BAB 1
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Perilaku keamanan informasi merujuk pada tindakan dan sikap karyawan terhadap kebijakan dan praktik keamanan informasi dalam suatu organisasi. Menurut Rafli et al. (2024) perilaku keamanan informasi dalam sebuah perusahaan adalah hal yang penting guna memastikan keamanan dan ketersediaan informasi yang dibutuhkan.

Karyawan merujuk pada individu yang berperan aktif dalam suatu organisasi atau perusahaan, dengan tujuan untuk memberikan kontribusi melalui upaya fisik, keterampilan, dan keahlian yang mereka miliki. Menurut Fadillah et al. (2021) mengemukakan bahwa karyawan merupakan elemen yang paling fundamental dalam sebuah perusahaan, karena keberhasilan atau kegagalan sebuah organisasi sangat bergantung pada kualitas kinerja setiap individu yang terlibat di dalamnya.

Para ekonom mendefinisikan bank sebagai perantara keuangan. Menurut Jindal & Mittal (2022) bank menerima simpanan dan memberikan pinjaman kepada nasabah dan mendapatkan keuntungan dari selisih suku bunga yang dibayarkan dan dibebankan. Karyawan bank, secara khusus, adalah individu yang bekerja di lembaga keuangan yang menyediakan berbagai layanan perbankan, seperti simpanan, pinjaman, dan layanan keuangan lainnya.

Di Indonesia, jumlah karyawan bank terus berubah sesuai dengan perkembangan teknologi dan kebutuhan operasional. Dilansir dari situs infobanknews.com berdasarkan data Biro Riset Infobank (BirI), jumlah pegawai bank pada tahun 2022 tercatat sebanyak 432.954 orang, dan baru naik menjadi 441.145 orang pada 2023 (Pratama, 2024). Untuk memahami konteks penelitian, penting untuk menguraikan kategori dan jenis bank yang ada di Indonesia. Dilansir dari Gramedia.com bank-bank di Indonesia terbagi menjadi beberapa kategori, yakni sebagai berikut:

Tabel 1.1 Kategori dan Jenis Bank

Kategori Bank	Jenis Bank	Contoh Bank
Bank Umum	Bank Pembangunan Daerah	Bank Jabar Banten, Bank DKI
	Bank Swasta Nasional	Bank BCA, Bank CIMB Niaga, Bank Danamon, dll.
	Bank Milik Pemerintah	Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI)
	Bank Campuran	Bank Capital Indonesia, dll.
	Bank Asing	HSBC, Bank of China, dll.
	Bank Syariah	Bank Muamalat, Bank Syariah Mandiri.
Bank Pengkreditan Rakyat (BPR)	BPR Konvensional	BPR Nusantara, BPR Dana Mandiri
	BPR Syariah	Bank Syariah Mitra Amanah
Bank Sentral	Bank Indonesia	Bank Indonesia

Sumber: (Rosyda, 2021)

1.2 Latar Belakang Penelitian

Teknologi digital dan pandemi COVID-19 telah mempercepat transformasi digital, sehingga membutuhkan penyesuaian dalam struktur layanan dan produk industri perbankan (Do et al., 2022). Menurut Belkhamza (2023) masalah keamanan siber telah muncul sebagai masalah global untuk operasi yang terkait dengan bisnis digital. Selama proses transformasi digital, perusahaan menjadi semakin rentan terhadap serangan siber dan pelanggaran keamanan (Saeed et al.,

2023). Kesulitan yang dialami bisnis dalam mempertahankan ketahanannya dalam menghadapi ancaman keamanan siber ini menggaris bawahi perlunya rencana atau strategi yang kuat untuk mengamankan informasi sensitif dan integritas operasi (Saeed et al., 2023)

Menurut laporan Mazumder & Hossain (2023) menunjukkan bahwa bahaya serangan siber di industri perbankan bisa mencapai 300 kali lipat lebih besar dibandingkan dengan industri lainnya. Otoritas Jasa Keuangan (OJK) menegaskan bahwa sektor keuangan, yang mencakup Inovasi Teknologi Sektor Keuangan (ITSK), tetap akan menjadi sasaran utama serangan siber. Sektor ini akan menghadapi kerentanannya yang signifikan apabila tidak mengimplementasikan kerangka keamanan dan ketahanan siber yang efisien serta responsif (OJK, 2024). Menurut laporan yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), sepanjang tahun 2024 jumlah total anomali trafik di Indonesia mencapai 330.527.636 kejadian. Aktivitas anomali tersebut berpotensi menyebabkan gangguan kinerja perangkat dan jaringan, kebocoran informasi sensitif, serta merusak reputasi dan menurunkan tingkat kepercayaan terhadap organisasi yang terdampak. Total serangan siber dan serangan malware yang terdeteksi pada sistem honeynet Badan Siber dan Sandi Negara (BSSN) mencapai 610,63 juta pada 2024 (Rizaty, 2025).

Indonesia berada dalam situasi yang sulit dalam hal keamanan siber jika dilihat dalam konteks global. Dilansir dari situs bnpp.go.id menurut perhitungan *realtime* dari Kaspersky, negara Indonesia ada di peringkat ke-10 sebagai target serangan siber, yang mengindikasikan bahwa lembaga keuangan harus meningkatkan kewaspadaan terhadap bahaya ini (BNPP, 2024). Menurut penelitian yang dilakukan oleh Faizal et al. (2023) dan Luthfah (2023) mengindikasikan bahwasannya serangan siber yang berpotensi membahayakan keamanan informasi pribadi nasabah merupakan salah satu dari sekian banyaknya risiko yang dihadapi industri perbankan di Indonesia dalam masa transisi menuju sistem digital.

Bank Syariah Indonesia (BSI) adalah salah satu target serangan siber yang terjadi di Indonesia pada bulan Mei 2023. Serangan ini melumpuhkan layanan keuangan termasuk ATM dan *mobile banking* selama berhari-hari. Dalam sebuah

pernyataan, kelompok peretas yang dikenal sebagai *Lockbit Ransomware* mengaku bertanggung jawab atas pelanggaran tersebut, menyatakan bahwa mereka telah mencuri 1,5 *terabyte* data pribadi milik nasabah (Pratama, 2023). Menurut Darem et al. (2023) serangan ini dapat menyebabkan berbagai akibat seperti kerugian finansial, kerusakan reputasi, dan konsekuensi hukum.

Setelah menggambarkan transformasi digital dan ancaman keamanan siber yang dihadapi sektor perbankan, penting untuk menyoroti peran utama karyawan sebagai garda terdepan dalam menjaga keamanan informasi di era digital ini. Penelitian terbaru menunjukkan bahwa manusia sebagai mata rantai terlemah, dan ada kebutuhan untuk memastikan kesadaran mereka akan bahaya yang terkait dengan keamanan siber untuk memperkuat pertahanan terhadap serangan (Saeed, 2023).

Transformasi digital membawa tantangan baru dalam keamanan informasi, di mana karyawan harus beradaptasi dengan teknologi baru dan ancaman yang muncul. Menurut Candiwan et al. (2022) perilaku yang tidak tepat dalam penggunaan teknologi, ditambah dengan tingkat kesadaran yang rendah, dapat menyebabkan tingginya risiko kejahatan siber. Di antara beberapa penelitian yang dilaksanakan oleh Krishnan et al. (2023) membahas perlunya meningkatkan kesadaran keamanan siber di kalangan pegawai bank di Malaysia. Terlepas dari kenyataan bahwa karyawan bank mungkin tidak memiliki pengetahuan khusus tentang teknologi informasi, penelitian ini menekankan bahwa mereka harus dididik tentang praktik-praktik keamanan siber yang mendasar. Praktik-praktik ini mencakup kemampuan untuk mengidentifikasi upaya *phishing* dan pemahaman tentang risiko yang terkait dengan praktik perbankan *online* yang tidak aman, seperti mengakses situs web yang tidak memiliki sertifikat SSL (Krishnan et al., 2023). Akibat ketidaktahuan pengguna, terdapat beberapa kasus masalah keamanan informasi dan privasi, termasuk *spam, spoofing,* insiden jaringan, *malware,* penyebaran informasi pribadi seperti alamat, nomor telepon, atau gambar, atau tidak memiliki perangkat lunak antivirus (Akraman et al., 2018).

Menurut laporan dari *Ponemon Institute*, sekitar 60% pelanggaran data disebabkan oleh kesalahan manusia. Ini termasuk tindakan seperti mengklik tautan

phishing atau menggunakan kata sandi yang lemah. Penelitian menunjukkan bahwa risiko akses yang tidak sah dapat dikurangi dengan menggunakan pengelola kata sandi dan menerapkan peraturan kata sandi yang kuat (Sari et al., 2023). Hal ini menunjukkan bahwa penting untuk seorang karyawan menerapkan *password management* yang baik. Berangkat dari kasus *phising* yang melibatkan email pengguna didalamnya, studi yang dilakukan oleh Saeed (2023) menekankan perlunya mengembangkan budaya kewaspadaan di antara karyawan tentang komunikasi email untuk mencegah pelanggaran keamanan. Mengingat seringnya upaya *phishing* yang menargetkan karyawan melalui email, maka *email management* juga merupakan aspek yang sangat penting.

Dalam penelitian yang dilakukan oleh Saeed (2023) melaporkan bahwa pengelolaan infrastruktur menjadi elemen penting dalam membentuk perilaku keamanan informasi. Hal ini menegaskan bahwa *infrastructure management* memiliki peran krusial dalam menjaga keamanan data dan sistem. Selain itu, kebijakan organisasi juga berkontribusi dalam membentuk perilaku keamanan informasi karyawan. Menurut Williams et al. (2019) standar dan kebijakan keamanan informasi berfungsi sebagai kerangka kerja yang mendukung pengelolaan keamanan informasi organisasi secara efektif. Oleh karena itu, sangat penting bagi setiap karyawan untuk mematuhi standar keamanan informasi internasional dan kebijakan organisasi mereka guna melindungi aset organisasi (Williams et al., 2019).

Menurut Yaokumah et al. (2019) pendidikan, pelatihan, dan peningkatan kesadaran keamanan merupakan aspek krusial dalam mengelola perilaku keamanan karyawan di suatu organisasi. Dengan memberikan karyawan keterampilan dan pengetahuan yang dibutuhkan untuk melindungi data penting serta menghadapi ancaman yang terus berkembang, bank dapat memperkuat strategi pertahanan mereka sekaligus menjaga kepentingan nasabah secara proaktif (Krishnan et al., 2023).

Persepsi karyawan terhadap keamanan teknologi yang mereka gunakan memiliki pengaruh besar terhadap perilaku mereka terkait keamanan informasi. He et al. (2020) menyatakan bahwa ketika karyawan menyadari potensi ancaman

keamanan yang dapat menyebabkan kerugian serius, mereka cenderung lebih berkomitmen untuk mengambil langkah-langkah pengamanan dan mengikuti pelatihan keamanan siber yang relevan. Menurut Sari et al. (2025) sistem keamanan yang lebih canggih tidak hanya memerlukan peraturan keamanan yang harus dipatuhi, sistem ini juga memerlukan karyawan dengan keahlian yang tepat untuk membantu melindungi sistem.

Para peneliti telah mengembangkan beberapa cara untuk mengukur bagaimana orang bertindak dalam hal keamanan informasi. Egelman & Peer (2015) dan digunakan kembali dalam studi menciptakan salah satu metode yang relevan, yang kemudian digunakan kembali dalam studi oleh Riemenschneider et al. (2023) untuk mengembangkan konstruksi perilaku keamanan informasi berdasarkan tugas sehari-hari karyawan, seperti *device securement, password generation, proactive awareness,* dan *updating.*

Pemilihan enam variabel independen dalam penelitian ini didasarkan pada relevansi teoritis, kebutuhan praktis di sektor perbankan, serta temuan dari literatur yang secara konsisten menyoroti aspek-aspek kunci dalam membentuk perilaku keamanan informasi karyawan. Masing-masing variabel dipilih karena mewakili dimensi penting dari faktor individu, organisasi, dan persepsi risiko yang berdampak terhadap perilaku keamanan.

Tabel 1.2 Pemilihan Variabel Penelitian

No.	Variabel Independen	Alasan Pemilihan	Sumber Pendukung
1	*Password Management*	*Password* yang lemah merupakan salah satu penyebab utama pelanggaran keamanan. Perilaku ini sangat kritikal dalam aktivitas perbankan digital.	(Saeed, 2023; Sari et al., 2023)

2	*Infrastructure Security Managament*	Infrastruktur yang tidak dikelola dengan baik berisiko membuka celah bagi serangan. Perlu pemahaman teknis dan praktik proteksi sistem.	(Saeed, 2023)
3	*Email Management*	Email merupakan jalur utama terjadinya *phishing.* Kesalahan pengguna sering menjadi titik awal kebocoran data.	(Krishnan et al., 2023; Saeed, 2023)
4	*Organizational Security Policy*	Kebijakan yang jelas akan membentuk standar perilaku karyawan terhadap keamanan. Ini juga bagian dari budaya organisasi.	(Saeed, 2023; Williams et al., 2019)
5	*Organizational Support & Training*	Dukungan organisasi dan pelatihan terbukti meningkatkan kesadaran dan kapabilitas karyawan dalam menghadapi ancaman siber.	(Yaokumah et al., 2019)
6	*Perception of Security*	Persepsi terhadap risiko dan potensi kerugian memengaruhi tingkat kepatuhan dan kehati-hatian dalam bertindak.	(Saeed, 2023; Sari et al., 2025)

Mengingat pentingnya kontribusi karyawan dalam menjaga keamanan informasi, penelitian ini bertujuan untuk mengevaluasi bagaimana perilaku keamanan informasi karyawan bank di Indonesia dipengaruhi oleh berbagai faktor, seperti *password management*, *infrastructure security management, email management, organizational security policy, organizational support and training* dan *perception of security.* Berdasarkan latar belakang dan fenomena tersebut, penulis memutuskan untuk mengangkat penelitian dengan judul "Analisis Perilaku

Keamanan Informasi Karyawan Bank di Indonesia dalam Era Transformasi Digital"

1.3 Perumusan Masalah

Merujuk pada latar belakang yang telah di uraikan di atas, rumusah masalah dalam penelitian ini yaitu:

1. Apakah *Password Management* berpengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia?
2. Apakah *Infrastructure Security Management* berpengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia?
3. Apakah praktik *Email Management* yang tepat memiliki pengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia?
4. Apakah *Organizational Security Policy* memiliki pengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia?
5. Apakah *Organizational Support and Training* mampu mendorong perilaku keamanan informasi pada karyawan bank di Indonesia?
6. Apakah *Perception of Security* tentang keamanan perangkat mengarah pada perilaku keamanan informasi yang efektif pada karyawan bank di Indonesia?

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk menganalisis pengaruh praktik manajemen kata sandi yang efektif terhadap perilaku keamanan informasi di kalangan karyawan bank di Indonesia.
2. Untuk mengevaluasi bagaimana penerapan langkah-langkah yang tepat untuk melindungi infrastruktur yang efektif di sektor perbankan Indonesia dapat mempengaruhi perilaku keamanan informasi.
3. Untuk mengetahui bagaimana aktivitas manajemen email yang tepat oleh karyawan bank di Indonesia dapat berkontribusi terhadap perilaku keamanan informasi.

4. Untuk mengeksplorasi bagaimana kebijakan keamanan organisasi yang diterapkan di bank-bank Indonesia dapat mendorong perilaku keamanan informasi di kalangan karyawan.
5. Untuk mengetahui bagaimana dukungan dan pelatihan organisasi yang diberikan kepada karyawan bank di Indonesia dapat berkontribusi pada perilaku keamanan informasi.
6. Untuk menganalisis bagaimana persepsi karyawan bank di Indonesia terhadap keamanan informasi dapat mempengaruhi perilaku keamanan informasi di kalangan mereka.

1.5 Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini harapannya dapat akan menambah literatur di bidang keamanan informasi dengan memberikan bukti empiris tentang pengaruh faktor-faktor tertentu (*password management*, *infrastructure security management, email management, organizational security policy, organizational support and training* dan *perception of security)* terhadap perilaku keamanan informasi karyawan di sektor perbankan Indonesia.

2. Manfaat Praktis

Penelitian ini harapannya dapat memberikan wawasan bagi manajer keamanan informasi di bank untuk merancang kebijakan dan program pelatihan yang lebih efektif dalam meningkatkan perilaku keamanan informasi karyawan.

1.6 Sistematika Penulisan Tugas Akhir

1) **BAB I**

   Bab ini akan membahas: Gambaran Umum Objek Penelitian, Latar Belakang Penelitian, Perumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Sistematika Penulisan Tugas Akhir

2) **BAB II**

   Bab ini akan membahas teori disertai penelitian terdahulu, serta dilanjutkan dengan kerangka pemikiran dan hipotesis.

3) **BAB II**

Bab ini akan menjelaskan jenis penelitian, variabel yang digunakan, skala pengukuran, populasi dan sampel, serta metode pengumpulan analisis data

4) **BAB IV**

Hasil penelitian dan pembahasan disajikan dalam sub judul yang terpisah dan diuraikan berdasarkan rumusan masalah dan tujuan penelitian. Bab ini terdiri dari dua bagian: bagian pertama menunjukkan temuan-temuan penelitian dan bagian kedua menunjukkan pembahasan dari hasil temuan.

5) **BAB V**

Kesimpulan dan saran akan dibahas pada bab ini.