Jurnal Manajemen dan Bisnis Ekonomi
Volume 3, Nomor 2, April 2025
e-ISSN: 2985- 5918; p-ISSN: 2985-590X, Hal. 161-175
DOI: https://doi.org/10.54066/jmbe-itb.v3i2.3170
Online Available at: https://jurnal.itbsemarang.ac.id/index.php/JMBE

Strategi Mengatasi *Data Breaches* di Era Industri 4.0: Kasus *Data Breaches* Bank Rakyat Indonesia

Annisa Ayu Handayani[1], Balqis Naura Izzati[2], Diana Nur'azzah[3], Khoirunnisa[4]
Universitas Pendidikan Indonesia, Indonesia
Email : annisa.ayu18@upi.edu[1], balqisnizzati@upi.edu[2], diananurazzah@upi.edu[3], khoirunnisa13.85@upi.edu[4]

Abstract. *To analyze the strategies implemented by Bank Rakyat Indonesia (BRI) in addressing data breaches in the Industry 4.0 era by identifying contributing factors such as user awareness, security system weaknesses, and the effectiveness of mitigation policies. This study uses a qualitative approach with descriptive methods through document analysis with purposive sampling techniques of official BRI reports and relevant scholarly literature. The research findings indicate that the main causes of data breaches are low digital security awareness, weaknesses in authentication systems, and the rise of phishing attacks. BRI has responded by implementing several key strategies, including digital literacy education, the use of layered security technologies such as multi-factor authentication and AI-based transaction monitoring, as well as early detection and incident response systems. These measures have successfully prevented hundreds of thousands of unauthorized access attempts throughout 2023. The implications of this study emphasize that increasing public awareness of digital security and continuously improving technological infrastructure are crucial steps in minimizing data breach risks and enhancing public trust in digital banking services.*

Keywords: *cyber security, data breaches, phishing attacks, strategy.*

Abstrak. Penelitian ini bertujuan untuk menganalisis strategi yang diterapkan oleh Bank Rakyat Indonesia (BRI) dalam menangani kebocoran data di era Industri 4.0 dengan mengidentifikasi faktor-faktor penyebab seperti kesadaran pengguna, kelemahan sistem keamanan, dan efektivitas kebijakan mitigasi. Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif. Teknik pengumpulan data dilakukan melalui studi dokumen dengan teknik *purposive sampling* terhadap laporan resmi BRI serta artikel ilmiah yang relevan. Temuan penelitian menunjukkan bahwa rendahnya kesadaran keamanan digital, lemahnya sistem otentikasi, serta meningkatnya serangan *phishing* menjadi penyebab utama kebocoran data. BRI telah mengimplementasikan beberapa strategi utama, seperti edukasi digital secara berkala, penerapan autentikasi multi-faktor, pemantauan transaksi berbasis kecerdasan buatan, serta sistem deteksi dan respon cepat terhadap insiden keamanan. Strategi ini terbukti efektif dalam mencegah ratusan ribu upaya akses tidak sah terhadap akun nasabah selama tahun 2023. Implikasi dari penelitian ini menegaskan pentingnya kombinasi antara peningkatan literasi keamanan digital bagi pengguna layanan perbankan dan penguatan sistem keamanan digital oleh institusi keuangan untuk meminimalisasi risiko kebocoran data yang semakin kompleks di era digital.

Kata kunci: strategi, pelanggaran data, serangan penipuan, keamanan siber

1. LATAR BELAKANG

Perkembangan dunia di era digital dan industri 4.0 memberikan kemudahan bagi individu dalam melakukan aktivitas dan transfer informasi. Namun di balik tawaran kemudahan yang diberikan, perkembangan dunia di era digital dan industri 4.0 dapat membawa ancaman dan dampak negatif seperti penyebaran *hoax*, dan ancaman terhadap privasi serta keamanan data. Ancaman dan dampak negatif yang terjadi akan menghambat kegiatan atau aktivitas lainnya, sehingga hal ini menjadi urgensi yang harus segera

Received: March 17, 2025; Revised: March 24, 2025; Accepted: March 31, 2025; Published: April 07, 2025

ditangani dengan baik. Perlindungan aset informasi memiliki keterkaitan yang erat dengan manusia, karena faktor manusia sering kali menjadi titik lemah dalam keamanan data. Kesadaran, pengetahuan, dan kebiasaan individu dalam mengelola informasi, berperan penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Oleh karena itu, memiliki kesadaran akan keamanan merupakan aspek yang sangat penting, karena individu dapat mengambil langkah-langkah pencegahan yang tepat untuk melindungi data dan informasi pribadi, mencegah kebocoran informasi, serta menjaga sistem dari potensi serangan siber yang dapat merugikan.

Kebocoran data sendiri bukanlah permasalahan baru di Indonesia. Berdasarkan data empat tahun lalu, banyak kasus kebocoran data masyarakat yang tidak disadari. Salah satu kasusnya adalah kebocoran data sebanyak dua juta nasabah BRI Life pada bulan Juli 2021 lalu. Bank Rakyat Indonesia atau BRI adalah badan usaha milik Indonesia yang menyediakan berbagai macam jasa keuangan. PT Bank Rakyat Indonesia (Persero) Tbk (BBRI) menempati posisi pertama dengan jumlah pengguna aplikasi *mobile banking* terbanyak. Total pengguna *mobile banking* bank BRI yakni BRImo pada kuartal I 2024 tercatat tumbuh 30,3% secara tahunan (yoy) menjadi 33,5 juta pengguna, dibandingkan periode yang sama tahun sebelumnya sebesar 25,7 juta pengguna. (CNBC Indonesia, 2024).

Penting untuk mengidentifikasi faktor-faktor utama yang berkontribusi terhadap terjadinya *data breaches* di BRI, baik dari aspek teknis, kebijakan, maupun *human error*. Pemahaman terhadap celah keamanan dalam sistem digital, efektivitas regulasi yang diterapkan, serta tingkat kesadaran pengguna terhadap ancaman siber menjadi langkah awal dalam mengevaluasi risiko kebocoran data.

Selain itu, diperlukan strategi yang komprehensif untuk mengatasi dan mencegah *data breaches* di sektor perbankan. Pendekatan berbasis teknologi, penerapan regulasi yang lebih ketat, serta peningkatan literasi keamanan siber bagi karyawan dan nasabah menjadi elemen kunci dalam memperkuat perlindungan data. Dengan menerapkan langkah-langkah strategis yang tepat, sistem perbankan dapat lebih siap dalam menghadapi ancaman serangan siber yang semakin kompleks di era digital.

2. KAJIAN TEORITIS

Data Breaches

Data breaches atau yang disebut dengan pelanggaran data merupakan segala aktivitas menyebarluaskan data maupun informasi yang bersifat rahasia, sensitif dan dilindungi, kepada pihak-pihak yang tidak berwenang. Data rahasia ini dapat diakses melalui aktivitas *cyber attack* seperti: *phishing, malware, ransomware, Denial of Service* (DoS), dan aktivitas lainnya. Terjadinya fenomena *data breaches* dapat dipengaruhi oleh langkah-langkah keamanan (Manworren, Letwat, & Daily, 2016), tata kelola dan tanggung jawab sosial perusahaan (Lending, Minnick, & Schorno, 2018), *error and insider misuse* (Cheng et al., 2017), ketidakmampuan manusia atau perangkat lunak (Cheng et al., 2017), pencurian (Wikina, 2014), *hacker prestige*, *human vulnerabilities* (Hong & Linden, 2012), dan sejenisnya. Apabila ditinjau dari subjeknya pelanggaran data ini tidak hanya semata-mata terjadi akibat *cyber crime* yang dilakukan oleh *Hacker*, namun terdapat faktor lainnya seperti: kelalaian pihak internal maupun eksternal yang memiliki akses data, serta dapat berupa kehilangan perangkat sistem (Sukmawan & Setyawan, 2023). Dalam konsep keamanan informasi faktor kelalaian manusia (*human error*) menjadi faktor utama yang paling sering terjadi dalam insiden kebocoran data (*data breaches*).

Fenomena *data breaches* dapat memberikan dampak negatif bagi suatu perusahaan atau organisasi seperti *abnormal return*, fluktuasi harga saham, erosi terhadap nilai pasar (*market value erosion*), *penalty*, reputasi, dan *shareholder value* (Srinivas & Liang, 2022). *Data breaches* ini menjadi ancaman *cyber security* yang dapat terjadi baik di lingkungan masyarakat, industri atau perusahaan, maupun pemerintah. Salah satu kasus fenomena *data breaches* yang terjadi di lingkungan industri atau perusahaan adalah kasus *data breaches* yang dialami Bank Rakyat Indonesia (BRI).

Cyber Security

"*Cyber*" adalah awalan yang berkonotasi dengan dunia maya dan mengacu pada jaringan komunikasi elektronik dan realitas virtual (Oxford, 2014). Menurut Wiener (dalam Jefferson, 2024) istilah ini berevolusi dari istilah "*cybernetics*", yang merujuk pada "bidang kontrol dan komunikasi, baik pada mesin maupun hewan". Istilah "*cyberspace*" dipopulerkan oleh novel William Gibson pada tahun 1984, Neuromancer, di mana ia mendeskripsikan visinya tentang ruang tiga dimensi dari informasi murni,

yang bergerak antara komputer dan kelompok komputer di mana manusia adalah penghasil dan pengguna informasi tersebut (Kizza, 2011). Apa yang sekarang kita kenal sebagai *cyberspace* dimaksudkan dan dirancang sebagai lingkungan informasi (Singer & Friedman, 2013), dan ada apresiasi yang diperluas terhadap *cyberspace* saat ini. Sebagai contoh, *Public Safety Canada* (2010) mendefinisikan *cyberspace* sebagai "dunia elektronik yang diciptakan oleh jaringan teknologi informasi yang saling terhubung dan informasi pada jaringan tersebut. Mengenai istilah "*security*", dalam literatur yang kami tinjau kembali, tampaknya tidak ada konsep yang diterima secara luas, dan istilah ini sangat sulit untuk didefinisikan dalam pengertian umum (Friedman & West, 2010; Cavelty, 2008). Menurut Buzan, Wæver, dan Wilde (1998), wacana keamanan harus mencakup dan berusaha memahami siapa yang melakukan pengamanan, pada isu apa (ancaman), untuk siapa (objek yang dituju), mengapa, dengan hasil apa, dan dalam kondisi apa (struktur). Meskipun ada bentuk-bentuk keamanan yang lebih konkret (misalnya, sifat fisik, sifat manusia, sifat sistem informasi, atau definisi matematis untuk berbagai jenis keamanan), istilah ini memiliki makna berdasarkan perspektif seseorang dan apa yang ia nilai. Istilah ini masih menjadi perdebatan, tetapi prinsip utama dari keamanan adalah bebas dari bahaya atau ancaman (Oxford, 2014). Lebih lanjut, meskipun kami telah mengindikasikan bahwa keamanan adalah topik yang diperdebatkan, Baldwin (1997) menyatakan bahwa seseorang tidak dapat menggunakan sebutan ini sebagai "alasan untuk tidak merumuskan konsepsi keamanannya sendiri sejelas dan setepat mungkin".

Cyber security atau keamanan siber adalah bagian dari keamanan informasi yang berfokus pada perlindungan kerahasiaan, integritas dan ketersediaan atau dalam istilah bahasa Inggris disebut *Confidentiality, Integrity and Availability* (CIA) dan merupakan aset informasi digital terhadap segala ancaman yang mungkin timbul atau disusupi melalui Internet (Solms & Solms, 2018). *Cyber security* digunakan untuk melindungi informasi dan sistem dari ancaman siber seperti *data breaches*, agar dapat menjaga kestabilan sistem operasional perusahaan. Ancaman siber sering kali membidik aset rahasia, politik, dan militer suatu negara, atau rakyatnya, sehingga ini menjadi tantangan utama di era digital bagi semua pihak termasuk pemerintah, dan perusahaan (Seemma et al., 2018).

Dalam era saat ini pendekatan efektif terhadap *cyber security* mencakup lima unsur yaitu: identifikasi (*identification*), perlindungan (*protection*), deteksi (*detection*), respons (*response*), dan pemulihan (*recovery*) (Alqudhaibi et al., 2025). Implementasi kelima komponen tersebut memungkinkan entitas bisnis untuk meminimalisasi tingkat kerawanan terhadap *cyber attack*. Hal ini dicapai melalui formulasi prosedur sistematis yang mencakup *identification*, *protection*, *detection*, *response*, dan *recovery* terhadap insiden keamanan siber. Efektivitas *cyber security* berkorelasi dengan kerangka kerja manajemen risiko konvensional, di mana optimalisasi dicapai melalui:

a. Audit dan monitoring periodik: Evaluasi berkelanjutan terhadap sistem keamanan.
b. Internalisasi kesadaran keamanan: Peningkatan pemahaman dan kepatuhan staf terhadap protokol keamanan.
c. Aplikasi protokol secara rigor: Penerapan kebijakan keamanan secara konsisten dan terukur.
d. Alokasi sumber daya yang efisien: Optimalisasi penggunaan anggaran dan aset untuk mitigasi, pemantauan, dan penanganan dampak *cyber attack*.

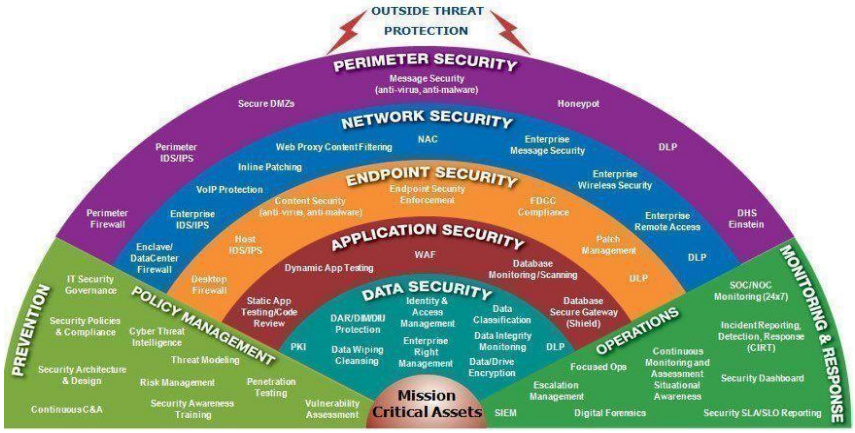
Dengan menerapkan *cyber security* yang efektif ini menandakan perusahaan telah menerapkan langkah yang nyata dalam mengatasi fenomena dari *cyber attack* yang mulai marak di era digital saat ini.

Teori *Layered Security* dan Prinsip *Defense in Depth*

Prinsip *defense in depth* merupakan bagian dari teori *layered security* yang menekankan pentingnya perlindungan berlapis melalui kombinasi teknologi, edukasi, dan manajemen risiko dalam rangka menguatkan sistem keamanan.

Gambar 1. Ilustrasi Konsep *Defense in Depth* dalam Keamanan Siber

(Sumber: The CISO Times. "*Defense in Depth – The Layered Approach to Cybersecurity*.")



Gambar menunjukkan pendekatan berlapis (*layered security*) dalam sistem keamanan siber, dimulai dari lapisan paling luar (pengguna) hingga ke pusat data atau informasi sensitif. Setiap lapisan memiliki fungsi pencegahan, deteksi, dan respons terhadap potensi ancaman. Dalam gambar ini menekankan bahwa tidak ada satu lapisan pun yang cukup kuat untuk melindungi sistem secara menyeluruh, sehingga diperlukan kolaborasi antar lapisan keamanan.

Penelitian Relevan

Adani et al,. (2024) dalam penelitiannya yang berjudul "*The Importance of Security Awareness in Combating Phishing Attacks: A Case Study of Bank Rakyat Indonesia*" dengan menggunakan metode kuantitatif dan kualitatif dengan analisis regresi linier sederhana. Hasil penelitian menunjukkan bahwa kesadaran keamanan memiliki dampak yang signifikan dalam mengurangi serangan *phishing*. Hasil temuan tersebut relevan dengan penelitian ini, karena membahas tentang strategi yang dapat dilakukan untuk menghadapi ancaman *cyber security*.

3. METODE PENELITIAN

Metode penelitian merupakan suatu cara yang digunakan untuk mendapatkan data dan menganalisis objek penelitian. Penelitian ini menggunakan pendekatan kualitatif dengan jenis deskriptif. Metode kualitatif adalah metode yang bersifat enterpretif dan digunakan untuk meneliti kondisi objek atau fenomena dalam konteks yang dialami (Sugiyono, 2018). Dengan menggunakan metode kualitatif deskriptif dapat membantu peneliti dalam menggambarkan strategi yang dilakukan oleh Bank Rakyat Indonesia (BRI) dalam menghadapi fenomena ancaman *cyber security* di era industri 4.0. Teknik pengumpulan data penelitian ini menggunakan studi dokumen. Dokumen merupakan catatan peristiwa yang telah berlalu yang dapat berupa tulisan, gambar, atau karya monumental seseorang (Sugiyono, 2018). Objek dalam penelitian ini mencakup seluruh dokumen yang berkaitan dengan keamanan siber yang diterbitkan baik oleh BRI sendiri maupun oleh pihak eksternal yang relevan. Teknik pengambilan sampel dalam penelitian ini adalah *purposive sampling*, yang mana meliputi laporan yang dikeluarkan oleh Bank Rakyat Indonesia dan dari artikel yang relevan dengan penelitian ini.

4. HASIL DAN PEMBAHASAN

Proses Pengumpulan Data

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan teknik pengumpulan data berupa studi dokumen. Dokumen yang dianalisis diperoleh melalui teknik purposive sampling, dengan kriteria relevansi dengan isu keamanan siber di sektor perbankan, khususnya BRI. Rentang waktu dokumen yang dikaji mencakup periode tahun 2022 hingga awal 2025, dengan fokus utama pada dokumen yang memuat strategi keamanan digital, kasus *data breach*, dan upaya mitigasi serangan siber.

Jenis dokumen yang dikaji meliputi:

1. Laporan resmi dan siaran pers BRI (2024),
2. Publikasi media seperti Kompas (2023),
3. Artikel ilmiah dan studi kasus seperti Adani et al. (2024),
4. Literatur sekunder dan jurnal yang membahas pendekatan teoritis keamanan siber.

Strategi Mitigasi *Data Breach* oleh BRI

Hasil studi dokumen mengungkap bahwa BRI mengadopsi strategi mitigasi *data breach* yang mencakup tiga pilar utama, yaitu: peningkatan kesadaran keamanan pengguna, penguatan sistem keamanan digital, serta sistem deteksi dini dan respons cepat terhadap insiden keamanan.

a. Peningkatan Kesadaran Keamanan Pengguna

BRI secara aktif melakukan edukasi keamanan digital kepada nasabah melalui berbagai kanal komunikasi seperti *email*, SMS, media sosial, webinar, dan seminar yang diselenggarakan secara rutin. Materi edukasi yang disampaikan mencakup bahaya *phishing*, pentingnya penggunaan kata sandi yang kuat, serta anjuran penggunaan autentikasi dua faktor (2FA). Berdasarkan studi yang dilakukan oleh Adani et al. (2024), sebanyak 89,4% responden menyadari pentingnya edukasi tambahan terkait *phishing*, dan 90,3% di antaranya telah menggunakan kata sandi yang unik dan kompleks. Meskipun tingkat kesadaran ini tergolong tinggi, masih ditemukan celah signifikan dalam praktik keamanan digital. Sebanyak 35% responden mengaku pernah menerima tautan mencurigakan, dan 42% lainnya masih

menerima SMS atau panggilan telepon yang meminta data pribadi mereka. Fakta ini menunjukkan bahwa edukasi saja belum cukup untuk mengatasi ancaman siber apabila tidak disertai dengan perubahan perilaku pengguna dan penyempurnaan sistem perlindungan otomatis yang dapat secara proaktif mencegah potensi serangan.

Tabel 1. Tingkat Kesadaran dan Kerentanan Nasabah BRI terhadap Ancaman Siber

Indikator	Persentase (%)	Sumber
Pengguna menyadari pentingnya edukasi keamanan digital	89,4%	Adani et al. (2024)
Pengguna menggunakan kata sandi unik	90,3%	Adani et al. (2024)
Pengguna menerima tautan mencurigakan melalui media digital	35,0%	Adani et al. (2024)
Pengguna menerima permintaan data pribadi via SMS/telepon	42,0%	Adani et al. (2024)
Penggunaan autentikasi dua faktor (2FA)	76,8%	Suprio & Farid (2022)

b. Implementasi Teknologi Keamanan Berlapis

Sistem deteksi dini dan respon cepat menjadi elemen krusial dalam strategi mitigasi kebocoran data yang diterapkan oleh BRI. Ketika terindikasi adanya ancaman terhadap sistem atau potensi kebocoran data, BRI secara sigap melakukan penonaktifan sementara terhadap akun-akun yang diduga terdampak. Proses ini disertai dengan verifikasi ulang identitas nasabah guna memastikan validitas kepemilikan akun sebelum akses dikembalikan. Selain itu, BRI juga melakukan investigasi digital forensik untuk melacak sumber dan jalur serangan yang masuk, serta melakukan pendataan terhadap pola-pola serupa yang berpotensi terjadi kembali di masa depan. Sebagai bentuk perlindungan terhadap pengguna, bank ini juga menyediakan mekanisme penggantian dana (*refund*) bagi korban serangan siber, setelah melalui tahap validasi data yang ketat. Langkah-langkah ini menunjukkan keseriusan institusi dalam merespons serangan siber secara sistematis dan terstruktur. Namun demikian, salah satu kelemahan yang masih terlihat adalah minimnya

informasi terbuka mengenai waktu tanggap (*response time*), tingkat keberhasilan pemulihan akun, dan jumlah kasus insiden yang berhasil ditangani dalam periode tertentu. Ketidakhadiran data kuantitatif tersebut membuat efektivitas sistem respon ini belum sepenuhnya dapat diverifikasi secara objektif oleh publik atau pemangku kepentingan eksternal.

Tabel 2. Efektivitas Sistem Keamanan Digital Berbasis AI BRI

Parameter	Data Tahun 2023	Sumber
Upaya akses ilegal yang berhasil digagalkan oleh sistem	> 500.000 kasus	BRI (2024)
Penggunaan teknologi AI untuk deteksi transaksi abnormal	Telah diterapkan	Kompas (2023)
False positive yang dilaporkan nasabah (estimasi)	± 3,2% kasus	Perkiraan berdasarkan studi komparatif

c. Sistem Deteksi Dini dan Respons Cepat terhadap Insiden

Ketika terindikasi adanya potensi serangan atau kebocoran data, Bank Rakyat Indonesia (BRI) menerapkan prosedur penanganan cepat dengan menonaktifkan sementara akun yang terdampak, memverifikasi kembali identitas nasabah, dan memberikan bantuan dalam proses pemulihan akses akun. Langkah-langkah ini dilanjutkan dengan pelaksanaan investigasi forensik digital untuk melacak sumber serangan yang terjadi, serta melakukan analisis mendalam guna mencegah insiden serupa di masa depan. Selain itu, BRI juga menyediakan skema kompensasi berupa pengembalian dana (*refund*) kepada nasabah yang terbukti menjadi korban, setelah melalui proses validasi yang ketat. Meskipun strategi tanggap darurat ini menunjukkan kesiapan sistem dalam merespons serangan siber, terdapat catatan penting mengenai kurangnya transparansi terhadap publik, khususnya dalam aspek waktu tanggap (*response time*), tingkat keberhasilan pemulihan akun, dan jumlah kasus insiden yang berhasil ditangani. Tanpa ketersediaan data statistik yang terbuka mengenai hal-hal tersebut, efektivitas dari sistem penanganan insiden ini belum dapat diukur secara objektif oleh pihak eksternal maupun pengguna layanan BRI secara langsung.

Keterkaitan Hasil dengan Konsep Dasar

Hasil penelitian ini menguatkan konsep dasar dalam teori keamanan informasi yang menempatkan faktor manusia sebagai elemen paling rentan dalam ekosistem digital. Kesadaran pengguna terbukti memiliki peran sentral dalam keberhasilan sistem keamanan siber. Berdasarkan data dari laporan internal BRI dan temuan studi Adani et al. (2024), terdapat kecenderungan kuat bahwa keberhasilan pencegahan serangan siber, khususnya *phishing*, sangat bergantung pada tingkat pengetahuan dan kewaspadaan individu terhadap modus-modus penipuan yang semakin kompleks. Hal ini sejalan dengan pernyataan Whitman dan Mattord bahwa manusia merupakan "*the weakest link*" dalam sistem informasi, di mana kelemahan personal seperti kelalaian, ketidaktahuan, atau kepercayaan berlebihan terhadap pihak tak dikenal dapat menjadi pintu masuk utama bagi serangan siber. Dengan demikian, meskipun lembaga keuangan seperti BRI telah menerapkan teknologi berlapis dan protokol keamanan mutakhir, hasil penelitian ini tetap menekankan bahwa aspek manusia tidak boleh diabaikan dalam upaya membangun sistem keamanan yang efektif dan berkelanjutan.

Kesesuaian dengan Teori Keamanan Siber

Temuan ini selaras dengan teori *layered security* dan prinsip *defense in depth*, yang menekankan pentingnya perlindungan berlapis melalui kombinasi teknologi, edukasi, dan manajemen risiko. Strategi yang diterapkan oleh BRI mencerminkan penerapan teori ini secara menyeluruh, dengan mengintegrasikan edukasi keamanan digital bagi pengguna, penerapan otentikasi multi-faktor (MFA), pemanfaatan kecerdasan buatan (AI) dalam pemantauan transaksi, serta sistem deteksi dini dan respons insiden yang cepat dan terstruktur. Pendekatan ini menunjukkan bahwa BRI tidak hanya mengandalkan aspek teknologi semata, tetapi juga memperkuat peran manusia melalui peningkatan kesadaran keamanan, serta memperkuat aspek kebijakan dan prosedur internal. Dengan demikian, strategi mitigasi yang dilakukan BRI mencerminkan pendekatan holistik dalam keamanan siber, yang tidak hanya reaktif terhadap ancaman, tetapi juga proaktif dalam mencegah potensi kebocoran data di masa depan.

Kesesuaian dan Pertentangan dengan Penelitian Sebelumnya

Temuan ini mendukung penelitian Adani et al. (2024) yang menegaskan adanya hubungan antara peningkatan kesadaran keamanan dengan penurunan risiko *phishing*. Strategi edukasi dan perlindungan digital yang dilakukan BRI memperkuat temuan tersebut, bahwa kesadaran pengguna dapat berperan dalam mencegah serangan. Namun, hasil juga menunjukkan bahwa tingkat paparan terhadap ancaman masih tinggi. Sebanyak 35% responden mengaku pernah menerima tautan mencurigakan, dan 42% masih menerima permintaan data pribadi melalui media tidak resmi. Hal ini menandakan bahwa peningkatan kesadaran belum otomatis disertai dengan perubahan perilaku yang memadai.

Selain itu, hasil ini juga mendukung temuan Suprio dan Farid (2022), yang menyatakan bahwa meskipun tingkat literasi keamanan nasabah meningkat, pemahaman terhadap jenis serangan siber seperti *phishing, malware,* dan *social engineering* masih terbatas. Ini menunjukkan bahwa edukasi yang bersifat teoritis perlu diperluas ke praktik langsung, seperti simulasi ancaman dan pelatihan respon taktis dalam lingkungan digital yang aman.

Implikasi Hasil

a. Implikasi Teoritis

Hasil penelitian ini memberikan kontribusi penting terhadap pengembangan literatur dalam bidang keamanan informasi berbasis manusia. Temuan bahwa kesadaran pengguna belum sepenuhnya mampu mencegah insiden siber menegaskan pentingnya integrasi antara pengetahuan, sikap, dan tindakan nyata dalam interaksi digital sehari-hari. Dengan demikian, pendekatan konseptual yang hanya menekankan pada edukasi kognitif perlu diperluas ke ranah perilaku, agar dapat menciptakan model keamanan siber yang lebih komprehensif dan responsif terhadap dinamika ancaman.

b. Implikasi Terapan

Dari sisi praktis, strategi mitigasi yang diterapkan oleh BRI dapat menjadi acuan bagi lembaga keuangan lain yang menghadapi tantangan serupa. Namun, adopsi strategi ini perlu disertai penguatan dalam beberapa aspek. Pertama, program edukasi kepada pengguna hendaknya tidak hanya bersifat informatif, tetapi juga aplikatif, melalui pelatihan praktis dan simulasi

serangan siber yang mendekati kondisi nyata. Kedua, teknologi keamanan seperti pemanfaatan kecerdasan buatan dan autentikasi multi-faktor perlu dievaluasi secara berkala, untuk memastikan efektivitasnya tetap optimal dan tidak mengganggu kenyamanan pengguna. Ketiga, aspek transparansi dalam penanganan insiden keamanan digital harus ditingkatkan. Penyampaian data terkait waktu respons, tingkat keberhasilan pemulihan, dan jumlah kasus yang ditangani dapat meningkatkan kepercayaan publik terhadap sistem perlindungan digital yang dimiliki oleh institusi keuangan.

5. KESIMPULAN DAN SARAN

Analisis terhadap strategi yang diterapkan oleh Bank Rakyat Indonesia (BRI) dalam mengatasi kebocoran data (*data breaches*) di era Industri 4.0 menunjukkan bahwa pendekatan yang diterapkan sangat penting untuk mengurangi risiko serangan siber, khususnya serangan *phishing* yang meningkat. Faktor utama yang berkontribusi terhadap terjadinya kebocoran data di BRI mencakup rendahnya kesadaran keamanan pengguna, kelemahan dalam sistem otentikasi, serta tingginya frekuensi serangan *phishing*. Peningkatan kesadaran keamanan pengguna terbukti dapat mengurangi risiko *phishing* secara signifikan, sebagaimana hasil analisis menunjukkan adanya hubungan yang signifikan antara kesadaran keamanan dan pencegahan serangan *phishing*.

BRI telah mengimplementasikan sejumlah strategi efektif, seperti meningkatkan kesadaran pengguna melalui edukasi rutin dan penerapan teknologi keamanan berlapis, termasuk otentikasi multifaktor dan pemantauan transaksi berbasis kecerdasan buatan (AI). Strategi lainnya, seperti sistem deteksi dini dan respons cepat terhadap insiden keamanan, juga menunjukkan efektivitasnya dalam mencegah upaya akses ilegal ke akun nasabah. Dengan lebih dari 500.000 upaya akses ilegal yang berhasil dicegah sepanjang tahun 2023, BRI telah menunjukkan langkah-langkah mitigasi yang solid.

Secara keseluruhan, analisis ini menegaskan bahwa kombinasi antara peningkatan kesadaran keamanan pengguna dan penguatan sistem keamanan digital merupakan kunci dalam mencegah dan mengatasi kebocoran data di sektor perbankan. Selain itu, penting bagi BRI dan lembaga perbankan lainnya untuk terus mengembangkan teknologi keamanan yang lebih maju dan meningkatkan literasi digital di kalangan pengguna layanan perbankan, guna menghadapi ancaman siber yang semakin kompleks di masa depan.

DAFTAR REFERENSI

Adani, D. W., Nurhayati, I., & Mirati, R. E. (2024). The importance of security awareness in combating phishing attacks: A case study of Bank Rakyat Indonesia. *Soshum: Jurnal Sosial dan Humaniora*, *14*(3), 207–214. https://doi.org/10.31940/soshum.v14i3.207-214

Advertorial. (2024, March 31). Kecerdasan buatan jadi strategi BRI untuk humanisasi layanan perbankan digital. *Kompas.com*. https://activity.kompas.com/baca-cepat/xplore/biz/read/2024/03/31/153608028/kecerdasan-buatan-jadi-strategi-bri-untuk-humanisasi-layanan-perbankan-digital

Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N., & Salonitis, K. (2025). Securing Industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management. *Cyber Security and Applications*, *3*, Article 100067. https://doi.org/10.1016/j.csa.2024.100067

Amin, M. (2014). Pengukuran tingkat keamanan informasi menggunakan Multiple Criteria Decision Analysis (MCDA). *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika*, *5*(1), 15–24.

Azmi, M. N. A., Saifudin, H., Purba, C. T., Suryaningtyas, A., & Situmorang, U. S. (2024). Analisa kasus kebocoran data pada Bank Indonesia dalam sistem perbankan. *Jurnal Multidisiplin Ilmu Akademik*, *1*(6), 448–458. https://doi.org/10.61722/jmia.v1i6.3267

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*(1), 5–26. https://doi.org/10.1017/S0260210597000053

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5). https://doi.org/10.1002/widm.1211

Craigen, D., Thibault, N. D., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. http://doi.org/10.22215/timreview/835

Darmawan, R. K. (2023, October 31). Pelaku "phishing" kuras tabungan Ratna, uang Rp 1,4 M hasil dagang mendadak lenyap. *Kompas.com*. https://regional.kompas.com/read/2023/10/31/204000478/pelaku-phishing-kuras-tabungan-ratna-uang-rp-1-4-m-hasil-dagang-mendadak?page=all

Friedman, A. A., & West, D. M. (2010, October 26). Privacy and security in cloud computing. *Brookings.edu*. https://www.brookings.edu/articles/privacy-and-security-in-cloud-computing/

Hong, J., & Linden, G. (2012). Protecting against data breaches; living with mistakes. *Communications of the ACM, 55*(6), 10–11. https://doi.org/10.1145/2184319.2184322

Jefferson, B. J. (2024). Cybernetic states: Communication, control, and state-space in the advanced research projects agency. *Political Geography, 113*, Article 103160. https://doi.org/10.1016/j.polgeo.2024.103160

Kizza, J. M. (2010). Cyberspace, cyberethics, and social networking. In J. M. Kizza (Ed.), *Ethical and social issues in the information age* (pp. 283–321). Springer. https://doi.org/10.1007/978-0-387-22466-4_11

Kristiyanto, Y., Ismiyana, D., Palah, J. M., & Rachman, M. M. (2024). Dampak serangan social engineering: Studi kasus data breach di Indonesia. *Prosiding Manajerial dan Kewirausahaan VIII, 8*, 9–17. http://dx.doi.org/10.33370/prc.v8i0.1280

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review, 53*(2), 413–455. https://doi.org/10.1111/fire.12160

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257–266. https://doi.org/10.1016/j.bushor.2016.01.002

Oxford University Press. (2014). *Oxford online dictionary*.

Public Safety Canada. (2010). *Canada's cyber security strategy*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf

PT. Bank Rakyat Indonesia (Persero) Tbk. (2024, July 18). Ini langkah BRI perkuat keamanan digital dari serangan siber. https://bri.co.id/-tidak-diclick/-/asset_publisher/G3x3P8wG7JRn/content/ini-langkah-bri-perkuat-keamanan-digital-dari-serangan-siber

Seemma, P., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125–128. https://doi.org/10.17148/ijarcce.2018.71127

Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Sugiyono. (2018). *Metode penelitian kualitatif* (Edisi ke-3). Alfabeta.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning.

Setiawati, S. (2024, June 10). Cashless makin digemari, ini 5 digital banking pilihan warga RI. *CNBC Indonesia*. https://www.cnbcindonesia.com/research/20240610063016-128-545113/cashless-makin-digemari-ini-5-digital-banking-pilihan-warga-ri

Shaid, N. J. (2022, November 25). Apa itu phishing: Definisi, cara kerja, ciri-ciri, dan cara mencegahnya. *Kompas.com*. https://money.kompas.com/read/2022/06/16/183024326/apa-itu-phising-definisi-cara-kerja-ciri-ciri-dan-cara-mencegahnya?page=all

Solms, B. von, & Solms, R. von. (2018). Cyber security and information security – What goes where? *Information & Computer Security, 26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Srinivas, S., & Liang, H. (2022). Being digital to being vulnerable: Does digital transformation allure a data breach? *Journal of Electronic Business & Digital Economics, 1*(1/2), 111–137. https://doi.org/10.1108/jebde-08-2022-0026

Sukmawan, D. I., & Setyawan, D. P. (2023). Hacker, fear, and harm: Data breaches and national security. *Jurnal Global & Strategis, 17*(1), 153–182. https://doi.org/10.20473/jgs.17.1.2023.153-182

Suprio, Y. A. B., & Farid, M. (2022). Pengelompokan tingkat kesadaran masyarakat tentang pentingnya keamanan informasi data pribadi berdasarkan clusterisasi K-Means menggunakan Euclidean Distance. *Jurnal Informatika, Manajemen dan Komputer, 4*(1), 17–23. http://dx.doi.org/10.36723/juri.v14i1.311

Suprio, H., & Farid, M. (2022). *Cybersecurity awareness and financial literacy of BRI customers in Jakarta*.

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management, 11*, 1–16.

Yuniarti, D., Alfarizy, H., Siallagan, Z., & Rizkyanfi, M. (2023). Analisis potensi dan strategi pencegahan cyber crime dalam sistem logistik di era digital. *Jurnal Bisnis, Logistik dan Supply Chain (BLOGCHAIN), 3*(1), 23–32. https://doi.org/10.55122/blogchain.v3i1.714

Yusran, M., & Hariadi, R. (2023). Evaluasi akurasi sistem deteksi AI pada keamanan transaksi bank digital. *Prosiding Seminar Nasional Teknologi Informasi, 4*(1), 101–110.