BAB I

PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Wom *Finance* merupakan Perusahaan yang bergerak di bidang pembiayaan sepeda motor khusus nya merek Honda. Wom *Finance* didirikan pada tahun 1982 dengan nama PT Jakarta Tokyo Leasing, namun pada tahun 2000 berganti nama menjadi PT Wahana Ottomitra Multiartha (WOM Finance, 2024). Dengan pengalaman lebih dari 40 tahun, WOM *Finance* telah menjadi salah satu pemain utama dalam industri pembiayaan, melayani berbagai segmen masyarakat dengan produk-produk keuangan yang inovatif dan fleksibel.

Sebagai perusahaan pembiayaan yang cukup besar, WOM *Finance* memiliki visi untuk Menjadi salah satu perusahaan pembiayaan terbaik di Indonesia dengan menerapkan tata kelola perusahaan yang baik. Misi perusahaan mencakup mengutamakan kepuasan konsumen dan mitra kerja lainnya, membangun infrastruktur berbasis IT untuk melaksanakan proses yang baik, pengembangan dan perluasan jaringan usaha terutama didaerah potensial, dan mengoptimalkan kinerja perusahaan. Komitmen ini tercermin dalam berbagai program dan layanan yang dirancang untuk memberikan kemudahan akses kepada masyarakat dalam memenuhi kebutuhan finansial mereka.

Berdasarkan *annual report* Wom *Finance* pada tahun 2023, Jumlah karyawan WOM *Finance* per 31 Desember 2023 sebanyak 2.335 karyawan dengan komposisi karyawan laki-laki sebanyak 1.592 dan Perempuan sebanyak 743, untuk jumlah karyawan di jawa barat itu sebanyak 700 karyawan (WOM Finance, 2023). Jumlah karyawan yang besar ini mencerminkan skala operasi perusahaan yang luas, dengan jaringan cabang di seluruh Indonesia. Dalam operasionalnya, WOM *Finance* sangat

mengandalkan teknologi informasi untuk mendukung proses bisnis, termasuk pengelolaan data pelanggan, sistem pembiayaan, dan transaksi keuangan.

Dengan menggunakan teknologi informasi, WOM *Finance* tentunya harus memiliki kesadaran yang tinggi terhadap segala serangan siber. Menurut laporan IBM (2023), sektor keuangan menempati peringkat kedua sebagai target utama kejahatan siber secara global setelah sektor kesehatan. Sebagai perusahaan yang bergerak di bidang pembiayaan, WOM *Finance* berada dalam posisi yang rentan terhadap ancaman tersebut. Tingginya ketergantungan pada teknologi informasi dalam pengelolaan data pelanggan, sistem pembiayaan, dan transaksi keuangan menjadikan ancaman siber seperti *ransomware* atau pencurian data sebagai risiko yang sangat berbahaya. Dengan begitu, penulis tertarik untuk meneliti WOM *Finance* sebagai objek penelitian.

1.2 Latar Belakang Penelitian

Perkembangan teknologi informasi saat ini telah membawa dampak yang sangat signifikan pada berbagai aspek kehidupan, termasuk dalam dunia bisnis. Organisasi semakin bergantung pada teknologi untuk mendukung operasional, penyimpanan data, dan komunikasi. Dengan meningkatnya penggunaan teknologi informasi (TI) untuk memperbaiki proses bisnis dan pengambilan keputusan, masalah keamanan informasi telah menjadi salah satu tantangan paling mendesak yang dihadapi organisasi diseluruh dunia (Chu & So, 2020). Dimana serangan siber telah meningkat secara dramatis dan penjahat siber telah menemukan cara baru untuk menyerang organisasi dan mencuri informasi sensitif (Saeed, 2023). Hal ini berdampak pada keberlanjutan sistem informasi serta kelangsungan bisnis organisasi secara keseluruhan (Chu & So, 2020).

Menurut Badan Siber dan Sandi Negara (BSSN), selama tahun 2023, terdapat sebanyak 1.417 aduan terkait insiden siber yang diterima dari berbagai sektor salah satu nya di sektor organisasi yang menjalankan bisnis. Dari total tersebut, bulan Juli mencatat jumlah aduan tertinggi dengan 286 laporan. Secara keseluruhan, aduan mengenai kejahatan siber (*cybercrime*) mendominasi mencapai 86% dari total aduan

atau sebanyak 1.216 laporan (Direktorat Operasi Keamanan Siber, 2023). Pesatnya digitalisasi dan ketergantungan pada teknologi informasi ini menghadirkan tantangan besar dalam hal keamanan informasi. Perusahaan pembiayaan seperti WOM *Finance* berada di bawah ancaman serius dari serangan siber. Risiko seperti pencurian data, peretasan sistem, hingga penipuan digital dapat mengancam keamanan operasional dan kepercayaan pelanggan sehingga dapat merugikan bisnis.

Menurut laporan IBM (2023), sektor keuangan menempati peringkat kedua sebagai target utama kejahatan siber global setelah sektor kesehatan, dengan rata-rata kerugian per insiden mencapai $5,9 juta. Insiden seperti kebocoran data pelanggan (64%), gangguan proses bisnis utama (40%), dan serangan ransomware (63% dari total ancaman) dan itu selalu meningkat setiap tahun (Rasyad, 2024). Bahkan, pada tahun 2022, biaya rata-rata pelanggaran data di sektor keuangan mencapai $5,97 juta, lebih dari satu juta dolar lebih tinggi dibandingkan rata-rata global (Robb, 2024). Selain itu, kerugian ekstrem akibat insiden siber meningkat lebih dari empat kali lipat sejak tahun 2017 mencapai $2,5 miliar (Natalucci et al., 2024). Serangan siber yang berhasil tidak hanya berdampak secara finansial tetapi juga dapat mengikis kepercayaan terhadap lembaga keuangan, yang berpotensi menyebabkan hilangnya pelanggan serta menurunnya kredibilitas bisnis. Dana Moneter Internasional (IMF) bahkan memperingatkan bahwa serangan siber berskala besar dapat merusak kepercayaan terhadap sistem keuangan secara keseluruhan (Feingold & Wood, 2024). Selain itu, berbagai jenis serangan siber seperti ransomware dan *Distributed Denial-of-Service* (DDoS) dapat melumpuhkan layanan keuangan yang krusial, membuatnya tidak dapat diakses oleh pelanggan yang sah. Dalam skenario terburuk, insiden siber di sektor keuangan dapat memicu kepanikan di pasar, yang berpotensi menyebabkan aksi jual besar-besaran hingga pembobolan bank (Natalucci et al., 2024).

Di Indonesia, kasus-kasus serangan siber seperti serangan ransomware terhadap perusahaan pembiayaan pernah dialami oleh BFI *Finance*, hal ini menjadi bukti nyata betapa rentannya sektor keuangan terhadap ancaman siber (Fallahnda, 2023). Insiden

tersebut mengakibatkan terganggunya layanan bagi konsumen serta menghambat berbagai aktivitas operasional akibat matinya beberapa sistem utama untuk sementara waktu (Aprilia, 2023). Selain ancaman eksternal seperti ransomware, faktor internal juga berperan dalam meningkatkan risiko keamanan siber. Menurut (Chu & So, 2020), Karyawan sering kali menjadi titik terlemah dalam keamanan informasi dan merupakan sumber utama pelanggaran keamanan. Hal ini terjadi karena mereka dapat terlibat dalam perilaku tidak etis di tempat kerja yang membahayakan keamanan informasi organisasi, atau mereka dapat memberikan peluang bagi peretas untuk menyerang atau membobol sistem komputer organisasi mereka. Pada perusahaan WOM Finance pada tahun 2023 pernah terjadi indikasi kebocoran data, ini disebabkan oleh *awareness* dari individu yang kurang baik.

Menurut survei yang dilakukan oleh Kaspersky, kebocoran data akibat serangan siber dan kesalahan manusia menjadi tantangan utama dalam keamanan informasi. Data menunjukkan bahwa insiden kebocoran dari sistem internal perusahaan mencatat angka yang cukup signifikan, dimana 28% responden mengidentifikasi kelalaian karyawan terhadap infrastruktur teknologi informasi (TI) sebagai salah satu sumber utama masalah (Suryakusumah, 2023). Selain itu, sekitar 70% pemimpin perusahaan mengakui bahwa banyak karyawan masih kurang memahami pentingnya keamanan siber. Kurangnya pemahaman mengenai keamanan siber ini, meningkatkan risiko pelanggaran seperti kesalahan dalam mengakses tautan phishing, penggunaan kata sandi yang lemah, atau ketidakpatuhan terhadap kebijakan keamanan internal perusahaan (Mamduh, 2024).

Dalam literatur sistem informasi, perilaku karyawan dalam hal keamanan informasi juga telah mendapatkan perhatian yang cukup signifikan karena dampak negatifnya terhadap keamanan informasi organisasi. Secara umum, perilaku karyawan yang merugikan keamanan informasi dapat dikategorikan menjadi tiga kelompok besar berdasarkan kesengajaan dan motif mereka. Pertama, perilaku tidak disengaja yang timbul akibat kesalahan manusia, kecelakaan, atau pengawasan. Kedua, terdapat

ketidakpatuhan yang disengaja tetapi tidak berbahaya, di mana karyawan secara sadar melanggar standar atau kebijakan keamanan informasi tanpa memiliki niat untuk merugikan organisasi. Terakhir, perilaku yang paling merusak adalah penyalahgunaan komputer yang disengaja dan jahat, di mana karyawan dengan niat buruk berupaya merusak sistem atau mencuri informasi sensitif (Posey & Shoss, 2024).

Salah satu elemen krusial dalam manajemen keamanan informasi adalah *willingness to report* atau kesediaan karyawan untuk melaporkan insiden keamanan informasi. Konsep ini mengacu pada kesiapan individu untuk melaporkan pelanggaran, potensi ancaman, atau insiden keamanan yang mereka temui di tempat kerja. Pelaporan insiden memainkan peran penting dalam membantu organisasi mendeteksi dini potensi kerugian dan memitigasi risiko keamanan yang lebih besar (Dinh et al., 2020). Namun, *willingness to report* sering kali terhambat oleh rasa takut terhadap konsekuensi pelaporan, seperti stigma atau pembalasan. Penelitian menunjukkan bahwa ketakutan ini dapat mengurangi tingkat pelaporan yang diperlukan untuk memastikan keamanan sistem informasi (Wei et al., 2020). Selain itu, perilaku tidak etis dapat semakin menurunkan kesediaan karyawan untuk melaporkan insiden (Chu & So, 2020).

Dalam penelitian yang dilakukan oleh (Chu & So, 2020), perilaku tidak etis karyawan dalam keamanan informasi dapat dikategorikan ke dalam empat jenis utama. Pertama, *misbehavior in networks/applications*, yaitu aktivitas yang melanggar kebijakan organisasi, seperti mengakses aplikasi atau sistem jaringan yang tidak diizinkan. Kedua, *dangerous web use*, di mana karyawan menggunakan internet secara tidak aman, seperti mengunjungi situs berisiko yang dapat membuka celah bagi malware atau ancaman siber lainnya. Ketiga, *omissive security behavior*, yakni kelalaian dalam menjaga keamanan data, seperti menggunakan kata sandi lemah atau tidak memperbarui perangkat lunak penting. Keempat, *poor access control* yang melibatkan kegagalan mematuhi prosedur kontrol akses yang tepat. Dengan begitu, organisasi perlu menerapkan program atau hukuman yang efektif untuk mencegah

perilaku tidak etis dan mendorong kesediaan karyawan melaporkan insiden keamanan informasi.

Program kesadaran keamanan informasi *(Information Security Awareness Programs)* memainkan peran penting dalam meningkatkan *willingness to report* di organisasi. Program ini dirancang untuk meningkatkan pemahaman karyawan tentang pentingnya pelaporan insiden dan memberikan keterampilan untuk mengenali serta merespons ancaman keamanan. Chu & So, (2020) menunjukkan bahwa karyawan yang memiliki pemahaman yang baik tentang risiko keamanan lebih mungkin untuk melaporkan insiden yang mereka temui. Selain itu, kebijakan hukuman yang tegas *(Punishment Severity)* juga memengaruhi kesediaan karyawan untuk melaporkan. Hukuman yang berat memberikan sinyal pentingnya keamanan informasi, sehingga mendorong karyawan untuk menghindari pelanggaran dan melaporkan insiden secara proaktif (Chu & So, 2020). Namun, kebijakan ini perlu disertai dengan perlindungan terhadap pelapor untuk mencegah rasa takut terhadap stigma atau pembalasan, yang dapat menjadi penghalang untuk pelaporan insiden (Wei et al., 2020).

Penelitian yang dilakukan oleh (Chu & So, 2020) difokuskan pada organisasi di luar negeri dengan cakupan yang masih bersifat umum dalam konteks manajemen keamanan informasi. Sementara itu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan mengkaji lebih spesifik pada sektor pembiayaan di Indonesia, yaitu WOM Finance, serta menyoroti perilaku tidak etis karyawan dalam konteks nyata operasional perusahaan keuangan yang berlokasi di wilayah Jawa Barat. Pendekatan ini diharapkan dapat memberikan pemahaman yang lebih kontekstual terhadap tantangan keamanan informasi di lingkungan kerja lokal, yang sebelumnya belum banyak dieksplorasi dalam literatur.

Berdasarkan penjelasan latar belakang dan fenomena di atas, penulis akhirnya memutuskan untuk melakukan penelitian yang bertujuan untuk meneliti lebih dalam bagaimana perilaku tidak etis karyawan dalam keamanan informasi mempengaruhi

keamanan sistem pada perusahaan yang bergerak dalam kegiatan pembiayaan konsumen dengan tajuk **"Analisis *Information Security Awareness Programs and Punisment Severity* Terhadap Pelaporan Insiden Keamanan Informasi di WOM *Finance*"**

1.3 Perumusan Masalah

Dari latar belakang dan fenomena yang telah penulis paparkan pada bagian sebelumnya, penulis mengangkat tiga pertanyaan penelitian. Adapun tiga pertanyaan penelitian sebagai Berikut:

1. Bagaimana hubungan antara *Information Security Awareness Programs* dengan *Unethical Information Security Behavior* karyawan dalam *Misbehavior in Network/Applications, Dangerous Web Use, Omissive Security Behavior, Poor Access Control*?
2. Bagaimana hubungan *Punishment Severity* dengan *Unethical Information Security Behavior* karyawan dalam *Misbehavior in Network/Applications, Dangerous Web Use, Omissive Security Behavior, Poor Access Control*?
3. Bagaimana *Unethical Information Security Behavior* karyawan dalam *Misbehavior in Network/Applications, Dangerous Web Use, Omissive Security Behavior, Poor Access Control* dapat berpengaruh terhadap pelaporan insiden keamanan informasi?

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah diatas, maka tujuan penelitian sebagai berikut:

1. Menganalisis hubungan antara *Information Security Awareness Programs* dengan *Unethical Information Security Behavior* karyawan WOM *Finance* dalam *Misbehavior in Network/Applications, Dangerous Web Use, Omissive Security Behavior, Poor Access Control*.

2. Menganalisis hubungan *Punishment Severity* terhadap *Unethical Information Security Behavior* karyawan WOM *Finance* dalam *Misbehavior in Network/Applications, Dangerous Web Use, Omissive Security Behavior, Poor Access Control*.
3. Mengidentifikasi dampak *Unethical Information Security Behavior* karyawan WOM *Finance* dalam *Misbehavior in Network/Applications, Dangerous Web Use, Omissive Security Behavior, Poor Access Control* terhadap pelaporan insiden keamanan informasi.

1.5 Manfaat Penelitian

A. Manfaat Akademis

Penelitian ini diharapkan dapat memperluas pemahaman mengenai hubungan antara program kesadaran keamanan informasi, tingkat keparahan hukuman, dan perilaku buruk karyawan terkait keamanan informasi. Pengaruh tingkat keparahan hukuman terhadap perilaku buruk karyawan, serta untuk menambah wawasan mengenai dampak perilaku buruk karyawan terhadap pelaporan insiden keamanan informasi.

B. Manfaat Praktis

Memberikan wawasan bagi manajer dan pengambil keputusan dalam merancang program kesadaran keamanan informasi yang efektif untuk mengurangi perilaku buruk karyawan dalam penggunaan jaringan, aplikasi, web, serta kontrol akses. Serta diharapkan dapat memberikan informasi bagi organisasi mengenai pentingnya penegakan hukuman yang sesuai untuk mencegah pelanggaran keamanan informasi oleh karyawan.

1.6 Sistematika Penulisan Tugas Akhir

Sistematika penulisan digunakan untuk memudahkan dalam mengetahui pembahasan yang ada dalam penelitian ini, adapun penulisan sistematika penulisan sebagai berikut:

1) **BAB I PENDAHULUAN**

Bab ini membahas objek penelitian, latar belakang, rumusan masalah, tujuan dan manfaat penelitian.

2) **BAB II TINJAUAN PUSTAKA**

Bab ini berisi teori dari umum sampai ke khusus, disertai penelitian terdahulu dan dilanjutkan dengan kerangka pemikiran penelitian yang diakhiri dengan hipotesis jika diperlukan.

3) **BAB III METODE PENELITIAN**

Bab ini menjelaskan jenis penelitian, bagaimana variabel digunakan, skala pengukuran, populasi dan sampel, dan metode pengumpulan dan analisis data.

4) **BAB IV HASIL PENILITIAN DAN PEMBAHASAN**

Sesuai dengan rumusan masalah dan tujuan penelitian, bab ini menjelaskan hasil dan pembahasan penelitian.

5) **BAB V KESIMPULAN DAN SARAN**

Hasil dan rekomendasi penelitian dibahas dalam bab ini