# Analisis Perilaku Keamanan Informasi Karyawan Bank di Indonesia dalam Era Transformasi Digital

## *Analysis of Information Security Behaviour of Bank Employees in Indonesia in the Era of Digital Transformation*

Tasya Desvika Rahmat1[1], Candiwan 2[1]
[1] Manajemen Bisnis Telekomunikasi dan Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom , Indonesia,
tasyadesvika@student.telkomuniversity.ac.id
[2] Manajemen Bisnis Telekomunikasi dan Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom , Indonesia,
candiwan@telkomuniversity.ac.id

***Abstrak***

Di era transformasi digital, keamanan informasi menjadi tantangan utama bagi sektor perbankan di Indonesia. Teknologi digital yang diadopsi oleh perbankan menciptakan efisiensi operasional dan meningkatkan kualitas layanan, tetapi di sisi lain membuka peluang terjadinya ancaman siber. Selain menjaga kelangsungan operasional, karyawan bank juga memiliki tanggung jawab penting dalam melindungi data pribadi nasabah yang rentan terhadap penyalahgunaan. Rendahnya tingkat kesadaran, pelatihan, dan pemahaman karyawan terkait praktik keamanan informasi menjadi salah satu faktor yang meningkatkan risiko terhadap keamanan data. Oleh karena itu, penting untuk mengevaluasi faktor-faktor yang memengaruhi perilaku keamanan informasi karyawan bank dalam menjaga keamanan data dan sistem perbankan.

Penelitian ini menggunakan *Theory Planned Behavior* untuk menganalisis faktor-faktor yang memengaruhi perilaku keamanan informasi karyawan bank di Indonesia, seperti pengelolaan kata sandi, pengelolaan keamanan infrastruktur, pengelolaan email, kebijakan keamanan organisasi, dukungan dan pelatihan organisasi, serta persepsi keamanan. Penelitian ini menggunakan metode kuantitatif dengan pendekatan survei kuisioner kepada 258 karyawan bank di Indonesia. Analisis data menggunakan metode PLS-SEM dengan *software* SmartPLS 4. Temuan menunjukkan lima dari enam variabel independen secara signifikan mempengaruhi perilaku keamanan informasi. Variabel-variabel tersebut meliputi pengelolaan kata sandi, pengelolaan keamanan infrastruktur, pengelolaan email, dukungan organisasi dan pelatihan dan persepsi keamanan. Sementara itu, kebijakan keamanan organisasi tidak menunjukkan dampak yang signifikan.

**Kata kunci:** keamanan informasi, transformasi digital, perilaku karyawan, manajemen kata sandi, kebijakan keamanan organisasi.

---

***Abstract***

*In the era of digital transformation, information security is a major challenge for the banking sector in Indonesia. Digital technology adopted by banks creates operational efficiency and improves service quality, but on the other hand opens up opportunities for cyber threats. In addition to maintaining operational continuity, bank employees also have an important responsibility in protecting customers' personal data, which is vulnerable to misuse. The low level of employee awareness, training and understanding of information security practices is one of the factors that increase the risk to data security. Therefore, it is important to evaluate the factors that influence bank employees' information security behaviour in maintaining data and banking system security.*

*This study uses Theory Planned Behaviour to analyse the factors that influence the information security behaviour of bank employees in Indonesia, such as password management, infrastructure security management, email management, organisational security policies, organisational support and training, and security perceptions. This research uses a quantitative method with a questionnaire survey approach to 258 bank employees in Indonesia. Data analysis used the PLS-SEM method with SmartPLS 4 software. The findings show that five of the six independent variables significantly influence information security behaviour. These variables include password management,*

*infrastructure security management, email management, organisational support and training and security perception. Meanwhile, organisational security policy showed no significant impact.*
***Keywords:*** *information security, digital transformation, employee behaviour, password management, organisational security policies.*

---

## I. PENDAHULUAN

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. Sektor ini akan menghadapi kerentanannya yang signifikan apabila tidak mengimplementasikan kerangka keamanan dan ketahanan siber yang efisien serta responsif (OJK, 2024). 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.

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.

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. Dalam mengukur perilaku keamanan informasi, berbagai pendekatan telah dikembangkan oleh peneliti terdahulu. Salah satu yang relevan dikembangkan oleh Egelman & Peer (2015) dan digunakan kembali dalam studi Riemenschneider et al. (2023) yang menyusun konstruk perilaku keamanan informasi berdasarkan aktivitas sehari-hari karyawan, seperti *device securement, password generation, proactive awareness,* dan *updating.* 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.*

## II. TINJAUAN LITERATUR

### *Theory Planned Behavior*

*Theory of Planned Behavior* adalah teori psikologi yang menjelaskan bagaimana niat mempengaruhi tindakan seseorang (Ajzen, 1991). Menurut Ajzen (1991) sikap ini dibentuk menurut keyakinan individu mengenai konsekuensi dari tindakan yang akan dilakukan dan penilaian terhadap norma sosial di sekitar mereka. Oleh karena itu, jika seseorang memiliki sikap yang positif, didukung oleh lingkungan sosial yang kuat, dan merasa memiliki kontrol atas tindakannya, maka niat untuk melaksanakan perilaku tersebut akan bertambah tinggi (Ajzen, 1991). Teori

Perencanaan Perilaku (TPB) menjelaskan bahwa niat individu untuk melaksanakan suatu perilaku dipengaruhi oleh 3 faktor utama: *Attitude Toward the Behavior* (Sikap terhadap Perilaku) yaitu sejauh mana seseorang menilai bahwa suatu perilaku itu baik atau buruk; *Subjective Norm* (Norma Subjektif) yaitu tekanan sosial atau pandangan orang lain yang penting terhadap perilaku tersebut; *Perceived Behavioral Control* (Kontrol Perilaku yang Dipersepsikan) yaitu sejauh mana seseorang merasa dirinya mampu atau memiliki kontrol untuk melakukan perilaku tersebut.

***Password Management***

Menurut Fernando et al. (2023) *password management* melibatkan pembuatan kata sandi, penyimpanan kata sandi dengan cara yang tepat, pembaruan kata sandi secara berkala, dan penyediaan kredensial kapan pun diperlukan. Password telah digunakan sebagai metode utama untuk autentikasi selama lebih dari enam dekade dekade (Bonneau et al., 2012). Pada penelitian yang dilakukan oleh Fagan et al. (2017) menyatakan bahwa pengguna sering terlibat dalam praktik berbahaya, seperti penyimpanan kata sandi secara fisik dan penggunaan ulang kata sandi, sebagai akibat dari masalah password management. Risiko akses yang tidak sah dapat dikurangi dengan menggunakan pengelola kata sandi dan menerapkan peraturan kata sandi yang kuat (Sari et al., 2023)

***Email Management***

Manajemen email mengacu pada praktik mengelola dan mengatur email secara efektif (Szóstek, 2011). Menurut Altulaihan et al. (2023) *phishing, spoofing,* dan bahkan misinformasi merupakan contoh operasi kejahatan siber yang dapat dilakukan dengan menggunakan email, yang juga menjadi alat untuk melakukan kejahatan lainnya, sehingga penting untuk memiliki kebijakan yang jelas mengenai penggunaan email yang aman. Menurut Candiwan et al. (2022) dalam penelitiannya mengatakan bahwa banyak individu yang masih memakai satu email untuk berbagai akun, yang dapat menimbulkan potensi risiko. Jika pihak yang berniat jahat berhasil mengakses email tersebut, mereka dapat menggunakannya untuk meretas akun-akun penting lainnya.

***Infrastructure Security Management***

Salah satu langkah dasar dalam menjaga keamanan infrastruktur adalah penggunaan perangkat lunak antivirus, yang membantu melindungi sistem dari virus dan ancaman komputer lainnya (Sanok, 2005). Menurut Putra et al. (2022) tahap dalam pengembangan perangkat lunak yang mempertimbangkan jumlah dan jenis mesin virtual yang diperlukan disebut desain infrastruktur. Salah satu keuntungan dari penerapan keamanan dan pemantauan infrastruktur jaringan adalah kemampuannya untuk mendeteksi atau menghentikan serangan siber. Keamanan infrastruktur jaringan dapat diterapkan pada server atau mesin virtual yang berfungsi sebagai sistem deteksi intrusi atau honeypot.

***Organizational Security Policy***

Kebijakan keamanan informasi di suatu organisasi menetapkan seperangkat aturan dan kebijakan yang berkaitan dengan akses karyawan dan penggunaan aset informasi organisasi (Yazdanmehr & Wang, 2016) . Menurut Saeed (2023) persyaratan keamanan siber organisasi bervariasi tergantung pada lini bisnis mereka; oleh karena itu, kebijakan keamanan siber organisasi perlu disesuaikan dengan karakteristik bisnis dan kebutuhan keamanan yang relevan. Meskipun banyak organisasi yang telah mengimplementasikan kebijakan keamanan informasi untuk mengurangi risiko keamanan yang ada, kepatuhan karyawan terhadap kebijakan tersebut bisa menjadi tantangan (Palanisamy et al., 2022)

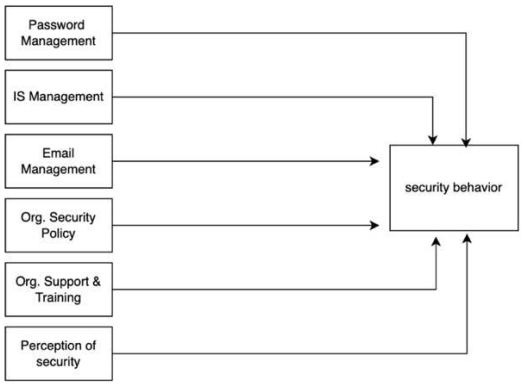
***Organizational Support & Training***

Pelatihan pada dasarnya terkait dengan komitmen dan kepuasan karyawan. Menurut Ocen et al. (2017) menegaskan bahwa pekerja lebih cenderung merasa dihargai dan berdedikasi kepada organisasi mereka ketika mereka melihat pelatihan sebagai indikasi dukungan organisasi. Hal ini sejalan dengan penelitian yang dilakukan oleh Muma et al. (2014) dan Jehanzeb et al. (2013) menemukan bahwa pelatihan karyawan meningkatkan kemauan dan kemampuan untuk mengadopsi perubahan teknologi baru dan metode produksi, guna meningkatkan penemuan dan kreativitas karyawan, serta mengurangi pergantian karyawan, yang kesemuanya berujung pada komitmen.

**Hipotesis dan Model Penelitian**

Kerangka pemikiran pada penelitian ini diadaptasi dari penelitian Saeed (2023). Dalam penelitiannya yang berjudul "*Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia"* ia mengangkat enam faktor yang mempengaruhi perilaku keamanan karyawan. Menurut Saeed (2023) *Theory of Planned Behavior* menyatakan bahwa, jika seorang individu mempersepsikan suatu kegiatan sebagai hal yang menyenangkan dan bermanfaat, menerima dukungan dari kelompok sosialnya, dan merasa bahwa mereka memiliki kemampuan dan keterampilan untuk memenuhi permintaan perilaku yang diminta, hal ini akan menghasilkan niat yang lebih kuat, dan ada probabilitas yang lebih tinggi bahwa individu tersebut akan terlibat dalam perilaku yang diinginkan. Dalam penelitian ini, praktik *password management, infrastructure security management,* dan *email*

*management* pengguna diambil sebagai kontrol perilaku yang dirasakan *(perceived behavioral controls)*. Sedangkan, organizational security policy serta organizational support and training dimodelkan sebagai norma subyektif *(subjective norms)* dan *perception of security* dikategorikan sebagai sikap perilaku *(attitude)*.




Gambar 1. Kerangka Pemikiran Penelitian
*Sumber: (Saeed, 2023)*

Oleh karena itu, peneliti menggunakan TPB sebagai lensa teoritis untuk memahami perilaku keamanan informasi karyawan bank di Indonesia. Berikut ini adalah hipotesis untuk penelitian ini:

- H1*: Password Management* berpengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia.
- H2: *Infrastructure Security Management* berpengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia.
- H3: *Email Management* berpengaruh terhadap perilaku keamanan irmasi pada karyawan bank di Indonesia.
- H4: *Organizational Security Policy* berpengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia.
- H5: *Organizational Support and Training* berpengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia.
- H6: *Perception of Security* berpengaruh terhadap perilaku keamanan informasi pada karyawan bank di Indonesia.

## III. METODOLOGI PENELITIAN

Penelitian ini mengadopsi pendekatan kuantitatif. Pendekatan ini diterapkan untuk menganalisis populasi atau sampel tertentu dengan cara mengumpulkan data menggunakan instrumen penelitian yang telah disiapkan. Selanjutnya, data yang terkumpul dianalisis secara statistik. Penelitian ini menggunakan instrumen yang diadaptasi dari studi Saeed (2023) disebarkan melalui survei secara *online* menggunakan *Google Forms*. Data yang telah terkumpul kemudian diuji dan dianalisa menggunakan SEM dengan menggunakan *software* SmartPLS 4. Jumlah sampel minimum ditentukan berdasarkan rumus metode akar kuadrat terbalik dengan nilai koefisien jalur minimum 0,2 dan tingkat signifikansi 5%, sehingga diperoleh jumlah sampel minimum yang dibutuhkan sebanyak 154.505 dibulatkan menjadi 155. Responden yang didapatkan dalam penelitian ini adalah 258 responden. Penelitian ini menargetkan para karyawan bank yang mencakup cabang bank sektor publik dan swasta di Indonesia. Kriteria yang diperlukan adalah karyawan laki-laki/perempuan yang menggunakan komputer/laptop sebagai responden survei. Responden dalam penelitian ini terdiri dari 148 orang perempuan dan 110 orang laki-laki.

## IV. HASIL DAN PEMBAHASAN

### 4.1 Validity dan realibility testing

Hasil pengujian ditampilkan pada Tabel 1. Berdasarkan hasil pada tabel, seluruh konstruk dalam model memenuhi kriteria ini, yang menunjukkan adanya validitas diskriminan yang baik.

Tabel 1. Uji *Fornell Larcker*

| | EM | ISM | OSP | OST | PM | POS | SB |
|---|---|---|---|---|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **EM** | 0,781 | | | | | | |
| **ISM** | 0,434 | 0,774 | | | | | |
| **OSP** | 0,507 | 0,409 | 0,886 | | | | |
| **OST** | 0,436 | 0,693 | 0,343 | 0,766 | | | |
| **PM** | 0,526 | 0,542 | 0,667 | 0,474 | 0,795 | | |
| **POS** | 0,464 | 0,565 | 0,385 | 0,489 | 0,458 | 0,833 | |
| **SB** | 0,575 | 0,697 | 0,550 | 0,684 | 0,682 | 0,597 | 0,701 |

Selain melakukan uji validitas, *outer model* juga mencakup uji reliabilitas. Ada dua metode yang dipergunakan pada uji reliabilitas dalam PLS, yaitu *cronbach's alpha* dan *composite reliability*. Kedua metode ini memerlukan nilai parameter yang harus ≥ 0,6 dan konstruk dikatakan valid apabila nilai AVE > 0,50 (Abdillah & Hartono, 2015). Tabel 2 menunjukkan bahwa seluruh konstruk telah memenuhi kriteria tersebut, sehingga dapat disimpulkan bahwa model ini memiliki konstruk yang valid dan reliabel secara keseluruhan.

Tabel 2. Uji *Validity* dan *Realibility*

| | ***Cronbach's alpha*** | ***Composite reliability (rho_a)*** | ***Composite reliability (rho_c)*** | ***Average variance extracted (AVE)*** |
|---|---|---|---|---|
| **EM** | 0.681 | 0.684 | 0.824 | 0.610 |
| **ISM** | 0.866 | 0.867 | 0.900 | 0.600 |
| **OSP** | 0.726 | 0.735 | 0.879 | 0.785 |
| **OST** | 0.703 | 0.708 | 0.834 | 0.627 |
| **PM** | 0.806 | 0.560 | 0.819 | 0.693 |
| **POS** | 0.558 | 0.902 | 0.930 | 0.770 |
| **SB** | 0.900 | 0.807 | 0.873 | 0.633 |

### 4.2 Inner Model

Model struktural dievaluasi untuk menganalisis hubungan antara faktor-faktor independen dan *Security Behavior (SB)* sebagai variabel dependen. Koefisien determinasi ($R^2$) sebesar 0.696 menunjukkan bahwa 69,6% variasi dalam perilaku keamanan informasi dijelaskan oleh enam konstruk: *Password Management (PM), Infrastructure Security Management (ISM), Email Management (EM), Organizational Support and Training (OST), Organizational Security Policy (OSP), and Perception of Security (POS).*

Tabel 3. Uji *Path Coeffiecients*

| | **Original sample (O)** | **Standard deviation** | **T statistics** | **P values** | **Result** |
|---|---|---|---|---|---|
| **EM -> SB** | 0.130 | 0.044 | 2.950 | 0.003 | Diterima |
| **ISM -> SB** | 0.201 | 0.056 | 3.610 | 0.000 | Diterima |
| **OSP -> SB** | 0.070 | 0.046 | 1.524 | 0.128 | Ditolak |
| **OST -> SB** | 0.275 | 0.048 | 5.713 | 0.000 | Diterima |
| **PM -> SB** | 0.158 | 0.055 | 4.436 | 0.001 | Diterima |
| **POS -> SB** | 0.243 | 0.048 | 3.296 | 0.000 | Diterima |

### 4.3 Hipotesis

#### 4.3.1 Pengaruh *Password Management* terhadap Perilaku Keamanan Informasi

Hasil uji menunjukkan bahwa variabel *Password Management* (PM) memiliki nilai koefisien 0.158, t-statistik sebesar 4.436, dan nilai p sebesar 0.001. Nilai p kurang dari 0.05, sehingga dapat disimpulkan bahwa pengaruhnya secara statistik signifikan. Temuan ini memperkuat penelitian sebelumnya tentang betapa pentingnya bagi pekerja untuk memiliki manajemen kata sandi yang baik, seperti menggunakan kata sandi yang kuat, menggantinya secara

berkala, dan tidak membagikannya dengan orang lain. Saeed (2023) melakukan studi dengan responden karyawan bisnis dan menemukan bahwa manajemen kata sandi yang baik merupakan salah satu hal terpenting yang dapat dilakukan untuk meningkatkan pemahaman dan kepatuhan terhadap kebiasaan keamanan informasi.

**4.3.2 Pengaruh *Infrastructure Security Management* terhadap Perilaku Keamanan Informasi**

Hasil analisis menunjukkan bahwa *Infrastructure Security Management* (ISM) memiliki pengaruh positif dan signifikan terhadap *security behavior,* dengan nilai koefisien sebesar 0.201, nilai *t-statistics* 3.610, dan *p-value* 0.000. Nilai p yang lebih kecil dari 0.05 menandakan bahwa hubungan ini signifikan secara statistik. Hubungan ini secara statistik signifikan jika nilai p kurang dari 0,05. Hal ini berarti bahwa metode manajemen keamanan infrastruktur yang baik, termasuk penggunaan *firewall,* enkripsi data, dan memperbarui perangkat lunak secara berkala, benar-benar membantu pekerja menjadi lebih berhati-hati dalam mengelola informasi mereka. Sebuah studi terhadap mahasiswa ilmu komputer juga menunjukkan bahwa manajemen infrastruktur dianggap relevan dan membantu orang mengembangkan kebiasaan keamanan informasi yang baik (Saeed, 2023).

**4.3.3 Pengaruh *Email Management* terhadap Perilaku Keamanan Informasi**

Berdasarkan hasil analisis uji hipotesis diketahui bahwa variabel *Email Management* (EM) berpengaruh terhadap *security behavior* (SB) dengan nilai *path coefficient* sebesar 0.130, nilai *t-statistics* sebesar 2.950, dan *p-value* sebesar 0.003. Dampak ini secara statistik signifikan karena nilai p kurang dari 0,05, yang merupakan tingkat signifikansi. Hasil penelitian ini sebanding dengan penelitian terdahulu yang dilakukan oleh Candiwan & Rianda (2024) yang menemukan bahwa pengguna dapat mengembangkan kebiasaan keamanan informasi yang baik dengan melakukan hal-hal seperti tidak membuka pesan atau lampiran dari pengirim yang tidak dikenal, menggunakan enkripsi dalam komunikasi email, dan memeriksa pengaturan keamanan pada aplikasi email berbasis web (Candiwan & Rianda, 2024).

**4.3.4 Pengaruh *Organizational Security Policy* terhadap Perilaku Keamanan Informasi**

Hubungan antara *Organizational Security Policy (*OSP) dan *Security Behavior* menunjukkan nilai koefisien sebesar 0.070, *t-statistics* 1.524, dan *p-value* sebesar 0.128. Dampak ini tidak signifikan secara statistik karena nilai p lebih besar dari 0,05. Hal ini tidak sejalan dengan penelitian sebelumnya yang dilakukan oleh Sohrabi Safa et al. (2016) mereka menemukan bahwa mengikuti kebijakan keamanan informasi organisasi dapat mengarah pada sikap dan niat perilaku yang baik terhadap aturan tersebut. Bagaimana orang bertindak terhadap aturan keamanan organisasi menunjukkan seberapa baik mereka memahami, mengikuti, atau bahkan mengabaikan peraturan keamanan informasi yang berlaku di tempat kerja.

**4.3.5 Pengaruh *Organizational Support and Training* terhadap Perilaku Keamanan Informasi**

Nilai *path coefficient* sebesar 0.275, *t-statistics* sebesar 5.713, dan *p-value* sebesar 0.000 semuanya menunjukkan bahwa variabel *Organizational Support & Training* (OST) memiliki pengaruh yang besar dan positif terhadap *Security Behavior*. Hal ini menunjukkan bahwa memberikan bantuan dan pelatihan kepada pekerja di tempat kerja merupakan bagian penting dalam mendorong perilaku keamanan informasi yang baik.

**4.3.6 Pengaruh *Perception of Security* terhadap Perilaku Keamanan Informasi**

Nilai koefisian untuk hubungan antara *Perception of Security* (POS) dengan *Security behavior* hanya 0,243, *t-statistic* sebesar 3.296, dan nilai p sebesar 0,000. Nilai p yang <0.05 menunjukkan bahwa terdapat hubungan yang antara bagaimana pekerja memandang keamanan dan bagaimana mereka bertindak untuk melindungi informasi mereka. Hal ini tidak sesuai dengan penelitian Saeed (2023) dalam jurnal *Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia* yang menunjukkan variabel ini tidak signifikan pada objek karyawan umum di Arab Saudi.

## V. KESIMPULAN DAN SARAN

Penelitian ini membuktikan bahwa perilaku karyawan bank terkait keamanan informasi tidak secara seragam dipengaruhi oleh semua faktor. Hasil menunjukkan bahwa *Password Management* (PM), *Infrastructure Security Management* (ISM), *Email Management* (EM), *Organizational Support & Training* (OST), serta *Perception of Security* (POS) secara signifikan mempengaruhi *security behavior* (SB). Faktor yang memiliki dampak terbesar adalah *Organizational Support & Training* (OST). Sebaliknya, *Organizational Security Policy* (OSP) tidak menunjukkan korelasi yang signifikan dengan perilaku keamanan. Hasil ini menyoroti pentingnya strategi praktis dan bantuan dari organisasi, daripada mengandalkan kebijakan tertulis. Oleh karena itu, untuk meningkatkan perilaku keamanan informasi, sangat penting untuk memprioritaskan pemberdayaan karyawan melalui pelatihan yang relevan, penyediaan infrastruktur yang aman, dan pengembangan praktik manajemen data yang efektif. Organisasi harus

menyediakan dukungan teknis yang mudah diakses dan pelatihan keamanan informasi yang berkelanjutan yang relevan dengan tanggung jawab karyawan. Selain itu, penerapan praktis kebijakan teknologi, termasuk penggunaan sistem IT yang aman, filter email, dan pengelola kata sandi, harus difasilitasi.

REFERENSI

Abdillah, W., & Hartono, J. (2015). *Partial Least Square (PLS) Alternatif Structural Equation Modeling (SEM) dalam Penelitian Bisnis* (1st ed.). Andi.

Ajzen, I. (1991). *The Theory of Planned Behavior*. *50*, 179–211.

Belkhamza, Z. (2023). *Cybersecurity in Digital Transformation Applications: Analysis of Past Research and Future Directions*.

BNPP. (2024, July 24). *Tingkatkan Keamanan Siber Nasional, BNPP Apresasi Launching CSIRT Bersama 2024 oleh Badan Siber dan Sandi Negara*. https://bnpp.go.id/berita/tingkatkan-keamanan-siber-nasional-bnpp-apresasi-launching-csirt-bersama-2024-oleh-badan-siber-dan-sandi-negara

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *Proceedings - IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44

Candiwan, C., Azmi, M., & Alamsyah, A. (2022). Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era. *International Journal of Safety and Security Engineering*, *12*(2), 229–237. https://doi.org/10.18280/ijsse.120212

Candiwan, C., & Rianda, L. M. (2024). Transactions at Your Fingertips: Influential Factors in Information Security Behavior for Mobile Banking Users. *International Journal of Safety and Security Engineering*, *14*(3), 795–806. https://doi.org/10.18280/ijsse.140312

Do, T. D., Pham, H. A. T., Thalassinos, E. I., & Le, H. A. (2022). The Impact of Digital Transformation on Performance: Evidence from Vietnamese Commercial Banks. *Journal of Risk and Financial Management*, *15*(1). https://doi.org/10.3390/jrfm15010021

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2873–2882.

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-Centric Computing and Information Sciences*, *7*(1). https://doi.org/10.1186/s13673-017-0093-6

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). *ANALISIS RISIKO TEKNOLOGI INFORMASI PADA BANK SYARIAH : IDENTIFIKASI ANCAMAN DAN TANTANGAN TERKINI*. *5*(2). http://journal.uiad.ac.id/index.php/asy-syarikah

Fernando, W. P. K., Dissanayake, D. A. N. P., Dushmantha, S. G. V. D., Liyanage, D. L. C. P., & Karunatilake, C. (2023). Challenges and Opportunities in Password Management: A Review of Current Solutions. *Sri Lanka Journal of Social Sciences and Humanities*, *3*(2), 9–20. https://doi.org/10.4038/sljssh.v3i2.96

Jehanzeb, K., Rasheed, A., & Rasheed, M. F. (2013). Organizational Commitment and Turnover Intentions: Impact of Employee's Training in Private Sector of Saudi Arabia. *International Journal of Business and Management*, *8*(8). https://doi.org/10.5539/ijbm.v8n8p79

Krishnan, S. G., Al-Nahari, A., Ismail, N. A., & Yao, D. N. L. (2023). Enhancing Cybersecurity Awareness among Banking Employees in Malaysia: Strategies, Implications, and Research Insights. *International Journal of Academic Research in Business and Social Sciences*, *13*(8). https://doi.org/10.6007/ijarbss/v13-i8/17413

Luthfah, D. (2023). PENGUATAN KEAMANAN SIBER PADA SEKTOR JASA KEUANGAN INDONESIA. *JURNAL PENELITIAN DAN KARYA ILMIAH LEMBAGA PENELITIAN UNIVERSITAS TRISAKTI*, 259–267. https://doi.org/10.25105/pdk.v9i1.18643

Mazumder, M. M. M., & Hossain, D. M. (2023). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*, *13*(2), 217–239.

Muma, M., Iravo, Dr. A., & Omondi, Dr. M. (2014). Effect of Training Needs Assessment on Employee Commitment in Public Universities: A Case Study of Jomo Kenyatta University of Agriculture and Technology. *International Journal of Academic Research in Business and Social Sciences*, *4*(9). https://doi.org/10.6007/ijarbss/v4-i9/1153

Ocen, E., Francis, K., & Angundaru, G. (2017). The role of training in building employee commitment: the mediating effect of job satisfaction. *European Journal of Training and Development*, *41*(9), 742–757. https://doi.org/10.1108/EJTD-11-2016-0084

OJK. (2024, July 9). *Siaran Pers: OJK Luncurkan Pedoman Keamanan Siber Bagi Penyelenggara Inovasi Teknologi Sektor Keuangan (ITSK)*.

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2022). BYOD Policy Compliance: Risks and Strategies in Organizations. *Journal of Computer Information Systems*, *62*(1), 61–72. https://doi.org/10.1080/08874417.2019.1703225

Putra, Nurwa, A. R. A., & Priambodo, F. D. (2022). Infrastructure as Code for Security Automation and Network Infrastructure Monitoring. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *22*(1), 201–214. https://doi.org/10.30812/matrik.v22i1.2471

Riemenschneider, C. K., Burney, L. L., & Bina, S. (2023). The influence of organizational values on employee attitude and information security behavior: the mediating role of psychological capital. *Information and Computer Security*, *31*(2), 172–198. https://doi.org/10.1108/ICS-10-2022-0156

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

Saeed, S. (2023). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. *Sustainability (Switzerland)*, *15*(12). https://doi.org/10.3390/su15129426

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. In *Sensors* (Vol. 23, Issue 15). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s23156666

Sanok, D. J. (2005). *An Analysis of How Antivirus Methodologies Are Utilized in Protecting Computers from Malicious Code*. http://computer.howstuffworks.com/virus.htm

Sari, P. K., Handayani, P. W., Hidayanto, A. N., & Busro, P. W. (2023). HOW INFORMATION SECURITY MANAGEMENT SYSTEMS INFLUENCE THE HEALTHCARE PROFESSIONALS' SECURITY BEHAVIOR IN A PUBLIC HOSPITAL IN INDONESIA. *Interdisciplinary Journal of Information, Knowledge, and Management*, *18*, 583–607. https://doi.org/10.28945/5185

Sari, P. K., Trianasari, N., & Prasetio, A. (2025). Investigating the Main Factors Affecting Healthcare Workers' Information Security Behaviors: An Empirical Study in Indonesia. *Journal of Internet Services and Information Security*, *15*(1), 1–15. https://doi.org/10.58346/JISIS.2025.I1.001

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/https://doi.org/10.1016/j.cose.2015.10.006

Szóstek, A. M. (2011). 'Dealing with My Emails': Latent user needs in email management. *Computers in Human Behavior*, *27*(2), 723–729.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36–46.