BAB 1

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan berkembangnya teknologi, informasi menjadi aset yang sangat penting bagi sebuah perusahaan dan karyawan sangat berperan penting dalam menjaga keamanan informasi. Tidak dapat dipungkiri informasi dengan sangat mudah dapat disebarluaskan, tetapi banyak pihak tidak bertanggung jawab yang menyalahgunakan informasi tersebut sehingga menimbulkan ancaman dan resiko yang dapat merugikan perusahaan. Seperti contoh data perusahaan dapat diambil oleh pesaing bisnisnya dan digunakan untuk menjatuhkan perusahaan tersebut. Tetapi masih banyak perusahaan yang belum menyadari pentingnya menjaga keamanan informasi yang merupakan aset dari perusahaan itu sendiri. Teknologi informasi dan komunikasi telah menjadi penting bagi organisasi dan individu untuk mempertahankan produktivitas tingkat tinggi. Adopsi teknologi ini disertai dengan sejumlah besar kerentanan baru, dan karenanya ancaman baru terhadap kerahasiaan dan integritas data pribadi dan perusahaan.[1]

Ketergantungan pada sistem informasi memaksa perusahaan untuk terus berupaya dalam menegakkan keamanan informasi yang mereka miliki. Untuk melindungi sistem informasi dan aset informasi oraganisasi pada tingkat individu, *information security awareness* atau kesadaran keamanan informasi dianggap sebagai faktor penting yang mempengaruhi perilaku keamanan individu.[2] Secara umum, kesadaran keamanan informasi meninjau pengetahuan dan pemahaman individu terkait dengan keamanan informasi seperti risiko dan ancaman keamanan, tujuan organisasi, prosedur dan kebijakan terkait dengan keamanan.

Perilaku manusia ditentukan oleh budaya, pengaruh interaksi dalam lingkungan sosial dan pekerjaan sehari-hari[3]. Lingkungan kerja memiliki banyak individu dari berbagai budaya dan lingkungan sosial yang berbeda, maka perilaku yang dimiliki juga berbeda terutama terhadap keamanan informasi. Perilaku manusia terhadap keamanan informasi tidak hanya sebatas menciptakan risiko tetapi juga mencegah pelanggaran yang akan terjadi.[4] Dalam konteks organisasi, penyebab utama kesalahan manusia adalah ketidakpatuhan atau ketidak-sadaran terhadap risiko daripada niat jahat yang disengaja. [5]

Dalam kasus *human error*, karyawan seringkali menjadi sumber dari kegagalan keamanan sistem informasi. Berdasarkan penelitian Global State of Information Security Survey pada tahun 2015, insiden keamanan informasi yang disebabkan oleh karyawan terjadi sebanyak 38% pada tahun 2014-2015 dan mengakibatkan kerugian pada perusahaan rata-rata sebanyak $2.5 Juta.[6] Dalam sebuah penelitian juga disebutkan bahwa kesalahan yang dilakukan manusia mendominasi 95% dari insiden keamanan informasi. [1] Menurut International Data Corporation, pengeluaran perusahaan global untuk meningkatkan keamanan IT diperkirakan meningkat dari 83,5 M USD pada 2017, menjadi 119,9 M USD pada 2021. Tetapi ada pengeluaran yang dianggarkan duakali lipat dari keamanan IT yaitu keamanan informasi, hal tersebut dikarenakan banyak kegagalan informasi yang terjadi sering kali mengakibatkan kerugian finansial yang besar dan membahayakan perusahaan. [7]

Bank BTN merupakan sebuah Badan Usaha Milik Negara (BUMN) yang berbentuk perseroan terbatas yang bergerak pada bidang jasa keuangan atau perbankan. Salah satu misi yang dimiliki oleh Bank BTN adalah melatih dan menghasilkan SDM yang berintegritas dan berkualitas, sehingga perlu diketahui sejauh apa karyawan yang mereka miliki memahami hal tersebut. Bank BTN KC Solo belum pernah melakukan pengukuran information security awareness atau kesadaran keamanan informasi sehingga penelitian akan dilakukan untuk melakukan pengukuran kesadaran keamanan informasi. Tujuan pengukuran ini adalah untuk menghasilkan validasi instrumen empiris untuk melihat sejauh mana karyawan pada sebuah perusahaan memahami pentingnya menjaga keamanan sistem informasi. Ada beberapa instrumen yang dapat digunakan pada pengukuran informasi seperti *Multiple Criteria Decision Analysis* (MCDA), *Analytical Hierarchy Process* (AHP), *The Risky, Impulsive, & Self-destructive behavior Questionnaire* (RISQ), *Social Learning Teory* (SLT) dan masih banyak lainnya. Instrumen yang akan digunakan pada penelitian ini adalah *Human Aspects of Information Security Questionnaire* (HAIS-Q), instrumen ini mengukur sejauh mana pengetahuan, sikap dan perilaku karyawan dalam menjaga keamanan informasi. Alat ini juga dapat dijadikan sebagai acuan, yang dapat digunakan untuk mengevaluasi keefektifan kontrol teknologi informasi, atau menyusun rencana jangka panjang perusahaan.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang ada diatas maka yang akan menjadi rumusan masalah adalah sebagai berikut:

Keamanan informasi merupakan hal yang sangat penting bagi sebuah perusahaan maka perlu diperhatikan keamanannya. Karyawan sangat berperan penting dalam menjaga keamanan informasi. Untuk mengetahui sejauh apa keamanan informasi yang dimiliki perusahaan, ada baiknya dilakukan pengukuran keamanan informasi untuk menjadi tolak ukur dalam meningkatkan dan menjaga keamanan informasi perusahaan. Dengan melakukan pengukuran keamanan informasi perusahaan dapat mengetahui seberapa jauh karyawan memahami kebijakan, aturan dan pedoman yang dimiliki perusahaan terkait dengan keamanan informasi. Perusahaan juga dapat melihat bagaimana pengetahuan, sikap dan perilaku yang dimiliki karyawan terhadap keamanan informasi. Bank BTN KANTOR CABANG Solo belum pernah melakukan pengukuran *Information Security Awareness* (ISA). Dengan melakukan pengukuran *Information Security Awareness* perusahaan dapat meningkatkan kompetensi dan dapat mencegah terjadinya kegagalan keamanan informasi yang berpotensi merugikan perusahaan.

1.3 Pertanyaan Penelitian

Pertanyaan penelitian adalah sebagai berikut:

1. Bagaimana tingkat *Information Security Awareness* (ISA) yang dimiliki oleh subjek penelitian?
2. Fokus area mana saja yang perlu ditingkatkan dan solusi apa yang dapat digunakan untuk meningkatkan *Information Security Awareness* (ISA) pada subjek penelitian?

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mendapatkan hasil pengukuran tingkat *Information Security Awareness* (ISA) yang dimiliki oleh subjek penelitian.
2. Mengetahui fokus area mana saja yang perlu ditingkatkan dan solusi apa yang bisa diberikan agar *Information Security Awareness* yang dimiliki subjek penelitian menjadi lebih baik.

1.5 Batasan Masalah

Dikarenakan luasnya permasalahan yang berhubungan dengan kesadaran keamanan informasi maka perlu dibuat batasan masalah sebagai berikut:

1. Tingkat kesadaran yang diukur menggunakan HAIS-Q sebagai pedoman. Terdapat 63 item yang menilai 7 fokus area yang diukur yaitu; manajemen *password*, pemakaian *email*, pemakaian internet, pemakaian social media, pemakaian perangkat seluler, penanganan informasi, dan pelaporan insiden.
2. Ruang lingkup penelitian ini terbatas pada subjek penelitian.

1.6 Manfaat Penelitian

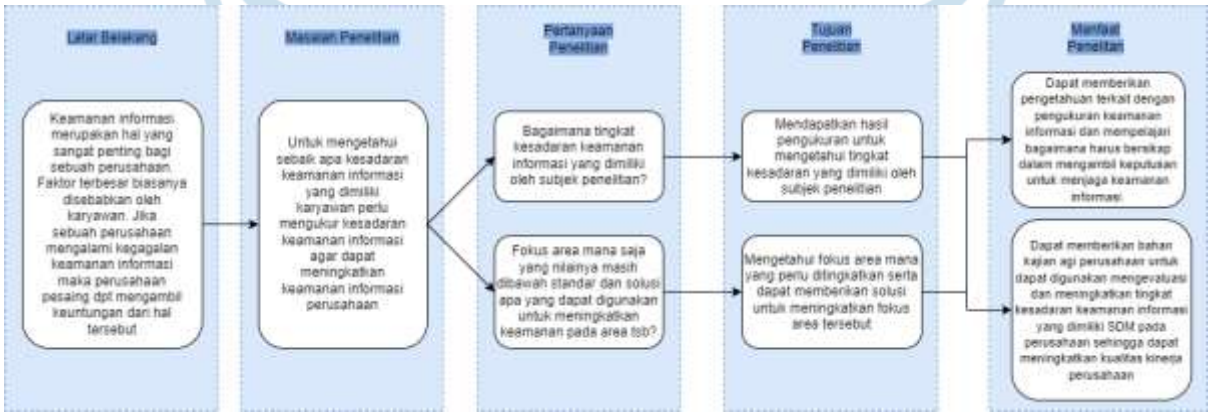
a. Bagi keilmuan atau perkembangan ilmu

Memberikan pengetahuan terkait dengan pengukuran *Information Security Awareness* (ISA) sehingga dapat lebih mendalami tentang keamanan informasi dan mempelajari bagaimana harus bersikap dalam mengambil keputusan untuk menjaga keamanan informasi.

b. Bagi organisasi/perusahaan/dll

Sebagai bahan kajian bagi perusahaan untuk mengevaluasi dan meningkatkan *Information Securirty Awareness* yang dimiliki SDM pada perusahaan tersebut, sehingga dapat meningkatkan kualitas dan kinerja perusahaan.

1.7 Bagan Keterkaitan



Bagan 1 Bagan Keterkaitan