BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Bank X merupakan representasi yang terdiri dari tiga bank Badan Usaha Milik Negara (BUMN) terbesar di Makassar. Ketiga bank ini memiliki peran paling berpengaruh dalam mendukung perekonomian di Indonesia khususnya di kota Makassar, yang menawarkan beragam produk dan layanan keuangan yang melayani segala kebutuhan nasabah individu, korporat, hingga institusi. Bank X memiliki komitmen terhadap inovasi dan teknologi agar terus memperbarui layanan digitalnya untuk mempermudah nasabah dalam melakukan segala transaksi perbankan yaitu, *mobile bangking*, *internet banking* dan solusi pembayaran digital lainnya. Selain menjadi produk simpanan, pinjaman pribadi, kartu kredit dan kartu debit, Bank X juga menawarkan solusi keuangan dalam bentuk berbagai jenis pinjaman, layanan asuransi dan investasi yang dapat dengan mudah diakses oleh nasabah. Bank X memiliki jaringan operasional yang luas dengan puluhan kantor cabang, kantor cabang pembantu, serta unit pelayanan yang tersebar di berbagai kota besar hingga ke daerah terpencil, Bank X berfokus meningkatkan kapasitas karyawan untuk meningkatkan layanan serta mengikuti perkembangan teknologi finansial.

Ketiga bank ini memiliki ribuan karyawan yang menunjukkan skala operasional yang luas dan kompleks. Karyawan Bank X merupakan tulang punggung perusahaan, yang memainkan peran penting dalam pengelolaan transaksi keuangan, layanan pelanggan, dan fungsi sistem perbankan secara keseluruhan. Karyawan Bank X diharuskan memiliki keterampilan teknis dan interpersonal mengenai teknologi perbankan saat ini. Bank juga meyakini bahwa kapabilitas, keterampilan dan keterpanggilan karyawan berpengaruh terhadap kinerja perusahaan yang sustain dalam jangka panjang. Karyawan Bank X memainkan peran penting dalam menumbuhkan kepercayaan pelanggan, interaksi mereka dengan pelanggan dapat mempengaruhi keputusan pelanggan untuk terus menggunakan layanan Bank X. Karyawan Bank X juga

merupakan aset penting perusahaan dalam menjaga keamanan untuk menjaga kepercayaan dan stabilitas perusahaan, terutama serangan siber yang semakin meningkat di sektor keuangan.

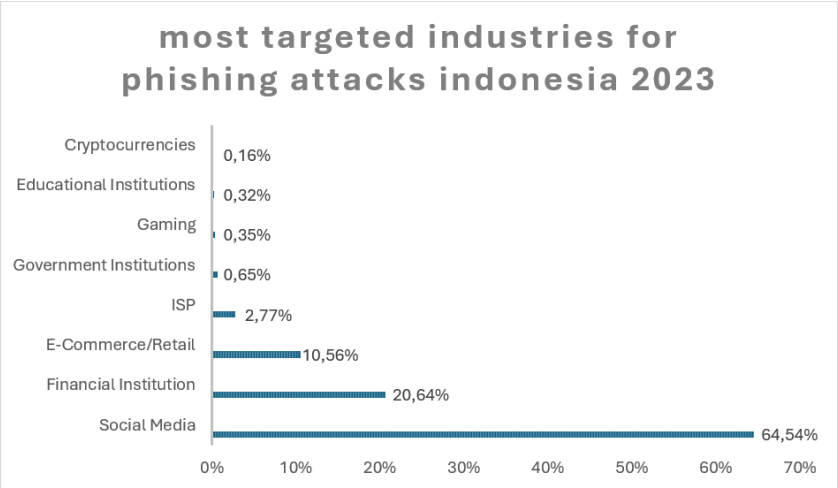
1.2 Latar Belakang Penelitian

Perkembangan teknologi informasi dan komunikasi membawa perubahan pada sektor perbankan di Indonesia. Pemanfaatan teknologi digital dapat menghemat waktu, mengurangi biaya operasional, mengoptimalkan pemantauan, manajemen risiko, dan prosedur kontrol yang memungkinkan bank untuk menawarkan ke pelanggan produk dan layanan yang lebih baik (Boufounou et al ., 2022). Hal ini menurunkan ketergantungan pada proses manual, sehingga mengurangi biaya operasional. Menurut Bank Indonesia pada Mei 2024, nilai transaksi perbankan digital meningkat 10,82% dibandingkan tahun sebelumnya, mencapai Rp5.570,49 triliun. Sehingga, semakin banyak individu yang percaya pada layanan perbankan berbasis teknologi, yang membuat transaksi finansial lebih mudah dan nyaman.

Penyebaran ini didorong oleh adopsi yang cepat oleh masyarakat indonesia, yang semakin banyak memanfaatkan layanan digital untuk berbagai transaksi keuangan. Alasan mereka memilih layanan ini karena fleksibilitas dan fitur yang memenuhi kebutuhan mereka, seperti keamanan, kemudahan transaksi, dan kemudahaan penggunaan (Sulaiman Fajar, 2024). Menurut Johri & Kumar (2023) Adanya *mobile banking* dan *internet banking* menjadi cara praktis untuk melakukan transaksi keuangan, namun di sisi lain terdapat beragam tantangan teknologi. (Stefanovic et al ., 2021) Studi ini menunjukkan bahwa digitalisasi tidak hanya meningkatkan kinerja bank, tetapi juga meningkatkan risiko operasional, termasuk ancaman keamanan informasi. Lembaga keuangan, bisnis, dan individu sering menjadi target serangan siber untuk mencuri data sensitif atau melakukan penipuan (Irughe et al ., 2022). Dilansir dari Laporan Badan Siber dan Sandi Negara (BSSN) 2021 menunjukkan bahwa terdapat 920 juta serangan siber di Indonesia dari Januari hingga September 2021, dengan sektor keuangan yang paling sering terkena dampak. Hal ini mencerminkan

pentingnya perlindungan yang lebih kuat terhadap infrastruktur digital di sektor perbankan untuk mencegah kerugian finansial dan melindungi data sensitif nasabah.

Keamanan informasi mengacu kepada peranan penting dalam menjaga aset digital milik bank maupun pelanggannya. Penyebaran kejahatan siber, data atau informasi telah menjadi sumber daya strategis yang memerlukan perlindungan dan menjadi isu utama dalam digitalisasi (Onyshchenko et al ., 2023). Kekhawatiran tentang serangan siber khususnya pada sektor perbankan yang terus meningkat, sangat penting untuk memahami situasi dan jenis ancaman siber yang paling umum, seperti *malware, phishing, dan ransomware* (Bhagwani et al . 2023). Serangan siber dalam bentuk *Ransomware* di Indonesia terjadi pada sistem Bank Syariah Indonesia (BSI) menggemparkan publik setelah mengalami serangan siber yang menyebabkan sistem dan layanan bank bermasalah dan tidak dapat diakses oleh nasabah selama beberapa hari (BBC News INDONESIA, 2023). BSI telah mengambil kebijakan mitigasi, termasuk meningkatkan jam layanan kepada pelanggan selama pemulihan *mobile banking* dan menegaskan bahwa mereka akan terus berupaya mencegah potensi ganguan data dengan meningkatkan sistem proteksi dan ketahanan sistem (Dewi et al . 2023). Langkah-langkah ini tidak hanya relevan bagi BSI, tetapi juga mencerminkan kebutuhan yang lebih luas di seluruh industri perbankan, mengingat tingginya risiko serangan *phishing* yang ditunjukkan pada Gambar 1.1.



Gambar 1. 1 Industri *online* terkena serangan *phishing* di Indonesia Q4 2023

Sumber: Statista.com (2024)

Gambar 1.1 menunjukkan bahwa pada kuartal keempat 2023, serangan *phishing* di Indonesia paling banyak menargetkan platform media sosial, dengan persentase mencapai 64,54%. Sektor keuangan, termasuk perbankan, berada di posisi kedua dengan 20,64%, menjadikannya salah satu industri paling rentan terhadap ancaman siber. Tingginya persentase ini menyoroti risiko signifikan yang dihadapi industri perbankan, karena serangan *phishing* sering kali menyasar data keuangan yang sensitif. Data ini mempertegas pentingnya implementasi langkah-langkah keamanan siber yang lebih ketat di sektor perbankan untuk melindungi nasabah dari ancaman siber seperti *phishing* yang terus meningkat dan semakin canggih. Hal ini menyatakan setiap anggota organisasi, termasuk karyawan, harus bertindak dan aktif untuk melindungi organisasi dari ancaman serangan siber.

Cybersecurity awareness mencakup pemahaman tentang ancaman siber yang mungkin terjadi dan langkah-langkah yang diperlukan untuk melindungi data dan sistem informasi(Akter et al ., 2022). Menurut Sulaiman et al (2022) Faktor-faktor seperti *perceived barriers, self-efficacy,* dan *response efficacy* mempengaruhi bagaimana karyawan merespons ancaman keamanan dan tingkat keyakinan mereka dalam menangani ancaman siber. *Perceived barriers* dapat menghalangi karyawan dalam merespons ancaman keamanan dengan

efektif. Hal ini dapat disebabkan oleh keterbatasan sumber daya, kurangnya pelatihan yang memadai, atau prosedur keamanan yang rumit dan sulit untuk diterapkan (Khan et al ., 2022). *Self-efficacy* dikaitkan dengan kepatuhan yang lebih baik terhadap protokol keamanan dan perilaku yang lebih proaktif dalam mencegah ancaman siber (Yu et al ., 2022). *Response efficacy* berkaitan dengan keyakinan bahwa tindakan yang diambil dapat secara signifikan mengurangi ancaman, sehingga karyawan yang merasa respons tersebut efektif cenderung lebih aktif dalam melaksanakan perilaku protektif dan mengikuti langkah-langkah keamanan (Yu et al ., 2022). Oleh karena itu, pengembangan kebijakan yang tepat menjadi sangat penting untuk mendukung peningkatan kesadaran keamanan siber.

Tanpa adanya kebijakan yang jelas, sekedar kesadaran tidak akan memadai untuk menghadapi kompleksitas ancaman siber. Pimpinan dalam suatu organisasi perlu menyelaraskan strategi keamanan siber dengan tujuan bisnis dan membangun budaya kepercayaan yang kuat untuk memperkuat ketahanan terhadap risiko siber, sehingga menegaskan perlunya *provion of policies* yang komprehensif dalam melindungi sistem informasi (Loonam et al ., 2022). Menurut Amer et al (2023) untuk melindungi diri dari serangan siber, karyawan dan organisasi harus mengambil tindakan pencegahan yang diperlukan, seperti membuat kebijakan tentang penggunaan perangkat lunak dan prosedur tanggap darurat terhadap ancaman siber. Penyediaan kebijakan yang efektif merupakan komponen penting dalam meningkatkan kepatuhan terhadap standar keamanan siber di tempat kerja. Meskipun kebijakan telah disusun, keberhasilannya sangat dipengaruhi oleh implementasi program pelatihan yang efektif, seperti SETA.

Pendidikan, pelatihan, dan kesadaran keamanan (SETA) adalah salah satu pendekatan yang paling umum untuk tata kelola keamanan organisasi (Hu et al ., 2022). *Programs SETA* yang diterapkan dengan baik dapat memberikan edukasi kepada karyawan mengenai ancaman yang mereka hadapi, besarnya risiko keamanan yang ada, serta cara terbaik untuk melindungi diri mereka dari potensi bahaya tersebut (Zwilling et al ., 2022). Bank X telah mengembangkan dan mengimplementasikan sebuah program kesadaran keamanan guna

meningkatkan kesadaran keamanan karyawan dengan memberikan pendidikan dan pelatihan kepada seluruh karyawan dari berbagai tingkatan. Program yang dilakukan Bank X ini mencakup topik-topik yang disampaikan melalui *e-Leaning*, *Newsletter*, *Podcast*, dan Poster. Selain itu karyawan Bank X juga ikut serta dalam melakukan kampanye *email phishing* untuk menjadi bekal dalam mengidentifikasi dan menghindari *email phishing*. *Programs SETA* yang efektif memiliki potensi untuk meningkatkan kesadaran keamanan siber karyawan terhadap praktik keamanan, yang pada gilirannya dapat meningkatkan perilaku mereka dalam menjaga keamanan sistem informasi (Davis et al ., 2023). Selain itu, niat untuk mematuhi kebijakan ini juga sangat penting untuk menentukan seberapa efektif pelatihan yang diberikan.

Beberapa penelitian empris menunjukkan bahwa pemikiran yang positif tentang kebijakan keamanan siber akan berdampak kepada tingkat kepatuhan yang lebih tinggi terhadap norma dan standar yang berkaitan dengan *Information security policy compliance (ISPC)* (Bulgurcu et al ., 2010; Siponen et al ., 2014; Swaim et al ., 2014). Program kesadaran sangat penting dalam membentuk sikap positif terhadap ISPC. *Intention toward ISPC* dapat diartikan karyawan yang lebih sadar akan langkah-langkah keamanan siber cenderung memiliki sikap yang lebih baik terhadap kepatuhan, yang pada gilirannya mempengaruhi niat mereka untuk mematuhi dan terlibat dalam perilaku protektif (Tran et al . 2024). Sikap yang muncul terhadap kebijakan ini sangat dipengaruhi oleh sikap individu terhadap keamanan informasi secara umum.

Untuk menjaga integritas, kerahasiaan, dan aset milik perusahaan, penting membentuk perilaku keamanan informasi dikalangan karyawan, bukan hanya tanggung jawab tim TI atau keamanan, tetapi seluruh individu dalam suatu organisasi. Risiko dan insiden keamanan dapat berkurang dengan perilaku kepatuhan keamanan individu (Donalds et al . 2020). Sikap terhadap kebijakan keamanan siber berdampak langsung pada kepatuhan dan perilaku pelanggaran. Teori seperti Teori Motivasi Perlindungan dan Teori Perilaku Terencana menyoroti peran sikap dalam membentuk niat kepatuhan. Karyawan dengan

sikap positif lebih cenderung patuh, sedangkan mereka yang memiliki sikap negatif mungkin terlibat dalam pelanggaran (Sulaiman et at., 2022).

Peran karyawan Bank X sangat penting karena mereka merupakan pengguna utama sistem informasi. Banyak penelitian sebelumnya yang lebih fokus pada aspek keamanan siber nasabah, sementara peran karyawan sebagai pengelola serta pihak yang bertanggung jawab atas data pelanggan dan aset perusahaan sering kali terabaikan (Candiwan & Rianda, 2024). Karyawan seringkali mengabaikan praktik kepatuhan keamanan informasi sehingga menempatkan perusahaan dalam risiko seperti serangan siber (Jamil et al ., 2024). Dalam sebuah studi yang dilakukan oleh *TalentLMS*, sebanyak 61% karyawan yang sudah menerima program edukasi keamanan siber masih gagal, ada kemungkinan karyawan tidak menganggap serius masalah keamanan informasi (Marousis a, 2021). Menurut Laporan Investigasi Pelanggaran Data yang diterbitkan oleh Verizon, sebagian besar serangan siber berasal dari pihak eksternal, yang mencakup individu atau kelompok kejahatan terorganisasi, dengan proporsi mencapai 65%. Sementara itu, 35% sisanya dipicu oleh pihak internal, seperti karyawan dan mitra bisnis perusahaan. Temuan ini menunjukkan bahwa ancaman keamanan tidak hanya berasal dari luar, tetapi juga dari dalam organisasi, sehingga upaya mitigasi harus mencakup strategi pengamanan terhadap kedua sumber ancaman ini. Sehingga, untuk menghindari hal tersebut perlu dipadukan dengan motivasi yang kuat untuk melindungi informasi organisasi.

Information protection motivation memainkan peran penting dalam memengaruhi perilaku karyawan dalam hal kepatuhan terhadap kebijakan keamanan informasi (Tran et al ., 2024). Tingkat keinginan karyawan untuk mengambil tindakan pencegahan serangan siber dikenal sebagai motivasi perlindungan informasi (Ma, 2022). Motivasi ini muncul sebagai hasil dari penilaian ancaman dan penanggulangan. Ini berfungsi sebagai variabel intervensi dan sebanding dengan motivasi lain yang mendorong, mempertahankan, dan mengarahkan tindakan karyawan (Martens et al ., 2019).

Motivasi ini akan tercermin dalam tindakan perlindungan yang dilakukan oleh karyawan dalam kegiatan sehari-hari.

Employee protective behaviour menjadi semakin penting di tengah tingginya intensitas ancaman siber yang dihadapi perusahaan dalam menjaga keamanan informasi. Ketergantungan yang meningkat pada teknologi digital telah memperbesar potensi risiko keamanan, sehingga dibutuhkan perilaku protektif yang lebih optimal dari karyawan untuk melindungi infrastruktur digital perusahaan dari berbagai ancaman (Saeed, 2023). Namun, karyawan cenderung mengabaikan perilaku keamanan yang diperlukan ketika mereka merasa bahwa tantangan untuk melindungi data lebih besar dibandingkan dengan manfaat yang diperoleh (Sari et al ., 2023). Untuk menghadapi kondisi ini, Bank X telah menerapkan kebijakan keamanan informasi yang ketat guna melindungi operasional perusahaan dan data nasabah. Selain itu, Bank X juga memiliki divisi khusus yang bertugas mengelola ancaman keamanan siber secara terfokus dan sistematis. Divisi ini berfungsi untuk menjamin kesesuian standar dan praktik yang baik internasional.

Salah satu bank yang menjadi objek penelitian ini menyatakan berkomitmen untuk menjaga keamanan data dan meningkatkan kesadaran karyawan terhadap risiko siber. Namun, perwakilan dari bank tersebut, mengungkapkan bahwa setiap harinya terdapat setidaknya 1 juta kali percobaan serangan siber yang harus dihadapi oleh bank ini. Perwakilan dari bank ini juga mengungkapkan serangan siber banyak terjadi karena faktor manusia, yaitu sekitar 80%. Pentingnya menjaga keamanan informasi dan memahami kebijakan keamanan informasi untuk meningkatkan sikap kepatuhan karyawan dalam meningkatkan kemampuan reaktif rantai pasokan (Wong et al ., 2022).

Penyediaan kebijakan keamanan informasi yang efektif sangat bergantung pada komunikasi yang jelas dan tepat guna meningkatkan tingkat kepatuhan. Penelitian menunjukkan bahwa cara kebijakan dikomunikasikan, termasuk kesesuaian media dan umpan balik segera, memiliki pengaruh signifikan terhadap kepatuhan terhadap kebijakan tersebut (Rantao & Njenga, 2020). Selain itu, program Pendidikan, Pelatihan, dan Kesadaran Keamanan (SETA)

berperan penting dalam meningkatkan pemahaman karyawan tentang ancaman keamanan siber serta perilaku perlindungan yang tepat, yang secara langsung berkontribusi pada pengurangan risiko di organisasi (Tabrizi, 2022). Kesadaran yang tinggi terhadap keamanan siber, yang dapat ditingkatkan melalui pelatihan dan pendidikan, membantu mengurangi kerentanannya terhadap ancaman seperti *malware dan phising*, serta memperkuat struktur keamanan organisasi (Tabrizi, 2022). Niat untuk mematuhi kebijakan keamanan informasi juga dipengaruhi oleh pemahaman yang baik tentang kebijakan tersebut, serta komunikasi yang efektif mengenai pentingnya kepatuhan (Rantao & Njenga, 2020). Sikap positif terhadap kepatuhan keamanan siber, yang dibentuk melalui pendidikan berkelanjutan dan penguatan pesan tentang pentingnya langkah-langkah keamanan, sangat penting untuk memastikan bahwa karyawan menjalankan praktik keamanan yang benar (Rantao & Njenga, 2020). Akhirnya, perilaku protektif karyawan menjadi tujuan utama dari semua inisiatif ini, dengan keterlibatan aktif karyawan dalam menjaga aset organisasi dan mengurangi serangan keamanan siber menjadi faktor kunci untuk mempertahankan tingkat perilaku protektif karyawan yang tinggi (Kannelønning & Katsikas, 2023; Reeves et al ., 2021).

Pada penelitian yang sebelumnya dilakukan oleh Dien Van Tran dkk, Studi ini terbatas pada organisasi Vietnam, yang dapat mempengaruhi generalisasi temuan ke negara atau wilayah lain. Dalam hal budaya, ekonomi, dan teknologi di Vietnam mungkin berbeda secara signifikan dari yang ada di negara berkembang atau maju lainnya, berpotensi membatasi penerapan hasil di luar pengaturan khusus ini. Studi ini juga tidak berfokus pada satu sektor saja. Maka dari itu, pada penelitian ini akan berfokus pada analisis sikap protektif karyawan dalam menjaga keamanan informasi di sektor perbankan di negara Indonesia.

Penelitian ini dilakukan oleh penulis dengan mengacu pada latar belakang diatas, peneliti akan fokus pada hubungan antara faktor-faktor yang memepengaruhi *cybersecurity behavior Compliance* terhadap sikap protektif karyawan untuk mengukur efektivitas kebijakan Bank X di Makassar. Melalui uraian tersebut, maka penulis tertarik untuk melakukan penelitian dengan judul

"Analisis Faktor-Faktor yang Mempengaruhi *Cybersecurity Compliance* terhadap *Employee Protective Behaviour* di Bank X".

1.3 Perumusan Masalah

Rumusan masalah ini disusun untuk mengidentifikasi hubungan antara faktor-faktor yang mempengaruhi sikap protektif karyawan dalam menjaga keamanan informasi Bank X di Makassar, mengingat pentingnya kesadaran dan perilaku keamanan siber dalam menghadapi ancaman siber yang terus meningkat. Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana pengaruh kesadaran dan perilaku keamanan siber karyawan terhadap sikap protektif dalam menjaga keamanan informasi di Bank X?
2. Bagaimana tata kelola Bank X memengaruhi kesadaran keamanan siber karyawan?
3. Bagaimana peran niat terhadap kepatuhan kebijakan keamanan informasi (ISPC) dalam memediasi hubungan antara perilaku protektif karyawan dan sikap mereka terhadap kepatuhan keamanan siber?
4. Bagaimana faktor-faktor dalam perilaku siber memengaruhi sikap protektif karyawan di Bank X untuk melindungi aset dan informasi di Bank X?

1.4 Tujuan Penelitian

Berdasarkan uraian perumusan masalah, maka tujuan penelitian ini di antaranya sebagai berikut:

1. Menganalisis pengaruh kesadaran dan perilaku keamanan siber karyawan terhadap Sikap protektif dalam menjaga keamanan informasi di Bank X
2. Menganalisis pengaruh tata kelola Bank X terhadap kesadaran keamanan siber karyawan.
3. Menguji hubungan niat terhadap kepatuhan kebijakan keamanan informasi (ISPC) memediasi hubungan antara perilaku protektif karyawan dan sikap kepatuhan keamanan siber.

4. Memberikan rekomendasi bagi Bank X untuk meningkatkan perilaku siber dan sikap protektif karyawan untuk melindungi aset dan informasi di Bank X.

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian dan dengan dilakukannya penelitian ini, maka diharapkan dapat memberikan kebermanfaatan secara menyeluruh, di antaranya sebagai berikut:

a. Manfaat Teoritis

Penelitian ini diharapkan bermanfaat untuk menambah wawasan penulis terkait keamanan informasi dalam perusahaan di Indonesia yang merupakan salah satu perusahaan yang berpengaruh atas perekonomian negara Indonesia dan memberikan kesempatan bagi penulis untuk mengimplementasikan materi dan teori dari hasil yang telah dipelajari semasa perkuliahan. Penelitian ini diharapkan dapat berkontribusi dalam memperkaya literatur dan penelitian terkait *cybersecurity behavior* di sektor perbankan. Penelitian ini diharapkan juga dapat menjadi referensi untuk peneliti selanjutnya, khususnya yang mengkaji lebih dalam terkait peran perilaku karyawan terhadap risiko siber.

b. Manfaat Praktis

Penelitian ini diharapkan dapat digunakan oleh Bank X sebagai bahan untuk mengevaluasi dan meningkatkan kinerja keamanan informasi perusahaan. Bank X yang diteliti dapat menggunakan hasil penelitian ini untuk memahami perilaku karyawan yang mempengaruhi penerapan kebijakan keamanan informasi. Penelitian ini diharapkan dapat meningkatkan kesadaran dan pengetahuan karyawan tentang pentingnya berperilaku siber dalam lingkungan kerja. Penelitian ini diharapkan juga dapat digunakan oleh bank dan perusahaan lain sebagai acuan dalam membuat kebijakan kesadaran dan sikap keamanan siber karyawannya.

c. Manfaat Sosial dan Ekonomi

Penelitian ini diharapkan sebagai bahan acuan untuk meningkatkan kesadaran dan sikap protektif karyawan, sehingga perusahaan dapat

mengurangi risiko kebocoran data atau insiden yang berpotensi merugikan perusahaan secara finansial. Perusahaan juga dapat menerapkan keamanan informasi yang baik tidak hanya untuk menjaga reputasi perusahaan, tetapi juga untuk menjaga kepercayaan nasabah dan publik. Terakhir, Keberhasilan dalam membentuk *employee protective behaviour* dalam menjaga keamanan informasi akan meningkatkan kepercayaan pelanggan terhadap layanan bank.

1.6 Sistematika Penulisan Tugas Akhir

Penelitian ini akan disusun dalam beberapa baba sesuai dengan menggunakan sistematika penulisan tugas akhir diantarnya sebagai berikut:

a. BAB I PENDAHULUAN

Bab pendahuluan memberikan penjelasan mengenai gambaran umum objek penelitian dan latar belakang penelitian yang membahas fenomena serta memberikan alasan teoritis, menguraikan rumusan masalah, tujuan penelitian yang ingin dicapai, manfaat penelitian dan sistematika penulisan tugas akhir.

b. BAB II TINJAUAN PUSTAKA

Bab tinjauan pustaka memberikan penjelasan tentang teori-teori terkait penelitian yang akan digunakan dan terkait penelitian terdahulu yang dianggap relevan dan telah diuji akan digunakan sebagai landasan penelitian ini, serta berisi tentang pengembangan hipotesis dan kerangka pemikiran.

c. BAB III METODE PENELITIAN

Bab metode penelitian memberikan penjelasan tentang metode yang digunakan dalam penelitian ini seperti, variabel, populasi dan sampel data, teknik pengumpulan data, serta teknik analisis data.

d. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab hasil penelitian dan pembahasan memberikan penjelasan tentang hasil penelitian yang telah dianalisis dan diolah dengan berlandaskan teori yang relevan untuk menghasilkan analisis hipotesis penelitian.

e. BAB V KESIMPULAN DAN SARAN

Bab kesimpulan dan sara memberikan kesimpulan serta jawaban dari pertanyaan penelitian atas hasil penelitian ini dan saran atas keterbatasan hasil penelitian yang dapat digunakan oleh peneliti berikutnya.