Telkom Indonesia, Tbk secara keseluruhan berdasarkan HAIS-Q

3. Untuk mengetahui pengaruh SETA *effectiveness* terhadap tingkat *Information Security Awareness* berdasarkan aspek *Knowledge, Attitude,* dan *Behavior*

1.5 Manfaat Penelitian

1.5.1 Manfaat teoritis

Secara teoritis hasil Penelitian ini diharapkan dapat bermanfaat sebagai referensi pada Penelitian-Penelitian selanjutnya dan perkembangan teori apakah model pengukuran menggunakan HAIS-Q efektif dalam pengukuran *Information Security Awareness*.

1.5.2 Manfaat praktis

Secara praktis hasil Penelitian ini bermanfaat bagi PT Telkom karena dapat menjadi model pengukuran bagi PT Telkom mengenai security awareness dengan model pengukuran HAIS-Q setelah dilakukan program *security education training awareness.*

1.6 Sistematika Penugasan Akhir

Berisi tentang sistematika dan penjelasan ringkas laporan Penelitian yang terdiri dari Bab I sampai Bab V dalam laporan Penelitian.

a. BAB I PENDAHULUAN

Dalam bab ini membahas mengenai gambaran umum objek Penelitian, latar belakang Penelitian yang berkaitan dengan fenomena yang terjadi, rumusan masalah, tujuan Penelitian, manfaat Penelitian dari aspek teoritis dan aspek praktis yang diambil dari Penelitian, dan sistematika Penelitian tugas akhir.

b. BAB II TINJAUAN PUSTAKA

Dalam bab ini berisi teori dari umum sampai ke khusus, disertai Penelitian terdahulu dan dilanjutkan dengan kerangka pemikiran Penelitian yang diakhiri dengan hipotesis jika diperlukan

c. BAB III METODE PENELITIAN

Dalam bab ini menegaskan pendekatan, metode dan teknik yang digunakan untuk mengumpulkan serta menganalisis temuan yang dapat menjawab masalah Penelitian. Bab ini meliputi uraian tentang: Jenis Penelitian, Operasionalisasi Variabel, Populasi dan Sampel (untuk kuantitatif) / Situasi Sosial (untuk kualitatif), Pengumpulan Data, Uji Validitas dan Reliabilitas, serta Teknik Analisis Data.

d. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Dalam bab ini hasil Penelitian dan pembahasan diuraikan secara sistematis sesuai dengan perumusan masalah serta tujuan Penelitian disajikan dalam sub judul tersendiri. Bab ini berisi dua bagian: bagian pertama menyajikan hasil Penelitian dan bagian kedua menyajikan pembahasan atau analisis dari hasil Penelitian. Setiap aspek pembahasan hendaknya dimulai dari hasil analisis data, kemudian diinterpretasikan dan selanjutnya diikuti oleh penarikan kesimpulan.

e. BAB V KESIMPULAN DAN SARAN

Dalam bab ini berisi kesimpulan merupakan jawaban dari pernyataan Penelitian, kemudian menjadi saran yang berkaitan dengan manfaat Penelitian.