Analisis *Information Security Awareness Programs and Punisment Severity* Terhadap Pelaporan Insiden Keamanan Informasi di WOM Finance

Zdikri Munawwar Ridha [1], Candiwan Candiwan[2],
[1] Manajemen Bisnis Telekomunikasi & Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia, zdikrimunawwar@student.telkomuniversity.ac.id
[2]Manajemen Bisnis Telekomunikasi & Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia, candiwan@telkomuniversity.ac.id

Abstrak
Ketergantungan organisasi pada teknologi informasi di era digital menjadikan keamanan informasi sebagai prioritas utama, terutama di sektor pembiayaan yang rentan terhadap serangan siber dan kelalaian internal karyawan. Penelitian sebelumnya berfokus pada konteks umum di luar negeri, sehingga penelitian ini mengisi kesenjangan dengan mengkaji secara spesifik faktor-faktor yang memengaruhi pelaporan insiden di industri pembiayaan Indonesia. Metode penelitian yang digunakan adalah kuantitatif dengan pendekatan survei terhadap 169 karyawan WOM Finance di Jawa Barat. Data dianalisis menggunakan Partial Least Squares Structural Equation Modeling. Hasil penelitian menunjukkan bahwa persepsi terhadap hukuman yang tegas secara signifikan mampu menurunkan seluruh bentuk perilaku tidak etis. Sebaliknya, program kesadaran keamanan informasi tidak berpengaruh signifikan terhadap lemahnya kontrol akses yang sejalan dengan teori deterrence. Ditemukan pula bahwa hanya kelalaian dalam menjaga keamanan yang berpengaruh signifikan terhadap kesediaan melaporkan insiden. Oleh karena itu, perusahaan disarankan untuk memperkuat kebijakan sanksi yang tegas dan konsisten untuk menekan pelanggaran. Selain itu, program edukasi perlu dievaluasi dan diperkuat dengan kontrol teknis, terutama pada aspek kebijakan kata sandi dan hak akses untuk membangun budaya keamanan yang lebih tangguh.

Kata kunci: Program Kesadaran Keamanan Informasi, Keparahan Hukuman, Kesediaan Melaporkan, Perilaku Tidak Etis, Partial Least Squares Structural Equation Modeling

I. PENDAHULUAN

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. Perusahaan pembiayaan seperti WOM Finance menghadapi ancaman serius dari serangan siber yang terus berkembang. Risiko seperti pencurian data, peretasan sistem, hingga penipuan digital dapat mengganggu keamanan operasional, merusak reputasi perusahaan, serta menurunkan tingkat kepercayaan pelanggan. Pada tahun 2023, WOM Finance mengalami indikasi kebocoran data yang diduga disebabkan oleh rendahnya tingkat kesadaran keamanan informasi dari individu di dalam organisasi. Insiden ini menjadi pengingat penting bahwa perlindungan data tidak hanya bergantung pada sistem teknologi, tetapi juga pada perilaku dan pemahaman setiap individu terhadap pentingnya menjaga keamanan informasi.

Dengan begitu, penelitian ini bertujuan untuk menguji hubungan antara program Kesadaran Keamanan Informasi dan perilaku keamanan karyawan yang tidak etis, termasuk penyalahgunaan jaringan atau aplikasi, penjelajahan web yang tidak aman, perilaku keamanan yang mengabaikan keamanan, manajemen email yang buruk, dan kontrol akses yang tidak memadai. Lebih lanjut, penelitian ini berusaha untuk menganalisis dampak dari tingkat keparahan hukuman terhadap perilaku tidak etis karyawan dalam hal keamanan dan menentukan apakah sanksi yang tegas secara efektif menghalangi tindakan tidak etis atau menciptakan keengganan dalam melaporkan insiden keamanan. Selain itu, penelitian ini juga menyelidiki bagaimana faktor-faktor tersebut secara kolektif mempengaruhi kesediaan karyawan untuk melaporkan ancaman keamanan di dalam organisasi. Dengan membahas tujuan-tujuan ini, penelitian ini memberikan wawasan berharga dalam merancang program kesadaran keamanan siber yang efektif dan kebijakan penegakan hukum yang meningkatkan kepatuhan keamanan, meminimalkan risiko, dan mempromosikan budaya keamanan yang proaktif di lembaga keuangan.

II. KAJIAN TEORI

A. Management Information System

Sistem Informasi Manajemen merupakan perpaduan antara Sumber Daya Manusia dan aplikasi teknologi informasi untuk memilih, menyimpan, mengolah dan mengambil kembali data dalam rangka mendukung proses pengambilan keputusan sebuah perusahaan (Rochaety, 2016). Sistem Informasi Manajemen mencakup berbagai bidang studi, termasuk sistem informasi dan sistem manajemen keamanan informasi (Candiwan et al., 2023).

Sistem Informasi Manajemen (SIM) dapat dianggap sebagai kumpulan subsistem yang didasarkan pada fungsi-fungsi organisasi. Setiap subsistem dirancang untuk mendukung proses informasi yang sesuai dengan fungsi spesifiknya (Rochaety, 2016). Komponen utama dari sistem informasi meliputi perangkat lunak, perangkat keras, data, manusia, jaringan, input, output, penyimpanan, serta kontrol (Candiwan et al., 2023). Dalam setiap subsistem fungsional, terdapat aplikasi yang mendukung berbagai proses, termasuk pemrosesan transaksi, pengendalian operasional, pengendalian manajemen, dan perencanaan strategis. Meskipun setiap subsistem memiliki fokus yang berbeda, semuanya terhubung melalui database, model dasar, dan sejumlah program komputer yang mendukung integrasi antarfungsi dalam organisasi (Rochaety, 2016).

B. Information Security Management

Informasi merupakan salah satu aset organisasi yang sangat berharga dan perlu dilindungi (Candiwan et al., 2016). Manajemen Keamanan Informasi (ISM) adalah pendekatan sistematis yang bertujuan untuk melindungi aspek-aspek kritis dalam informasi organisasi, seperti integritas, kerahasiaan, ketersediaan, autentikasi, keandalan, serta akuntabilitas informasi. Dengan berkembangnya teknologi informasi dan komunikasi, ISM menjadi semakin

penting untuk menjaga bisnis dari berbagai ancaman, termasuk malware, phishing, dan serangan siber lainnya. Dalam konteks organisasi modern, ISM tidak hanya melindungi informasi namun juga berperan penting dalam memastikan kontinuitas bisnis dan membangun kepercayaan pelanggan terhadap keamanan sistem informasi yang diterapkan oleh organisasi (Zammani et al., 2019).

ISM menyediakan arah strategis bagi organisasi untuk menerapkan proses dan aktivitas keamanan yang diperlukan guna memastikan terpenuhinya tujuan keamanan, manajemen risiko yang konsisten, dan penggunaan sumber daya informasi yang efektif. Di dalam ISM, terdapat elemen-elemen teknis dan non-teknis yang harus diperhatikan untuk memastikan lingkungan yang aman dalam melindungi informasi organisasi. Keberhasilan implementasi ISM dipengaruhi oleh faktor-faktor yang diklasifikasikan ke dalam empat aspek utama, yaitu Orang, Dokumen Organisasi, Proses, dan Teknologi (Zammani et al., 2021).

Manajemen keamanan informasi mencakup serangkaian kegiatan yang melibatkan pengelolaan sumber daya untuk memenuhi kebutuhan keamanan informasi suatu organisasi. Karena ISM adalah tanggung jawab kolektif dari semua karyawan di setiap tingkat organisasi, maka penilaian terhadap implementasi kegiatan ISM di tingkat strategis, taktis, dan operasional menjadi sangat penting (Singh & Gupta, 2019). Keberhasilan ISM juga menjadi salah satu faktor utama dalam membangun dan mempertahankan daya saing organisasi. Oleh karena itu, manajemen informasi organisasi harus selaras dengan aspek keamanan informasi untuk memastikan validitas dan akurasi informasi yang dikelola (Halim & Yusof, 2019).

C. Unethical Information Security Behavior

Perilaku keamanan informasi mencakup tindakan seperti menjaga perangkat tetap aman dan tidak mengirim informasi sensitif tanpa enkripsi merupakan perilaku yang diperlukan untuk melindungi aset informasi dengan aman (Sari et al., 2022). Spanaki et al., (2019) mengungkapkan bahwa perilaku tidak etis sering terjadi karena kurangnya pemahaman tentang pentingnya keamanan informasi. Norma sosial yang cenderung mengabaikan pelanggaran dapat mendorong individu untuk tidak mematuhi kebijakan keamanan yang berlaku. Sementara itu, (Lankton et al., 2019) menjelaskan bahwa bagaimana seseorang menilai dampak dari tindakannya, atau yang disebut intensitas moral, sangat memengaruhi keputusan mereka untuk bertindak secara etis, termasuk dalam menjaga keamanan informasi.

Menurut (Chu & So, 2020) dalam penelitiannya, perilaku keamanan informasi yang tidak etis merupakan tindakan sukarela yang dilakukan oleh karyawan, yang tercermin dalam ketidakpatuhan terhadap aturan, standar, kode, atau prinsip organisasi. Perilaku ini dapat memengaruhi aspek privasi, akurasi, hak kepemilikan, maupun aksesibilitas informasi di lingkungan kerja. (Chu & So, 2020) juga menyebutkan bahwa terdapat empat jenis utama perilaku tidak etis terkait keamanan informasi, yaitu: (1) Penyalahgunaan pada jaringan/aplikasi (*Misbehavior in Network/Applications*), (2) Penggunaan Web yang berisiko (*Dangerous Web Use*), (3) Perilaku keamanan yang lalai (*Omissive Security Behavior*), (4) Pengendalian akses yang buruk (*Poor Access Control*).

D. Misbehavior in Networks/Applications

Misbehavior in Networks/Applications mengacu pada tindakan yang dilakukan oleh karyawan dalam menggunakan jaringan dan aplikasi secara tidak sah atau tidak sesuai dengan kebijakan keamanan organisasi, yang berpotensi menimbulkan risiko keamanan informasi (Chu & So, 2020). Tindakan ini mengancam keamanan informasi organisasi karena memungkinkan pihak luar atau pihak yang tidak berwenang untuk mendapatkan akses ke data sensitif perusahaan. Dampak dari misbehavior ini dapat mencakup kebocoran informasi dan kerugian yang terkait dengan privasi, kepemilikan, dan aksesibilitas data perusahaan (Chu & Chau, 2014).

Menurut (Dang-Pham et al., 2017), salah satu motivasi karyawan melakukan misbehavior ini adalah untuk mendapatkan manfaat pribadi, seperti kemudahan akses atau penghematan waktu, yang seringkali mengesampingkan risiko keamanan yang ditimbulkan bagi organisasi. Hal ini menunjukkan bahwa karyawan mungkin tidak sepenuhnya menyadari atau menghargai potensi dampak negatif dari tindakan tersebut terhadap keselamatan data perusahaan.

E. Dangerous Web Use

Dangerous Web Use mengacu pada penggunaan internet yang tidak aman oleh karyawan, seperti mengunjungi situs web mencurigakan yang dapat menjadi sumber malware dan penipuan. Chu & So, (2020) menjelaskan bahwa aktivitas ini termasuk ke dalam perilaku tidak etis dalam keamanan informasi di tempat kerja. Dalam penelitiannya mereka mengungkapkan bahwa meskipun penggunaan internet pribadi oleh karyawan dapat bermanfaat jika diawasi dengan baik, penggunaan yang tidak hati-hati berisiko membahayakan informasi organisasi. Hal ini dapat menyebabkan kebocoran informasi atau peretasan sistem komputer perusahaan, yang pada akhirnya mengancam properti dan aksesibilitas data perusahaan.

Selain itu, aktivitas seperti mengunduh file dari situs web mencurigakan dan menyebarkan tautan berbahaya di lingkungan kerja adalah salah satu contoh dari *Dangerous Web Use*. Menurut (Asker & Tamtam, 2023), perilaku ini bisa terjadi karena karyawan berusaha memperoleh keuntungan pribadi, misalnya hiburan, tetapi tanpa memperhatikan keamanan informasi organisasi. Pada penelitian yang dilakukan oleh (Gmel et al., 2019) mengungkapkan bahwa penggunaan internet yang tidak terkontrol dapat memperlihatkan pola adiktif, di mana pengguna lebih cenderung terlibat dalam aktivitas berisiko tinggi tanpa menyadari konsekuensinya.

F. Omissive Security Behavior

Omissive Security Behavior adalah perilaku di mana karyawan yang memiliki pengetahuan tentang langkah-langkah keamanan informasi justru gagal untuk menerapkannya. Cox, (2012) menjelaskan bahwa perilaku ini dapat muncul karena adanya knowing–doing gap, yaitu kesenjangan antara pemahaman dan tindakan yang diambil oleh pengguna dalam menjaga keamanan informasi. Meskipun karyawan mengetahui kebijakan dan prosedur keamanan yang ada, mereka sering kali tidak menerapkannya karena alasan kenyamanan, ketidakpedulian, atau kelalaian.

Dalam penelitian lain yang dilakukan oleh (Workman et al., 2008) menekankan bahwa *Omissive Security Behavior* melibatkan tindakan seperti tidak mengunci komputer saat ditinggalkan, meninggalkan perangkat penyimpanan data di tempat yang tidak aman, dan tidak mencadangkan data secara teratur. Perilaku ini tidak selalu dilakukan dengan maksud jahat, namun tetap berisiko karena dapat mengancam integritas, kerahasiaan, dan ketersediaan informasi yang vital bagi organisasi.

Chu & So, (2020) juga menjelaskan bahwa perilaku yang lalai dapat berdampak serius pada keamanan informasi dan keberlanjutan sistem informasi di suatu organisasi. Mereka menyoroti bahwa meskipun perilaku ini mungkin tidak memiliki niat jahat, tindakan seperti membiarkan informasi sensitif tanpa pengawasan dapat membuka peluang bagi kebocoran data dan ancaman lainnya.

G. *Poor Access Control*

Berdasarkan buku ISO/IEC 27001:2022 *Access Control* adalah aturan untuk mengontrol akses fisik dan logis ke informasi serta aset lainnya harus dirancang dan diterapkan sesuai dengan kebutuhan bisnis dan keamanan informasi (ISO/IEC 27001, 2022). Menurut Kashmar et al., (2021) Kontrol akses adalah proses membatasi akses ke suatu tempat atau sumber daya berdasarkan kebijakan keamanan yang telah ditetapkan. Kontrol akses sangat terkait dengan kerentanan keamanan informasi dan privasi informasi. Pendekatan kontrol akses yang berhasil melindungi keamanan informasi dan mencegah akses tidak sah ke data Perusahaan (Chu & So, 2020). Namun, Kontrol akses yang buruk (*Poor Access Control*) dapat melanggar aturan perusahaan tentang keamanan data.

Kontrol akses yang buruk tidak hanya melibatkan kontrol keamanan data yang tidak memadai, seperti akses tidak sah, tetapi juga langkah-langkah perlindungan data yang lemah seperti praktik kata sandi yang buruk. Kedua jenis perilaku tersebut dapat mengakibatkan kebocoran informasi. Kontrol akses yang buruk merupakan bentuk perilaku tidak etis dalam keamanan informasi yang dapat mengakibatkan pengguna yang tidak berwenang memperoleh akses yang tidak semestinya terhadap informasi perusahaan (Chu & So, 2020).

H. *Information Security Awareness Programs*

Information Security Awareness Programs merupakan inisiatif yang bertujuan meningkatkan kesadaran dan kewaspadaan individu terhadap risiko keamanan informasi di tempat kerja (Aldawood & Skinner, 2019)). Program ini tidak hanya memberikan keterampilan teknis, tetapi juga menumbuhkan rasa tanggung jawab karyawan dalam melindungi aset informasi (Chu & So, 2020).

Zheng et al., (2023) menunjukkan bahwa peningkatan Information Security Awareness (ISA) melalui program ini mampu mengurangi penyalahgunaan sistem informasi dan insiden keamanan. (Alkhazi et al., 2022) menambahkan bahwa program yang komprehensif dapat mengubah sikap dan perilaku karyawan serta membentuk budaya organisasi yang peduli terhadap keamanan data. Sementara itu, (Djotaroeno & Beulen, 2024) menekankan pentingnya pendekatan individual dan integrasi aspek teknis dengan pendekatan kognitif dan perilaku agar program lebih efektif dalam mengubah pola pikir dan tindakan karyawan.

I. *Punishment Severity*

Punishment Severity merujuk pada tingkat keparahan hukuman yang dapat memengaruhi tingkat kepatuhan karyawan terhadap kebijakan keamanan informasi. Hukuman yang berat terbukti mampu mengurangi niat dan perilaku penyalahgunaan sistem informasi (Kuo et al., 2021; Park et al., 2023). Chu & So, (2020) juga menegaskan bahwa keparahan hukuman berdampak langsung terhadap pengendalian perilaku tidak etis terkait keamanan informasi. (Zhu et al., 2022) menunjukkan bahwa semakin besar konsekuensi negatif yang dirasakan, semakin

kecil kemungkinan individu terlibat dalam pelanggaran. (Trang & Brendel, 2019) menambahkan bahwa hukuman formal, terutama yang berat, efektif dalam meningkatkan kepatuhan, sementara sanksi informal seperti penurunan reputasi memiliki dampak lebih lemah.

Dari perspektif deterrence theory, tiga faktor utama (*sanction severity, sanction certainty, dan sanction celerity*) harus dikombinasikan untuk efektivitas maksimum (Trang & Brendel, 2019; Bansal et al., 2021; Park et al., 2023). Kepastian dan kecepatan penerapan hukuman memperkuat efek pencegahan dari hukuman yang berat. Selain itu, (Khan & AlShare, 2019) menekankan pentingnya tekanan sosial dan tanggapan dari rekan kerja. Jika hukuman memengaruhi harga diri dalam kelompok, kepatuhan cenderung meningkat. Dalam kasus di mana peringatan tidak efektif, hukuman moneter dapat menjadi solusi, meskipun komitmen moral tetap perlu diperhatikan sebelum menerapkan sanksi formal.

J. *Willingness to Report*

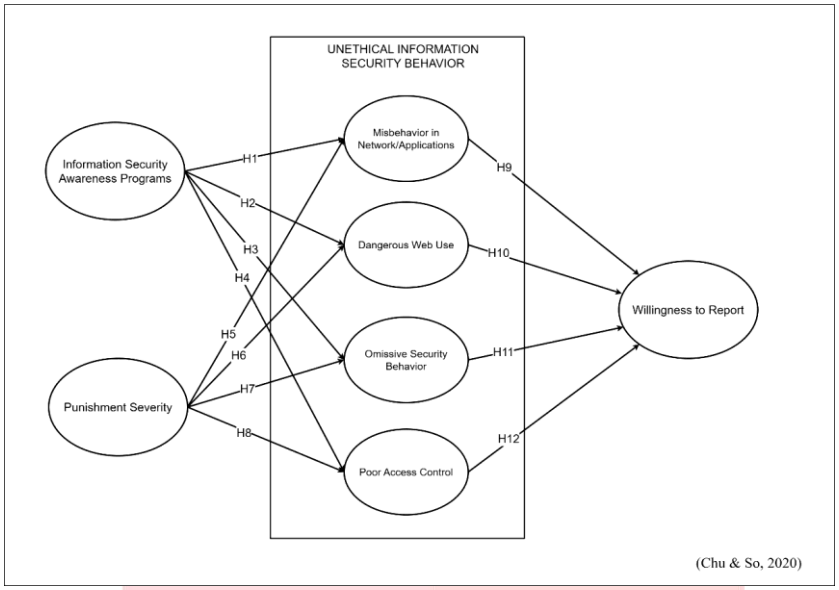
Willingness to Report adalah aspek penting dalam menjaga keamanan informasi di organisasi, khususnya dalam konteks pelaporan insiden keamanan. Konsep ini mencakup kesiapan karyawan atau anggota organisasi untuk melaporkan insiden atau perilaku yang dianggap membahayakan keamanan informasi (Chu & So, 2020). Dalam penelitian yang dilakukan oleh (Dinh et al., 2020), ditemukan bahwa keadilan organisasi dan komitmen afektif dapat menjadi pendorong utama bagi karyawan untuk melaporkan perilaku tidak etis di sektor publik. Penelitian ini menggarisbawahi pentingnya lingkungan kerja yang adil dan dukungan emosional dalam mendorong *Willingness to Report*.

Wang et al., (2023) juga menyebutkan bahwa privasi menjadi salah satu hambatan utama dalam *Willingness to Report*. Faktor lain yang turut memengaruhi *Willingness to Report* adalah kesadaran akan konsekuensi hukum dan manfaat pelaporan bagi keselamatan bersama. Penelitian oleh (Wei et al., 2020) menemukan bahwa pemahaman akan konsekuensi hukum dan manfaat pelaporan dapat meningkatkan keinginan untuk melaporkan insiden yang relevan. Di sisi lain, stigma dan ketakutan akan dampak negatif dapat menurunkan *Willingness to Report*.

Ballreich et al., (2023) juga menyatakan bahwa pelaporan insiden keamanan informasi adalah elemen krusial dalam meningkatkan respons organisasi terhadap insiden keamanan. Mereka mencatat bahwa karyawan adalah pihak pertama yang sering menyadari adanya insiden, sehingga penting bagi organisasi untuk menghapus hambatan pelaporan. Salah satu hambatan utama yang disebutkan adalah ketakutan akan sanksi, terutama jika insiden tersebut terjadi akibat kesalahan karyawan sendiri. Artikel ini merekomendasikan bahwa pengurangan atau penghapusan sanksi atas kesalahan ringan dapat meningkatkan *Willingness to Report*.

K. Kerangka Pemikiran

Kerangka pemikiran dalam penelitian ini diadaptasi dari penelitian Chu & So, (2020) yang berjudul "Organizational Information Security Management for Sustainable Information Systems: An Unethical Employee Information Security Behavior Perspective". Dalam penelitiannya terdapat dua faktor utama yaitu Information Security Awareness Programs dan Punishment Severity (Tingkat keparahan hukuman) yang diasumsikan memiliki pengaruh terhadap perilaku keamanan informasi karyawan yang tidak etis dan kesediaan untuk melaporkan insiden terkait keamanan informasi di organisasi. Menurut Chu & So, (2020) *Unethical Information Security Behavior* dikelompokkan ke dalam empat jenis yaitu *misbehavior in networks/applications, Dangerous Web Use, Omissive Security Behavior, dan Poor Access Control*.



Gambar 1 Kerangka Penelitian (*Chu & So, 2020)*

Berdasarkan kerangka penelitian diatas, hipotesis yang penulis diajukan adalah sebagai berikut:
H1: *Information Security Awareness Programs* memiliki pengaruh negatif terhadap *Misbehavior in Network/Applications*.
H2: *Information Security Awareness Programs* memiliki pengaruh negatif terhadap *Dangerous Web Use*.
H3: *Information Security Awareness Programs* memiliki pengaruh negatif terhadap *Omissive Security Behavior*.
H4: *Information Security Awareness Programs* memiliki pengaruh negatif terhadap *Poor Access Control*.
H5: *Punishment Severity* memiliki pengaruh negatif terhadap *Misbehavior in Network/Applications*.
H6: *Punishment Severity* memiliki pengaruh negatif terhadap *Dangerous Web Use*.
H7: *Punishment Severity* memiliki pengaruh negatif terhadap *Omissive Security Behavior*.
H8: *Punishment Severity* memiliki pengaruh negatif terhadap *Poor Access Control*.
H9: *Misbehavior in Network/Applications* memiliki pengaruh negatif terhadap *Willingness to Report* keamanan informasi.
H10: *Dangerous Web Use* memiliki pengaruh negatif terhadap *Willingness to Report* keamanan informasi.
H11: *Omissive Security Behavior* memiliki pengaruh negatif terhadap *Willingness to Report* keamanan informasi.
H12: *Poor Access Control* memiliki pengaruh negatif terhadap *Willingness to Report* keamanan informasi.

III. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kuantitatif dengan pendekatan deskriptif yang bertujuan untuk mengumpulkan data numerik secara objektif dan sistematis guna menggambarkan serta menganalisis hubungan antara *Information Security Awareness Programs* dan *Punishment Severity* terhadap pelaporan insiden keamanan informasi, dengan *Unethical Information Security Behavior* yang mencakup *Misbehavior in Network/Applications, Dangerous Web Use, Omissive Security Behavior, Poor Access Control, dan Misbehavior Email Use* sebagai variabel mediasi. Strategi yang digunakan adalah survei melalui kuesioner yang disebarkan kepada responden, mencerminkan pendekatan *noncontrived*, yaitu data dikumpulkan dalam kondisi alami tanpa manipulasi atau intervensi peneliti, dan responden mengisi kuesioner secara mandiri. Teknik pengumpulan data dilakukan secara *cross-sectional*, yakni dalam satu titik waktu tertentu, dengan tujuan memperoleh gambaran yang representatif terhadap fenomena yang sedang diteliti (Sekaran & Bougie, 2016)

Dalam penelitian ini, digunakan skala ordinal untuk mengukur variabel seperti *Information Security Awareness Programs, Punishment Severity*, serta *Unethical Information Security Behavior*. Skala ordinal memungkinkan pengurutan kategori berdasarkan tingkat kepentingan, kesetujuan, atau persepsi responden (Sekaran & Bougie, 2016). Instrumen pengukuran yang dipakai adalah skala Likert, yang dirancang untuk menilai tingkat persetujuan terhadap suatu pernyataan dengan interval yang sama, menggunakan 7 poin skala (Paramita et al., 2021). Pendekatan ini memberikan pemahaman yang lebih terstruktur mengenai pandangan responden terhadap variabel-variabel yang diteliti.

Dalam penelitian ini, populasi yang menjadi objek kajian adalah seluruh karyawan WOM Finance yang berada di wilayah Jawa Barat. Sampel merupakan bagian dari populasi yang dipilih untuk mewakili keseluruhan, dan harus mampu memberikan informasi valid agar hasilnya dapat digeneralisasikan (Sekaran & Bougie, 2016). Penelitian ini menggunakan pendekatan *Partial Least Squares Structural Equation Modeling* (PLS-SEM), dengan penentuan ukuran sampel minimum berdasarkan *Inverse Square Root Method* sebagaimana direkomendasikan oleh (Hair et al., 2022). Metode ini dipilih karena dinilai konservatif dan akurat, mempertimbangkan tingkat signifikansi 5% dan kekuatan statistik sebesar 80%. Dengan koefisien jalur minimum yang diharapkan sebesar 0.2, perhitungan menghasilkan jumlah minimum sampel sebesar 155 responden. Oleh karena itu, penelitian ini menargetkan minimal 155 karyawan WOM Finance di wilayah Jawa Barat sebagai responden. Pada penelitian ini menggunakan 169 responden sehingga rate responden pada penelitian ini 169/155.

Uji validitas dalam penelitian ini dilakukan dalam dua tahap: validitas isi dan validitas konstruk. Validitas isi dinilai melalui penilaian ahli *(expert judgement)* yang melibatkan dua orang ahli dan satu orang awam untuk memastikan bahwa butir-butir pertanyaan dalam kuesioner telah jelas, relevan, dan mencakup seluruh aspek penting dari faktor-faktor yang diteliti. Validitas konstruk dievaluasi melalui validitas konvergen dan diskriminan untuk memastikan bahwa setiap konstruk mengukur konsep yang berbeda. Pengujian reliabilitas menggunakan PLS-SEM meliputi *Cronbach's Alpha* dan *Composite Reliability*, yang keduanya harus melebihi ambang batas 0,7, dan *Average Variance Extracted* (AVE) harus di atas 0,5-mengkonfirmasikan bahwa model pengukuran tersebut dapat diandalkan dan valid.

Untuk analisis data, penelitian ini menggunakan PLS-SEM karena keefektifannya dalam menganalisis hubungan yang kompleks di antara variabel laten dengan banyak indikator. Perangkat lunak SmartPLS 4 digunakan untuk pemrosesan data yang efisien dan akurat. Proses evaluasi meliputi dua tahap utama: Outer Model, yang menguji validitas dan reliabilitas, dan Inner Model, yang menganalisis hubungan antar variabel laten. Hipotesis diuji dalam Inner Model dengan menggunakan analisis bootstrapping. Suatu hubungan dianggap signifikan secara statistik jika t-statistik melebihi 1,65 dan nilai p-value di bawah 0,05.

IV. HASIL DAN PEMBAHASAN

A. Karakteristik Responden

Dalam penelitian ini, 169 karyawan berkontribusi dalam menganalisis pelaporan insiden keamanan siber di WOM Finance, seperti yang tercantum dalam Tabel 1. Mayoritas responden adalah laki-laki (67,5%, n = 114), berasal dari Generasi Z (56,8%, n = 96), dan memiliki gelar sarjana (59,8%, n = 101). Dalam hal pengalaman kerja, sebagian besar partisipan memiliki pengalaman kurang dari satu tahun (39,6%, n = 67). Demografi ini menunjukkan bahwa penelitian ini terutama melibatkan individu-individu muda dan berpendidikan.

Tabel 1. Karakteristik Responden

Kategori	Subkategori	Persentase (%)	n (Jumlah Responden)
Jenis Kelamin	Laki-laki	67,5%	114
	Perempuan	32,5%	55
Generasi	Generasi Z	56,8%	96
	Milenial	34,9%	59
	Generasi X	5,3%	9
	Baby Boomers	3%	5
Tingkat Pendidikan	SMA	30,2%	51
	Diploma 3 (D3)	3%	5
	Diploma 4 (D4)	3,6%	6
	Sarjana (S1)	59,8%	101
	Magister (S2)	3,6%	6
Lama Bekerja	< 1 Tahun	39,6%	67
	1 – 3 Tahun	30,2%	51
	4 – 6 Tahun	15,4%	26
	> 6 Tahun	14,8%	25

Sumber: Data Olahan Penliti (2025)

B. Deskriptif Analisis

Statistik deskriptif adalah proses mengolah data untuk menggambarkan atau mendeskripsikan sampel populasi yang telah dikumpulkan guna menyusun kesimpulan (Darwin et al., 2021). Data yang dikumpulkan pada penelitian ini berdasarkan jawaban dari responden terkait pernyataan yang diajukan pada kuisioner. Respon atau jawaban dari responden tersebut akan dilakukan analisis dengan menggambarkan atau mendeskripsikan apa yang mempengaruhi pelaporan insiden di WOM Finance.

Penelitian ini mengacu pada kerangka pemikiran yang menyoroti perilaku keamanan informasi yang tidak etis *(Unethical Information Security Behavior)*, seperti perilaku menyimpang dalam penggunaan jaringan/aplikasi,

penggunaan web yang berbahaya, kelalaian dalam menjaga keamanan, penyalahgunaan email, dan kontrol akses yang buruk. Dua variabel utama yang menjadi fokus adalah *Information Security Awareness Programs* dan *Punishment Severity*, variabel utama tersebut dianggap memiliki hubungan dengan kecenderungan perilaku keamanan informasi. Analisis ini bertujuan untuk mengidentifikasi pengaruh faktor-faktor tersebut terhadap kemauan responden untuk melaporkan insiden *(Willingness to Report).* Hasil dari analisis deskriptif dapat dilihat pada table 2.

Tabel 2. Deskriptif Analisis

No	Variabel	Total Skor	Skor Ideal	Persentase	Klasifikasi	Item Tertinggi (Skor)
1	Misbehaviour in Network or Application	4336	4732	92%	Sangat Tinggi	MNA2 (92%)
2	*Dangerous Web Use*	3266	3549	92%	Sangat Tinggi	DWU3 (93%)
3	Omissive Security Behaviour	3232	3549	91%	Sangat Tinggi	OSB2 (92%)
4	*Poor Access Control*	3196	3549	90%	Sangat Tinggi	PAC3 (29,84%)
5	*Information Security Awareness Programs*	1.866	2.366	78,87%	Tinggi	ISAP2 (80,47%)
6	*Punishment Severity*	2.930	3.549	82,56%	Sangat Tinggi	PUS1 (83,26%)
7	*Willingness to Report*	2.731	3.549	76,95%	Tinggi	WTR2 (79,12%)

Sumber: Data Olahan Penliti (2025)

Hasil analisis deskriptif terhadap seluruh variabel penelitian menunjukkan bahwa sebagian besar indikator yang berhubungan dengan perilaku tidak etis terhadap keamanan informasi, seperti *Misbehaviour in Network or Application, Dangerous Web Use, Omissive Security Behaviour, dan Poor Access Control*, semuanya berada dalam kategori "Sangat Tinggi" dengan rentang persentase antara 90% hingga 92%. Hal ini menunjukkan bahwa responden memiliki tingkat kepatuhan yang sangat tinggi dalam menghindari perilaku menyimpang terkait keamanan informasi. Jawaban mayoritas responden terkonsentrasi pada kategori "Tidak Pernah" (TP) dan "Hampir Tidak Pernah" (HTP), yang menunjukkan kepatuhan mereka terhadap kebijakan keamanan yang ada.

Sementara itu, variabel *Information Security Awareness Programs* mendapatkan klasifikasi "Tinggi", dengan persentase sebesar 77,26% dan 80,47% untuk masing-masing indikator. Temuan ini menunjukkan bahwa sebagian besar responden menyadari pentingnya program kesadaran keamanan informasi, serta merasakan manfaat dari inisiatif organisasi dalam meningkatkan pemahaman akan isu-isu keamanan. Selanjutnya, variabel *Punishment Severity* memperoleh klasifikasi "Sangat Tinggi", dengan skor di atas 82% untuk semua item. Ini mencerminkan pandangan responden bahwa keberadaan sanksi atau hukuman memiliki peran penting dalam menjaga disiplin dan meminimalisir pelanggaran keamanan informasi di organisasi.

Terakhir, variabel *Willingness to Report* berada dalam klasifikasi "Tinggi", dengan rata-rata skor sebesar 76,95%. Temuan ini mencerminkan adanya budaya pelaporan insiden keamanan yang cukup kuat, walaupun tetap perlu penguatan dalam aspek kenyamanan dan proteksi terhadap pelapor. Secara keseluruhan, hasil ini memberikan gambaran positif bahwa tingkat kesadaran dan kepatuhan terhadap keamanan informasi di lingkungan kerja sudah cukup baik, meskipun masih terdapat ruang untuk perbaikan, terutama dalam meningkatkan efektivitas program edukasi dan sistem pelaporan insiden keamanan.

C. Uji *Outer Model*

Model pengukuran atau *Outer Model* dalam *Partial Least Square* (PLS) adalah tahap analisis yang bertujuan untuk memastikan bahwa hubungan antara variabel laten dan indikatornya valid dan reliabel. Model ini bertujuan untuk mengevaluasi sejauh mana indikator dapat merefleksikan atau membentuk variabel laten yang diukur (Rahadi, 2023). Hasil Uji *outer model* dapat dilihat pada tabel 3.

Tabel 3. Hasil Uji Outer Model

Variabels	*Indicator*	*Loading Factor*	*Composite Factor*	*Cronbach's Alpha*	*AVE*
Securiy Awareness Program	ISAP1	0.959	0.964	0.926	0.931
	ISAP2	0.971			
Punishment Severity	PUS1	0.939	0.968	0.951	0.911
	PUS2	0.975			
	PUS3	0.948			
Misbehavior in Networks/Applications	MNA1	0.903	0.971	0.961	0.894
	MNA2	0.948			
	MNA3	0.970			
	MNA4	0.960			
Dangerous Web Use	DWU1	0.943	0.969	0.952	0.913
	DWU2	0.964			

	DWU3	0.959			
	OSB1	0.859	0.943	0.909	0.846
Omissive Security Behavior	OSB2	0.958			
	OSB3	0.939			
	PAC1	0.876	0.905	0.842	0.760
Poor Access Control	PAC2	0.892			
	PAC3	0.847			
	WTR1	0.809	0.933	0.891	0.823
Willingness to Report	WTR2	0.964			
	WTR3	0.941			

Sumber: Data Olahan Penliti (2025)

Berdasarkan hasil analisis, konstruk *Willingness to Report* terbukti valid dan reliabel dalam mengukur niat individu untuk melaporkan insiden keamanan. Seluruh indikator memiliki nilai *loading factor* di atas ambang minimum 0,70, seperti WTR1 (0,809), WTR2 (0,964), dan WTR3 (0,941), yang menunjukkan bahwa masing-masing indikator secara akurat merepresentasikan konstruk. Hal ini diperkuat oleh nilai *Composite Reliability* sebesar 0,823 dan *Cronbach's Alpha* sebesar 0,891, yang keduanya melampaui batas minimum 0,70, menunjukkan konsistensi internal yang baik. Selain itu, nilai AVE sebesar 0,931 menunjukkan validitas konvergen yang sangat baik, di mana lebih dari 82,3% varians indikator dijelaskan oleh konstruk tersebut.

Konstruk lain seperti *Information Security Awareness Programs, Punishment Severity, Misbehavior in Networks/Applications, Dangerous Web Use, Omissive Security Behavior,* dan *Poor Access Control* juga menunjukkan hasil uji outer model yang sangat memuaskan. Seluruh indikator memiliki nilai loading factor tinggi (mayoritas di atas 0,90), dengan nilai *Composite Reliability* dan *Cronbach's Alpha* yang konsisten berada di atas 0,90, menandakan reliabilitas yang sangat tinggi. Nilai AVE pada konstruk-konstruk tersebut berkisar antara 0,823 hingga 0,931, menunjukkan bahwa indikator yang digunakan mampu menjelaskan sebagian besar varians dari konstruk utamanya secara akurat dan relevan.

Selanjutnya, pengujian outer model akan dilakukan melalui discriminant validity, yang bertujuan untuk mengevaluasi sejauh mana suatu konstruk berbeda secara empiris dari konstruk lainnya. Pengujian ini akan dilakukan menggunakan metode *Cross Loading* dan *Fornell-Larcker Criterion Model*.

Tabel 4. Hasil Uji *Cross Loading*

	DWU	**ISAP**	**MNA**	**OSB**	**PAC**	**PUS**	**WTR**
DWU1	**0.943**	0.372	0.863	0.868	0.879	0.557	0.433
DWU2	**0.964**	0.439	0.871	0.874	0.858	0.544	0.403
DWU3	**0.959**	0.387	0.885	0.841	0.877	0.460	0.334
ISAP1	0.362	**0.959**	0.377	0.423	0.362	0.509	0.446
ISAP2	0.439	**0.971**	0.464	0.477	0.420	0.561	0.439
MNA1	0.816	0.358	**0.903**	0.782	0.795	0.476	0.347
MNA2	0.903	0.469	**0.948**	0.886	0.838	0.595	0.442
MNA3	0.892	0.420	**0.970**	0.864	0.862	0.565	0.408
MNA4	0.840	0.407	**0.960**	0.841	0.825	0.604	0.448
OSB1	0.754	0.375	0.726	**0.859**	0.757	0.449	0.317
OSB2	0.895	0.468	0.899	**0.958**	0.891	0.584	0.464
OSB3	0.832	0.441	0.826	**0.939**	0.827	0.591	0.445
PAC1	0.817	0.370	0.779	0.815	**0.876**	0.459	0.338
PAC2	0.781	0.352	0.738	0.809	**0.892**	0.435	0.396
PAC3	0.786	0.343	0.775	0.731	**0.847**	0.507	0.412
PUS1	0.508	0.520	0.551	0.530	0.490	**0.939**	0.645
PUS2	0.581	0.525	0.612	0.623	0.571	**0.975**	0.670
PUS3	0.473	0.553	0.538	0.542	0.471	**0.948**	0.691
WTR1	0.268	0.332	0.312	0.328	0.299	0.494	**0.809**

WTR2	0.473	0.477	0.484	0.497	0.483	0.717	**0.964**
WTR3	0.347	0.420	0.370	0.379	0.389	0.667	**0.941**

Sumber: Data Olahan Penliti (2025)

Merujuk pada hasil yang disajikan dalam Tabel 4, seluruh indikator menunjukkan bahwa nilai loading terhadap konstruk asalnya masing-masing lebih tinggi dibandingkan dengan korelasinya terhadap konstruk lain. Hal ini mengindikasikan bahwa setiap indikator mampu merepresentasikan konstruknya secara spesifik dan tidak terjadi tumpang tindih antar konstruk. Dengan demikian, model ini dinyatakan telah memenuhi kriteria validitas diskriminan melalui pengujian *cross loading*, yang menjadi salah satu indikator penting dalam memastikan kejelasan dan keakuratan pengukuran dalam model penelitian.

Tabel 5. Hasil Uji *Fornell-Larcker Criterion Model*

	DWU	**ISAP**	**MNA**	**OSB**	**PAC**	**PUS**	**WTR**
DWU	**0.956**						
ISAP	0.419	**0.965**					
MNA	0.913	0.439	**0.946**				
OSB	0.902	0.469	0.893	**0.920**			
PAC	0.912	0.407	0.878	0.900	**0.872**		
PUS	0.548	0.557	0.596	0.595	0.538	**0.954**	
WTR	0.412	0.458	0.438	0.451	0.440	0.700	**0.907**

Sumber: Data Olahan Penliti (2025)

Mengacu pada hasil yang ditampilkan dalam tabel 5, seluruh konstruk dalam penelitian ini menunjukkan bahwa nilai akar kuadrat dari AVE lebih besar dibandingkan dengan korelasi antar konstruk lainnya. Kondisi ini menandakan bahwa model telah memenuhi kriteria validitas diskriminan berdasarkan Fornell-Larcker Criterion, yang mengindikasikan bahwa setiap konstruk mampu merepresentasikan variabel yang diukur secara eksklusif, tanpa adanya percampuran dengan konstruk lainnya.

D. Uji *Inner Model*

Model struktural atau inner model merupakan model yang menganalisis hubungan antar variabel laten. Menurut (Hair et al., 2022), inner model menggambarkan bagaimana variabel-variabel laten saling berhubungan dengan menunjukkan konstruksi dan jalur hubungan di dalam model struktural. Dalam *inner model* penelitian ini mengevaluasi R Square, F Square, Q Square, dan Uji Hipotesis.

Tabel 6. Hasil Uji R Square

	R-square	**R-square adjusted**
Dangerous Web Use **(DWU)**	0.319	0.311
Misbehavior in Network/Applications **(MNA)**	0.372	0.364
Omissive Security Behavior **(OSB)**	0.381	0.374
Poor Access Control **(OSB)**	0.306	0.298
Willingness to Report **(W)**	0.217	0.198

Sumber: Data Olahan Penliti (2025)

Berdasarkan hasil pengolahan data pada Tabel 6 diketahui bahwa nilai R-Square dan Adjusted R-Square dari konstruk Willingness to Report (W) masing-masing sebesar 0,217 dan 0,198, yang menunjukkan bahwa sebesar 21,7% varians dari niat untuk melaporkan insiden keamanan informasi dapat dijelaskan oleh konstruk eksogen seperti Misbehavior in Networks/Applications, Omissive Security Behavior, dan Poor Access Control. Meskipun tergolong rendah, hasil ini tetap menunjukkan adanya pengaruh, meski terbatas, antar variabel dalam model.

Konstruk Misbehavior in Networks/Applications (M) dan Omissive Security Behavior (O) juga menunjukkan kontribusi yang relatif rendah, dengan nilai R-Square masing-masing sebesar 0,372 dan 0,381. Hal ini menunjukkan bahwa sekitar 37,2% dan 38,1% varians dari masing-masing konstruk tersebut dapat dijelaskan oleh variabel-variabel dalam model, meskipun nilainya belum mencapai kategori sedang menurut kriteria umum.

Konstruk lainnya seperti Poor Access Control (C) dan Dangerous Web Use (D) memiliki nilai R-Square yang lebih rendah, masing-masing sebesar 0,306 dan 0,319, dengan nilai Adjusted R-Square sebesar 0,298 dan 0,311. Nilai-nilai ini memperkuat bahwa daya prediksi model terhadap variabel-variabel tersebut belum optimal. Mengacu pada kriteria Hair et al. (2022), di mana nilai R-Square sebesar 0,25 dikategorikan sebagai lemah, 0,50 sedang, dan 0,75 kuat, maka secara keseluruhan model struktural dalam penelitian ini termasuk dalam kategori lemah dalam menjelaskan hubungan antar konstruk karena belum ada nilai R-Square yang mencapai kategori sedang maupun kuat.

Tabel 7. Hasil Uji F Square

	DWU	ISAP	MNA	OSB	PAC	PUS	WTR
DWU							0.006
ISAP	0.027		0.027	0.044	0.024		
MNA							0.007
OSB							0.012
PAC							0.007
PUS	0.212		0.285	0.261	0.202		
WTR							

Sumber: Data Olahan Penliti (2025)

Berdasarkan hasil analisis ukuran efek (f-square) yang ditampilkan pada Tabel 7, diketahui bahwa variabel *Information Security Awareness Programs* (ISAP) memiliki pengaruh yang relatif kecil terhadap keempat dimensi *Unethical Information Security Behavior*, yakni *Misbehavior in Network/Applications* ($f^2 = 0.027$), *Dangerous Web Use* ($f^2 = 0.027$), *Omissive Security Behavior* ($f^2 = 0.044$), dan *Poor Access Control* ($f^2 = 0.024$). Hal ini menunjukkan bahwa meskipun program kesadaran keamanan memberikan kontribusi dalam menekan perilaku tidak etis, namun dampaknya tidak terlalu kuat.

Sebaliknya, variabel *Punishment Severity* (PUS) menunjukkan ukuran efek yang lebih besar terhadap perilaku tidak etis, dengan kategori efek sedang pada *Dangerous Web Use* ($f^2 = 0.212$), *Misbehavior in Network/Applications* ($f^2 = 0.285$), *Omissive Security Behavior* ($f^2 = 0.261$), dan *Poor Access Control* ($f^2 = 0.202$). Hal ini mengindikasikan bahwa ancaman hukuman yang berat secara efektif dapat menekan kecenderungan karyawan untuk melakukan pelanggaran terhadap kebijakan keamanan informasi. Lebih lanjut, seluruh dimensi perilaku tidak etis (MNA, DWU, OSB, PAC) juga menunjukkan ukuran efek yang sangat kecil terhadap Willingness to Report, dengan nilai f^2 masing-masing di bawah 0.015.

Tabel 8. Hasil Uji Q Square

	Q^2predict
Dangerous Web Use (DWU)	0.282
Misbehavior in Network/Applications (MNA)	0.344
Omissive Security Behavior (OSB)	0.345
Poor Access Control (OSB)	0.265
Willingness to Report (W)	0.315

Sumber: Data Olahan Penliti (2025)

Berdasarkan Tabel 8, seluruh konstruk dalam model ini memiliki nilai Q^2 Predict yang lebih besar dari nol, yang mengindikasikan bahwa model jalur PLS memiliki kemampuan prediktif yang lebih baik dibandingkan dengan tolok ukur paling naif. Hal ini sesuai dengan pendapat (Hair et al., 2022) yang menyatakan bahwa nilai

Q^2 Predict > 0 menunjukkan adanya relevansi prediktif model. Konstruk *Omissive Security Behavior* menunjukkan nilai tertinggi sebesar 0,345, menandakan bahwa model mampu memprediksi variabel tersebut dengan baik. Dengan demikian, model ini dapat dikatakan efektif dalam menjelaskan faktor-faktor yang mendorong seseorang untuk melaporkan pelanggaran keamanan informasi.

Sementara itu, konstruk lain seperti *Misbehavior in Network/Applications* dan *Willingness to Report* memiliki nilai Q^2 Predict sebesar 0,344 dan 0,315 hasil ini menunjukkan bahwa model memiliki kemampuan prediksi terhadap konstruk lainnya. Nilai Q^2 Predict yang paling rendah terdapat pada konstruk *Poor Access Control* dan *Dangerous Web Use*, yaitu 0,265 dan 0,282. Meskipun nilai tersebut tergolong rendah, keduanya masih melampaui diatas 0 dan mendekati 1.

Tabel 9. Hasil Uji Hipotesis

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values	Result
DWU -> WTR	-0.204	-0.234	0.189	1.082	0.140	Ha10 Ditolak
ISAP -> DWU	0.164	0.16	0.099	**1.653**	**0.049**	**Ha2 Diterima**
ISAP -> MNA	0.156	0.154	0.086	**1.811**	**0.035**	**Ha1 Diterima**
ISAP -> OSB	0.199	0.198	0.101	**1.979**	**0.024**	**Ha3 Diterima**
ISAP -> PAC	0.156	0.154	0.098	1.585	0.057	Ha4 Ditolak
MNA -> WTR	0.205	0.204	0.166	1.238	0.108	Ha9 Ditolak
OSB -> WTR	0.264	0.269	0.159	**1.668**	**0.048**	**Ha11 Diterima**
PAC -> WTR	0.209	0.238	0.215	0.969	0.166	Ha12 Ditolak
PUS -> DWU	0.457	0.465	0.107	**4.250**	**0.00**	**Ha6 Diterima**
PUS -> MNA	0.509	0.514	0.095	**5.341**	**0.00**	**Ha5 Diterima**
PUS -> OSB	0.484	0.491	0.105	**4.623**	**0.00**	**Ha7 Diterima**
PUS -> PAC	0.451	0.461	0.108	**4.159**	**0.00**	**Ha8 Diterima**

Sumber: Data Olahan Penliti (2025)

Berdasarkan hasil pengujian hipotesis menggunakan pendekatan bootstrapping dalam metode PLS-SEM, *Information Security Awareness Programs* (ISAP) terbukti memiliki pengaruh signifikan terhadap tiga konstruk perilaku tidak aman, yaitu *Misbehavior in Networks/Applications* (t = 1,811; p = 0,035), *Dangerous Web Use* (t = 1,653; p = 0,049), dan *Omissive Security Behavior* (t = 1,979; p = 0,024). Namun, ISAP tidak berpengaruh signifikan terhadap *Poor Access Control* (t = 1,585; p = 0,057), yang mengindikasikan bahwa edukasi dan pelatihan yang diberikan belum cukup efektif untuk menekan praktik buruk dalam kontrol akses, kemungkinan karena lemahnya kebijakan pengawasan internal.

Sebaliknya, *Punishment Severity* (PUS) menunjukkan pengaruh yang lebih kuat dan konsisten terhadap seluruh konstruk perilaku tidak aman. Seluruh hubungan dinyatakan signifikan, yakni terhadap *Misbehavior in Networks/Applications* (t = 5,341; p = 0,000), Dangerous Web Use (t = 4,250; p = 0,000), *Omissive Security Behavior* (t = 4,623; p = 0,000), dan *Poor Access Control* (t = 4,159; p = 0,000). Hal ini menunjukkan bahwa persepsi terhadap hukuman berat secara signifikan menurunkan kecenderungan individu untuk melakukan pelanggaran terhadap keamanan informasi, menjadikan pendekatan sanksi sebagai strategi pencegahan yang lebih efektif dibandingkan sekadar sosialisasi.

Adapun pengaruh perilaku tidak aman terhadap *Willingness to Report* (WTR) menunjukkan bahwa hanya *Omissive Security Behavior* (t = 1,668; p = 0,048) yang berpengaruh signifikan. Sementara itu, *Misbehavior in Networks/Applications* (t = 1,238; p = 0,108), *Dangerous Web Use* (t = 1,082; p = 0,140), dan *Poor Access Control* (t = 0,969; p = 0,166) tidak memiliki pengaruh signifikan terhadap kemauan melapor. Temuan ini mengindikasikan bahwa individu yang tidak lalai dalam praktik keamanan cenderung lebih memiliki kesadaran dan rasa tanggung jawab untuk melaporkan insiden, sedangkan bentuk pelanggaran lainnya tidak cukup mendorong tindakan pelaporan.

E. Pembahasan Hasil Penelitian

Hasil pengujian terhadap *Information Security Awareness Programs* (ISAP) menunjukkan bahwa ISAP memiliki pengaruh signifikan terhadap tiga bentuk *Unethical Information Security Behavior*, yaitu *Misbehavior in Networks/Applications, Dangerous Web Use, dan Omissive Security Behavior*. Hal ini menandakan bahwa pelatihan dan edukasi keamanan yang dilakukan organisasi cukup efektif dalam menekan perilaku tidak etis dalam konteks keamanan informasi. Namun, pada konstruk *Poor Access Control* (PAC), ISAP tidak menunjukkan pengaruh yang signifikan, yang mengindikasikan bahwa program kesadaran belum mampu mendorong perubahan perilaku dalam aspek kontrol akses. Aspek ini kemungkinan lebih dipengaruhi oleh faktor kebijakan, struktur organisasi, dan sistem pengawasan yang diterapkan secara teknis dan administratif. Temuan ini berbeda dengan penelitian (Chu & So, 2020) yang menyatakan ISAP belum efektif dalam mencegah perilaku menyimpang, namun hasil penelitian ini justru menunjukkan sebaliknya, didukung oleh data persepsi tinggi dari karyawan (78,87%).

Sebaliknya, variabel *Punishment Severity* (PUS) menunjukkan pengaruh yang kuat dan signifikan terhadap seluruh bentuk *Unethical Information Security Behavior*, termasuk MNA, DWU, OSB, dan PAC. Temuan ini menguatkan teori Deterrence bahwa persepsi terhadap keparahan hukuman dapat menekan niat maupun tindakan pelanggaran keamanan informasi. PUS efektif dalam mencegah pelanggaran yang dilakukan secara sengaja untuk keuntungan pribadi, seperti mengakses situs mencurigakan atau memasang aplikasi ilegal, karena adanya ketakutan terhadap konsekuensi. Persepsi terhadap ancaman sanksi yang tinggi (82,56%) menunjukkan bahwa organisasi telah berhasil membangun sistem hukuman yang tegas dan disegani. Hasil ini juga didukung oleh literatur sebelumnya (Kuo et al., 2021; Park et al., 2023; Chu & So, 2020), yang menyimpulkan bahwa hukuman formal memainkan peran sentral dalam meningkatkan kepatuhan terhadap kebijakan keamanan informasi.

Sementara itu, pengujian terhadap hubungan antara *Unethical Information Security Behavior* dan *Willingness to Report* (WTR) menunjukkan bahwa hanya *Omissive Security Behavior* yang berpengaruh signifikan terhadap kemauan untuk melaporkan insiden keamanan. Hal ini menunjukkan bahwa individu yang sadar akan kelalaiannya cenderung lebih terdorong untuk melapor karena rasa tanggung jawab. Sementara itu, bentuk penyimpangan lain seperti MNA, DWU, dan PAC tidak menunjukkan hubungan signifikan terhadap WTR, kemungkinan karena faktor psikologis seperti rasa takut, stigma sosial, atau budaya organisasi yang belum mendukung pelaporan. Temuan ini sejalan dengan studi dari (Dinh et al., 2020) dan (Wang et al., 2023), yang menyoroti pentingnya keadilan organisasi, perlindungan terhadap pelapor, dan budaya pelaporan yang aman. Oleh karena itu, peningkatan *willingness to report* memerlukan pendekatan yang lebih holistik, tidak hanya fokus pada kontrol perilaku menyimpang, tetapi juga melalui penguatan etika, dukungan struktural, dan insentif bagi pelapor.

V. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, disarankan agar WOM Finance mengevaluasi ulang pelaksanaan *Information Security Awareness Programs* (ISAP) yang belum berpengaruh signifikan terhadap seluruh *bentuk Unethical Information Security Behavior*, khususnya *Poor Access Control* (PAC). Edukasi perlu dikembangkan menjadi pelatihan praktis yang kontekstual dan berbasis studi kasus, serta dilengkapi dengan kebijakan teknis seperti penguatan autentikasi, pembatasan akses berbasis peran, dan audit perilaku akses secara berkala. Mengingat penggunaan kata sandi yang lemah masih menjadi titik rawan, perusahaan juga perlu memperjelas penerapan sanksi terhadap pelanggaran kontrol akses agar lebih tegas dan efektif.

Hasil penelitian juga menunjukkan bahwa *Punishment Severity* (PUS) berpengaruh signifikan terhadap seluruh bentuk perilaku tidak etis. Oleh karena itu, WOM Finance disarankan untuk mempertahankan konsistensi penerapan sanksi dan memastikan bahwa kebijakan disiplin dikomunikasikan secara merata kepada semua karyawan. Sistem hukuman perlu diimbangi dengan pendekatan pembinaan agar tidak hanya menekan pelanggaran, tetapi juga membentuk kesadaran jangka panjang. Dalam aspek *Willingness to Report* (WTR), ditemukan bahwa hanya *Omissive Security Behavior* (OSB) yang berpengaruh signifikan, sehingga perusahaan perlu membangun budaya pelaporan yang suportif, menjamin anonimitas pelapor, dan memberikan umpan balik yang profesional.

Untuk penelitian selanjutnya, disarankan memperluas cakupan studi ke berbagai institusi dan wilayah guna meningkatkan generalisasi hasil dan memahami konteks budaya keamanan informasi secara lebih luas. Selain itu, metode penelitian dapat diperkuat dengan pendekatan triangulasi, menggabungkan data kualitatif (wawancara atau FGD) dan data perilaku aktual (seperti log sistem atau laporan insiden), guna meningkatkan validitas temuan dan memahami kesenjangan antara persepsi dan perilaku nyata karyawan dalam keamanan informasi.

REFERENSI

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. In *Future Internet* (Vol. 11, Issue 3). MDPI AG. https://doi.org/10.3390/fi11030073

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Aprilia, Z. (2023, May 30). *Ternyata Ini Penyebab BFI Finance Bisa Diserang Hacker*. CNBC INDONESIA. https://www.cnbcindonesia.com/market/20230530100511-17-441683/ternyata-ini-penyebab-bfi-finance-bisa-diserang-hacker

Asker, H., & Tamtam, A. (2023). Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya. *European Scientific Journal, ESJ*, *19*(15), 238. https://doi.org/10.19044/esj.2023.v19n15p238

Ballreich, F. L., Volkamer, M., Müllmann, D., Berens, B. M., Häußler, E. M., & Renaud, K. V. (2023). Encouraging Organisational Information Security Incident Reporting. *ACM International Conference Proceeding Series*, 224–236. https://doi.org/10.1145/3617072.3617098

Bansal, G., Muzatko, S., & Shin, S. Il. (2021). Information system security policy noncompliance: the role of situation-specific ethical orientation. *Information Technology and People*, *34*(1), 250–296. https://doi.org/10.1108/ITP-03-2019-0109

Candiwan, Pertiwi Sudirman, B., & Kencana Sari, P. (2023). *Differences in Information Security Behavior of Smartphone Users in Indonesia Using Pearson's Chi-square and Post Hoc Test*. *13*(2). https://doi.org/https://doi.org/10.18517/ijaseit.13.2.17975

Candiwan, Sari, P. K., & Nurshabrina, N. (2016). Assessment of Information Security Management on Indonesian Higher Education Institutions. *Lecture Notes in Electrical Engineering*, *362*. https://doi.org/https://doi.org/10.1007/978-3-319-24584-3_31

Chu, A. M. Y., & Chau, P. Y. K. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems*, *66*, 93–101. https://doi.org/10.1016/j.dss.2014.06.008

Chu, A. M. Y., & So, M. K. P. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability (Switzerland)*, *12*(8), 1–25. https://doi.org/10.3390/SU12083163

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Exploring behavioral information security networks in an organizational context: An empirical case study. *Journal of Information Security and Applications*, *34*, 46–62. https://doi.org/10.1016/j.jisa.2016.06.002

Darwin, M., Mamondol, M., Sormin, S., Nurhayati, Y., Tambunan, H., Sylvia, D., & Adnyana, M. (2021). *Metode penelitian pendekatan kuantitatif*. https://www.researchgate.net/publication/354059356

Dinh, H. P., Nguyen, P. V., Trinh, T. V. A., & Pham, T. H. (2020). Ethical behaviors and willingness to report misconduct in the public sector. *Management Science Letters*, *10*(13), 3081–3088. https://doi.org/10.5267/j.msl.2020.5.015

Direktorat Operasi Keamanan Siber. (2023). *Lanskap Keamanan Siber Indonesia 2023*.

Djotaroeno, M., & Beulen, E. (2024). Information Security Awareness in the Insurance Sector: Cognitive and Internal Factors and Combined Recommendations. *Information (Switzerland)*, *15*(8). https://doi.org/10.3390/info15080505

Fallahnda, B. (2023). *4 Kasus Peretasan di Indonesia 2023: Ada BFI Finance hingga BSI*. Tirto.Id. https://tirto.id/4-kasus-peretasan-di-indonesia-2023-ada-bfi-finance-hingga-bsi-gKFK

Feingold, S., & Wood, J. (2024, May 15). *Global financial stability at risk due to cyber threats, IMF warns. Here's what to know*.

Gmel, G., Khazaal, Y., Studer, J., Baggio, S., & Marmet, S. (2019). Development of a short form of the compulsive internet use scale in Switzerland. *International Journal of Methods in Psychiatric Research*, *28*(1). https://doi.org/10.1002/mpr.1765

Hair, J. F., Hult, T., Ringle, C., & Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) Third Edition*.

Halim, H., & Yusof, M. M. (2019). Framework for Digital Data Access Control from Internal Threat in the Public Sector. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 10, Issue 8). www.ijacsa.thesai.org

Kashmar, N., Adda, M., Atieh, M., & Ibrahim, H. (2021). A review of access control metamodels. *Procedia Computer Science*, *184*, 445–452. https://doi.org/10.1016/j.procs.2021.03.056

Khan, H. U., & AlShare, K. A. (2019). Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 4–23. https://doi.org/10.1080/10919392.2019.1552743

Kuo, K. M., Talley, P. C., & Lin, D. Y. M. (2021). Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables. *Inquiry (United States)*, *58*. https://doi.org/10.1177/00469580211029599

Lankton, N. K., Stivason, C., & Gurung, A. (2019). Information protection behaviors: morality and organizational criticality. *Information and Computer Security*, *27*(3), 468–488. https://doi.org/10.1108/ICS-07-2018-0092

Natalucci, F., Qureshi, M., & Suntheim, F. (2024, April 9). *Rising Cyber Threats Pose Serious Concerns for Financial Stability*. IMF. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Paramita, D., Rizal, M. M. N., Riza, C., Sulistyan, B., & Wijayanti, R. (2021). *METODE PENELITIAN KUANTITATIF*.

Park, E. H., Kim, J., & Wiles, L. (2023). The role of collectivism and moderating effect of IT proficiency on intention to disclose protected health information. *Information Technology and Management*, *24*(2), 177–193. https://doi.org/10.1007/s10799-022-00362-y

Rahadi, D. (2023). *Pengatar Partial Least Square Strctural Equation Model PLS-SEM*.

Rasyad, M. (2024). *Ancaman siber terhadap industri keuangan: hasil sementara untuk tahun 2023*. IdNSA - Indonesia Network Security Association. https://idnsa.id/article/ancaman-siber-terhadap-industri-keuangan-hasil-sementara-untuk-tahun-2023

Robb, B. (2024, January 22). *The Cost of Cybercrime in the Financial Sector*. https://www.blackfog.com/cybercrime-in-the-financial-sector-follow-the-money/

Rochaety, E. (2016). *SISTEM INFORMASI MANAJEMEN*. www.mitrawacanamedia.com

Saeed, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability (Switzerland)*, *15*(7). https://doi.org/10.3390/su15076019

Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors. In *Healthcare (Switzerland)* (Vol. 10, Issue 12). MDPI. https://doi.org/10.3390/healthcare10122531

Sekaran, U., & Bougie, R. (2016). *Research Methods for Business*. www.wileypluslearningspace.com

Singh, A. N., & Gupta, M. P. (2019). Information Security Management Practices: Case Studies from India. *Global Business Review*, *20*(1), 253–271. https://doi.org/10.1177/0972150917721836

Spanaki, K., Gürgüç, Z., Mulligan, C., & Lupu, E. (2019). Organizational cloud security and control: a proactive approach. *Information Technology and People*, *32*(3), 516–537. https://doi.org/10.1108/ITP-04-2017-0131

Trang, S., & Brendel, B. (2019). A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Information Systems Frontiers*, *21*(6), 1265–1284. https://doi.org/10.1007/s10796-019-09956-4

Wang, L., Wang, R., Williams-Ceci, S., Menda, S., & Zhang, A. X. (2023). *"Is Reporting Worth the Sacrifice of Revealing What I Have Sent?": Privacy Considerations When Reporting on End-to-End Encrypted Platforms*. http://arxiv.org/abs/2306.10478

Wei, L., Sha, Z., Wang, Y., Zhang, G., Jia, H., Zhou, S., Li, Y., Wang, Y., Liu, C., Jiao, M., Sun, S., & Wu, Q. (2020). Willingness and beliefs associated with reporting travel history to high-risk coronavirus disease 2019 epidemic regions among the Chinese public: A cross-sectional study. *BMC Public Health*, *20*(1). https://doi.org/10.1186/s12889-020-09282-4

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Zammani, M., Razali, R., & Singh, D. (2019). Factors Contributing to the Success of Information Security Management Implementation. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 10, Issue 11). www.ijacsa.thesai.org

Zammani, M., Razali, R., & Singh, D. (2021). Organisational Information Security Management Maturity Model. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 12, Issue 9). www.ijacsa.thesai.org

Zheng, B., Tse, D., Ma, J., Lang, X., & Lu, Y. (2023). An Empirical Study of SETA Program Sustaining Educational Sector's Information Security vs. Information Systems Misuse. *Sustainability (Switzerland)*, *15*(17). https://doi.org/10.3390/su151712669

Zhu, R., Li, X., Liu, Q., & Zhou, Q. (2022). Executives' unethical behaviour with directions for future research. In *Frontiers in Psychology* (Vol. 13). Frontiers Media S.A. https://doi.org/10.3389/fpsyg.2022.977130