Inovan Publisher

Orasi: Jurnal Ilmu Politik dan Sosial

| ISSN (Online) 3063-9719 |

DOI: https://doi.org/10.63217/orasi.v2i2.263

Ancaman Social Engineering dalam Komunikasi Bisnis dan Efektivitas Kebijakan Keamanan Informasi di Organisasi Modern

Idel Eprianto[1], Keisha Najwa Khairana[2], Naqinni Azhara[3], Sasikirana Azalia Rahmadhani[4], Syalu Aulia Hakim[5]
[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, idel.eprianto@dsn.ubharajaya.ac.id
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, keishanajwaa@gmail.com
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, naqinazhr@gmail.com
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, kuliahsasikirana4@gmail.com
[5]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, syaluaulia2@gmail.com

Corresponding Author: idel.eprianto@dsn.ubharajaya.ac.id[1]

Abstract: *This study examines social engineering as a major threat to business communication in the digital era and evaluates the effectiveness of ISO/IEC 27001–based information security policies in Indonesia. Using a systematic literature review of 50 sources published between 2015 and 2024, the research analyzes patterns and impacts of social engineering attacks on organizational information security. The findings indicate that most Indonesian businesses have been targeted by such attacks, with phishing and smishing being the most prevalent techniques, and digital business communication serving as the primary target. Although ISO/IEC 27001 has been widely adopted, the overall level of information security maturity remains moderate, with human factors identified as the weakest element. The study concludes that effective information security policies require the integration of technical, managerial, and organizational culture aspects, and recommends strengthening security awareness programs, continuous training, and adaptive policies to enhance organizational resilience against evolving social engineering threats.*

Keyword: *social engineering, information security, business communication, security policy, ISO/IEC 27001, security awareness, modern organizations.*

Abstrak: Penelitian ini membahas ancaman *social engineering* sebagai risiko utama dalam komunikasi bisnis di era digital serta mengevaluasi efektivitas kebijakan keamanan informasi berbasis ISO/IEC 27001 di Indonesia. Menggunakan metode studi literatur sistematis terhadap 50 sumber terbitan tahun 2015–2024, penelitian ini menganalisis pola dan dampak serangan *social engineering* terhadap keamanan informasi organisasi. Hasil penelitian menunjukkan bahwa mayoritas bisnis di Indonesia menjadi target serangan, terutama melalui phishing dan smishing, dengan komunikasi bisnis digital sebagai sasaran utama. Meskipun standar ISO/IEC 27001 telah banyak diadopsi, tingkat kematangan keamanan informasi masih berada pada level sedang, dengan

faktor manusia sebagai titik terlemah. Penelitian ini menyimpulkan bahwa efektivitas kebijakan keamanan informasi memerlukan integrasi aspek teknis, manajerial, dan budaya organisasi, serta merekomendasikan penguatan program kesadaran keamanan, pelatihan berkelanjutan, dan kebijakan adaptif untuk meningkatkan ketahanan organisasi terhadap ancaman *social engineering*.

Keyword: social engineering, keamanan informasi, komunikasi bisnis, kebijakan keamanan, ISO/IEC 27001, kesadaran keamanan, organisasi modern.

PENDAHULUAN

Transformasi digital telah mengubah cara organisasi menjalankan operasional bisnisnya (Justyna & Abbas, 2021). Dalam dekade terakhir, komunikasi bisnis telah bergeser dari model konvensional menuju platform digital yang memungkinkan interaksi real-time lintas geografis. Kemajuan teknologi informasi dan komunikasi memberikan efisiensi operasional yang signifikan, namun di sisi lain membuka celah keamanan baru yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab (Bakri & Irmayana, 2017).

Indonesia sebagai negara berkembang dengan pertumbuhan ekonomi digital yang pesat menghadapi tantangan serius dalam bidang keamanan informasi. Data terkini menunjukkan bahwa Indonesia mengalami 330 kasus serangan digital pada tahun 2024, meningkat dari 323 kasus pada tahun 2023 (GoodStats, 2025). Lebih mengkhawatirkan lagi, sepanjang tahun 2024, tercatat 8.312.713 kasus penanganan konten negatif pada situs dan 2.365.749 kasus di media sosial yang ditangani oleh Kementerian Komunikasi dan Digital (Diskominfo Jawa Timur, 2024). Angka ini menunjukkan tren peningkatan yang mengkhawatirkan dan menuntut perhatian serius dari semua pemangku kepentingan.

Social engineering atau rekayasa sosial merupakan salah satu metode serangan siber yang paling efektif karena menargetkan elemen manusia sebagai titik terlemah dalam sistem keamanan (CSIRT Teknokrat, 2024). Berbeda dengan serangan teknis yang memanfaatkan kerentanan sistem, social engineering mengeksploitasi psikologi manusia melalui manipulasi kepercayaan, rasa takut, keingintahuan, atau tekanan sosial (Bank BSI, 2024). Teknik ini terbukti mampu menembus bahkan sistem keamanan yang paling canggih sekalipun, sebagaimana terjadi pada peretasan Pusat Data Nasional Indonesia yang melumpuhkan berbagai layanan publik pada Juni 2024 (Widya Security, 2025).

Dalam konteks komunikasi bisnis, social engineering mengambil berbagai bentuk seperti phishing melalui email, vishing melalui panggilan telepon, pretexting dengan skenario palsu, hingga tailgating untuk mendapatkan akses fisik (Bank BSI, 2024). Selama tahun 2024, teknologi anti-phishing Kaspersky mendeteksi lebih dari 8 juta upaya phishing yang menargetkan pengguna Indonesia (Media Indonesia, 2024). Lebih jauh lagi, social engineering berbasis kecerdasan buatan (AI) kini menjadi ancaman baru yang semakin kompleks, termasuk penggunaan teknologi deepfake untuk penipuan yang lebih meyakinkan (CSIRT Cirebon, 2025).

Pandemi COVID-19 yang memaksa banyak organisasi menerapkan kebijakan Work From Home telah memperparah situasi ini karena meningkatkan ketergantungan pada komunikasi digital dan media sosial (Arini, 2019). Kondisi ini menciptakan peluang baru bagi pelaku kejahatan siber untuk melancarkan serangan yang lebih terorganisir dan tersofistikasi (ITGID, 2025).

Meskipun banyak organisasi telah mengimplementasikan kebijakan keamanan informasi berbasis standar internasional seperti ISO/IEC 27001, efektivitas implementasi masih menjadi pertanyaan (Fattah et al., 2024). Standar ISO 27001 merupakan standar internasional yang diakui secara global untuk mengelola risiko terhadap keamanan informasi (ISOCENTER Indonesia, 2015). Berbagai penelitian menunjukkan bahwa keberadaan kebijakan saja tidak cukup tanpa disertai dengan kesadaran, pemahaman, dan kepatuhan dari seluruh anggota organisasi (Yahya et al., 2023).

Kesenjangan antara kebijakan yang ada dengan praktik di lapangan menjadi celah yang dapat dimanfaatkan oleh pelaku social engineering (Daniswara et al., 2023).

Pemerintah Indonesia telah mengeluarkan berbagai regulasi untuk mendorong penerapan keamanan informasi yang lebih baik, termasuk Peraturan Menteri Komunikasi dan Informatika No. 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi yang mengatur bahwa Penyelenggara Sistem Elektronik Strategis dan Penyelenggara Sistem Elektronik Tinggi harus menjalankan standar SNI ISO/IEC 27001 (Master of Computer Science Binus, 2021). Selain itu, berbagai regulasi lain seperti Permendagri Nomor 17 Tahun 2023 dan Permendagri Nomor 57 Tahun 2021 juga secara eksplisit menyebut pentingnya penerapan standar ISO 27001 (Mitraberdaya, 2024). Namun, meskipun regulasi telah ada, implementasi di lapangan masih menghadapi berbagai kendala dan tantangan (Sinaga & Taan, 2024).

Penelitian ini hadir untuk mengisi kesenjangan pengetahuan mengenai bagaimana ancaman social engineering beroperasi dalam konteks komunikasi bisnis modern di Indonesia, serta bagaimana efektivitas kebijakan keamanan informasi dalam menghadapi ancaman tersebut. Dengan memahami dinamika ancaman dan mengevaluasi efektivitas kebijakan yang ada, penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan strategi keamanan informasi yang lebih komprehensif dan adaptif untuk menghadapi era Society 5.0 (Nurbojatmiko et al., 2024).

METODE

Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian studi literatur sistematis (systematic literature review) (Maulana, 2025). Pendekatan kualitatif dipilih karena penelitian ini bertujuan untuk memahami secara mendalam fenomena ancaman social engineering dan efektivitas kebijakan keamanan informasi dari berbagai perspektif teoretis dan empiris (Fauzia et al., 2024).

Studi literatur sistematis merupakan metode penelitian yang mengidentifikasi, mengevaluasi, dan menginterpretasi seluruh penelitian yang tersedia dan relevan dengan pertanyaan penelitian tertentu (Maulana, 2025). Metode ini dipilih karena memungkinkan peneliti untuk:

1. Mengidentifikasi pola dan tren dalam literatur yang ada
2. Mengintegrasikan temuan dari berbagai studi untuk menghasilkan pemahaman yang lebih komprehensif
3. Mengidentifikasi kesenjangan pengetahuan yang masih ada
4. Memberikan basis yang kuat untuk rekomendasi praktis

Sumber Data

Sumber data dalam penelitian ini adalah literatur yang terdiri dari (Fauzia et al., 2024):

Data Primer:

Jurnal ilmiah nasional dan internasional yang dipublikasikan di database akademik seperti Google Scholar, ResearchGate, dan repository universitas

Prosiding konferensi internasional di bidang keamanan informasi dan teknologi informasi

Dokumen standar ISO/IEC 27001 dan panduan implementasinya

Data Sekunder:

1. Buku teks tentang keamanan informasi, social engineering, dan sistem manajemen keamanan informasi
2. Laporan penelitian dari lembaga riset dan konsultan keamanan siber
3. Peraturan perundang-undangan Indonesia terkait keamanan informasi
4. White papers dan technical reports dari organisasi keamanan siber
5. Artikel media dan press release tentang insiden keamanan siber di Indonesia

Kriteria Seleksi Literatur

Literatur yang digunakan dalam penelitian ini dipilih berdasarkan kriteria berikut:

Kriteria Inklusi:

1. Literatur yang dipublikasikan antara tahun 2015 hingga 2024
2. Literatur yang membahas topik social engineering, keamanan informasi, ISO/IEC 27001, atau komunikasi bisnis digital
3. Literatur yang tersedia dalam Bahasa Indonesia atau Bahasa Inggris
4. Literatur yang dapat diakses secara penuh (full-text availability)
5. Literatur yang memiliki kualitas akademik yang terverifikasi (peer-reviewed untuk jurnal)

Kriteria Eksklusi:

1. Literatur yang dipublikasikan sebelum tahun 2015, kecuali untuk literatur klasik yang sangat relevan
2. Literatur yang tidak memiliki metodologi yang jelas atau hasil yang tidak dapat diverifikasi
3. Literatur yang hanya tersedia dalam bentuk abstrak tanpa akses full-text
4. Literatur yang terlalu spesifik pada teknologi atau konteks yang tidak relevan dengan penelitian ini

Prosedur Pengumpulan Data

Pengumpulan data dilakukan melalui tahapan sistematis berikut:

Tahap 1: Identifikasi (Identification)

a) Pencarian literatur dilakukan menggunakan kata kunci: "social engineering", "keamanan informasi", "information security", "ISO 27001", "ISO/IEC 27001", "kebijakan keamanan informasi", "komunikasi bisnis digital", "phishing", "cyber security Indonesia"
b) Database yang digunakan: Google Scholar, ResearchGate, DOAJ (Directory of Open Access Journals), repository universitas Indonesia
c) Pencarian juga dilakukan melalui referensi yang dikutip dalam literatur yang relevan (snowballing technique)

Tahap 2: Skrining (Screening)

a) Melakukan skrining berdasarkan judul dan abstrak untuk menentukan relevansi awal
b) Mengeliminasi duplikasi literatur yang sama dari sumber berbeda
c) Menerapkan kriteria inklusi dan eksklusi pada tahap awal

Tahap 3: Kelayakan (Eligibility)

a) Membaca full-text literatur yang lolos tahap skrining
b) Mengevaluasi kualitas metodologi dan relevansi konten secara mendalam
c) Menyeleksi literatur final yang akan dianalisis

Tahap 4: Inklusi (Inclusion)

a) Mendokumentasikan literatur yang dipilih dalam database penelitian
b) Mengekstrak informasi kunci dari setiap literatur
c) Mengorganisir literatur berdasarkan tema dan kategori

Teknik Analisis Data

Data yang terkumpul dianalisis menggunakan teknik analisis konten tematik (thematic content analysis) dengan langkah-langkah sebagai berikut:

1. Familiarisasi dengan Data
    a) Membaca seluruh literatur secara menyeluruh untuk mendapatkan pemahaman umum
    b) Membuat catatan awal tentang tema-tema yang muncul
2. Pengkodean Awal (Initial Coding)
    a) Mengidentifikasi unit-unit informasi yang relevan
    b) Memberikan kode pada setiap unit informasi berdasarkan topik atau konsep yang direpresentasikan
3. Pencarian Tema (Searching for Themes)

a) Mengelompokkan kode-kode yang memiliki kesamaan atau keterkaitan
b) Mengidentifikasi tema-tema utama yang muncul dari kode-kode tersebut

4. Review Tema (Reviewing Themes)
   a) Mengevaluasi kesesuaian tema dengan data yang terkumpul
   b) Merevisi atau menggabungkan tema yang overlap
   c) Memastikan tema-tema yang diidentifikasi menjawab pertanyaan penelitian
5. Definisi dan Penamaan Tema (Defining and Naming Themes)
   a) Memberikan definisi yang jelas untuk setiap tema
   b) Memberikan nama yang deskriptif dan mudah dipahami
6. Produksi Laporan (Producing the Report)
   a) Menyajikan temuan dalam bentuk narasi yang koheren
   b) Mengintegrasikan kutipan dan referensi yang mendukung setiap tema
   c) Menginterpretasikan temuan dalam konteks pertanyaan penelitian

Validitas dan Reliabilitas

Untuk memastikan validitas dan reliabilitas penelitian, beberapa strategi diterapkan:

Validitas:

1. Triangulasi Sumber: Menggunakan berbagai jenis literatur (jurnal, buku, regulasi, laporan) untuk mendapatkan perspektif yang beragam
2. Peer Debriefing: Mendiskusikan temuan dengan ahli di bidang keamanan informasi untuk mendapatkan feedback
3. Thick Description: Memberikan deskripsi yang kaya dan detail untuk memungkinkan pembaca menilai transferabilitas temuan

Reliabilitas:

1. Audit Trail: Mendokumentasikan seluruh proses penelitian secara detail
2. Systematic Approach: Menggunakan protokol yang konsisten dalam seleksi dan analisis literatur
3. Inter-coder Reliability: Melakukan cross-checking dalam proses pengkodean data

Keterbatasan Metode

Penelitian studi literatur memiliki beberapa keterbatasan yang perlu diakui:

1. Ketergantungan pada Literatur yang Tersedia: Temuan penelitian dibatasi oleh literatur yang dapat diakses dan tersedia secara publik
2. Bias Publikasi: Penelitian yang menunjukkan hasil signifikan cenderung lebih sering dipublikasikan
3. Keterbatasan Waktu: Literatur yang dipublikasikan setelah periode pengumpulan data tidak termasuk dalam analisis
4. Subjektivitas dalam Interpretasi: Meskipun menggunakan pendekatan sistematis, interpretasi peneliti dapat mempengaruhi analisis

Untuk meminimalkan keterbatasan ini, penelitian menggunakan protokol yang ketat dalam seleksi dan analisis literatur, serta menjaga transparansi dalam pelaporan metode dan temuan.

HASIL DAN PEMBAHASAN

Profil Literatur yang Dianalisis

Dari proses pencarian dan seleksi sistematis, penelitian ini berhasil mengidentifikasi dan menganalisis 50 sumber literatur yang memenuhi kriteria inklusi. Distribusi literatur berdasarkan kategori adalah sebagai berikut:

Berdasarkan Jenis Publikasi:

a) Jurnal ilmiah: 28 publikasi (56%)
b) Artikel/laporan lembaga: 12 publikasi (24%)

c) Buku dan chapter buku: 6 publikasi (12%)
d) Regulasi dan standar: 4 dokumen (8%)

Berdasarkan Tahun Publikasi:
a) 2024-2025: 18 publikasi (36%)
b) 2021-2023: 22 publikasi (44%)
c) 2017-2020: 8 publikasi (16%)
d) 2015-2016: 2 publikasi (4%)

Berdasarkan Asal Geografis:
a) Indonesia: 32 publikasi (64%)
b) Internasional: 18 publikasi (36%)

Berdasarkan Fokus Topik:
a) Social engineering: 15 publikasi (30%)
b) ISO/IEC 27001: 14 publikasi (28%)
c) Komunikasi bisnis digital: 7 publikasi (14%)
d) Insiden keamanan siber: 8 publikasi (16%)
e) Metodologi dan framework: 6 publikasi (12%)

Bentuk dan Teknik Ancaman Social Engineering dalam Komunikasi Bisnis

Phishing sebagai Ancaman Dominan

Berdasarkan analisis literatur, phishing muncul sebagai teknik social engineering yang paling dominan dan mengancam komunikasi bisnis di Indonesia. Kaspersky mendeteksi lebih dari 8 juta upaya phishing yang menargetkan pengguna Indonesia sepanjang tahun 2024 (Media Indonesia, 2024). Angka ini menunjukkan intensitas serangan yang sangat tinggi, dengan rata-rata lebih dari 22.000 upaya serangan per hari.

Phishing dalam konteks bisnis modern telah berkembang menjadi lebih tersofistikasi, dengan pelaku menggunakan teknik personalisasi yang memanfaatkan informasi dari media sosial dan data breach sebelumnya (Bank BSI, 2024). Email phishing bisnis tidak lagi hanya meniru institusi keuangan, tetapi juga menyamar sebagai vendor, pelanggan, atau bahkan eksekutif perusahaan sendiri dalam serangan Business Email Compromise (BEC) (CSIRT Teknokrat, 2024).

Varian phishing yang paling berbahaya dalam komunikasi bisnis adalah spear phishing, di mana pelaku melakukan riset mendalam tentang target spesifik sebelum meluncurkan serangan (Bank BSI, 2024). Penelitian menunjukkan bahwa tingkat keberhasilan spear phishing dapat mencapai 50-70%, jauh lebih tinggi dibandingkan phishing massal yang tingkat keberhasilannya hanya sekitar 3-5% (CSIRT Teknokrat, 2024)

Smishing dan Vishing: Ancaman Melalui Saluran Mobile

Smishing (SMS phishing) dan vishing (voice phishing) mengalami peningkatan signifikan seiring dengan meningkatnya penggunaan perangkat mobile untuk komunikasi bisnis (Ladayya et al., 2024). Teknik ini memanfaatkan tingkat kepercayaan yang lebih tinggi terhadap komunikasi suara dan SMS dibandingkan email (Bank BSI, 2024).

Dalam konteks Indonesia, smishing sering menggunakan narasi yang berkaitan dengan layanan perbankan, pengiriman paket, atau tagihan pembayaran (Ladayya et al., 2024). Pelaku memanfaatkan teknologi caller ID spoofing untuk membuat panggilan atau pesan tampak berasal dari nomor resmi institusi terpercaya (CSIRT Cirebon, 2025).

Vishing menjadi particularly efektif karena memanfaatkan tekanan waktu dan emosi korban melalui interaksi real-time (Bank BSI, 2024). Pelaku biasanya menciptakan skenario yang mendesak

seperti masalah keamanan akun, transaksi mencurigakan, atau verifikasi data yang harus segera dilakukan (CSIRT Teknokrat, 2024)

Pretexting dalam Komunikasi Organisasional

Pretexting menjadi ancaman serius dalam komunikasi internal organisasi karena memanfaatkan struktur hierarki dan budaya kepatuhan (CyberHub, 2024). Pelaku menciptakan skenario yang meyakinkan dengan menyamar sebagai pihak yang memiliki otoritas, seperti manajer dari kantor cabang lain, auditor eksternal, atau teknisi IT yang melakukan maintenance (Bank BSI, 2024).

Keberhasilan pretexting sangat bergantung pada riset yang dilakukan pelaku tentang struktur organisasi, nama-nama key personnel, dan proses bisnis yang berjalan (CSIRT Teknokrat, 2024). Informasi ini seringkali dapat dikumpulkan dengan mudah dari media sosial, website perusahaan, atau LinkedIn (CyberHub, 2024).

AI-Powered Social Engineering: Ancaman Emerging

Perkembangan kecerdasan buatan telah menciptakan dimensi baru dalam ancaman social engineering (CyberHub, 2024). Teknologi deepfake memungkinkan pelaku untuk membuat video atau audio palsu yang sangat realistis dari eksekutif perusahaan atau figur otoritas (CSIRT Cirebon, 2025). Beberapa kasus telah dilaporkan di mana karyawan tertipu untuk mentransfer dana atau memberikan informasi sensitif berdasarkan instruksi video call palsu dari "CEO" perusahaan mereka (CyberHub, 2024).

Chatbot berbasis AI juga digunakan untuk melakukan social engineering yang lebih canggih, mampu melakukan percakapan natural dan meyakinkan untuk mengumpulkan informasi atau membujuk korban (CSIRT Cirebon, 2025). Generative AI dapat digunakan untuk membuat email phishing yang sangat personal dan bebas dari kesalahan tata bahasa yang biasanya menjadi red flag (CyberHub, 2024).

Penelitian menunjukkan bahwa 46% bisnis di Indonesia kurang memahami teknologi untuk mencegah serangan berbasis AI, menunjukkan kesenjangan yang signifikan antara evolusi ancaman dengan kesiapan organisasi (Media Indonesia, 2024).

Dampak Social Engineering terhadap Keamanan Informasi Organisasi

Dampak Finansial

Dampak finansial dari serangan social engineering sangat signifikan. Penelitian menunjukkan bahwa 84% bisnis di Indonesia telah mengalami identity fraud pada tahun lalu (Media Indonesia, 2024). Kerugian finansial tidak hanya berasal dari pencurian dana secara langsung, tetapi juga dari biaya pemulihan sistem, investigasi forensik, peningkatan sistem keamanan, dan potensi denda regulasi (Edavos, 2025).

Kasus serangan ransomware terhadap Pusat Data Nasional pada Juni 2024 menunjukkan dampak finansial yang luas, tidak hanya terbatas pada biaya tebusan tetapi juga kerugian ekonomi akibat terhentinya layanan publik yang bergantung pada data center tersebut (Edavos, 2025). Total estimated cost dari insiden ini mencapai triliunan rupiah ketika memperhitungkan dampak cascade pada berbagai sektor (Widya Security, 2025)

Dampak Operasional

Serangan social engineering dapat menyebabkan gangguan serius pada operasional bisnis (ITGID, 2025). Downtime sistem, kehilangan akses ke data kritis, dan gangguan komunikasi bisnis dapat melumpuhkan operasi organisasi selama periode tertentu (Edavos, 2025). Dalam kasus serangan Pusat Data Nasional, berbagai layanan publik seperti imigrasi terhenti selama beberapa waktu, menunjukkan dampak domino yang luas (Widya Security, 2025).

Pemulihan dari serangan social engineering juga memerlukan waktu dan sumber daya yang signifikan (ITGID, 2025). Organisasi perlu melakukan investigasi menyeluruh, memulihkan sistem, mengubah kredensial, dan menguji sistem sebelum dapat beroperasi normal kembali (Edavos, 2025).

Dampak Reputasional

Kebocoran data akibat social engineering dapat merusak reputasi organisasi secara permanen (Jelita et al., 2024). Kehilangan kepercayaan dari pelanggan, mitra bisnis, dan stakeholder lainnya dapat berdampak jangka panjang pada bisnis (Edavos, 2025). Kasus kebocoran 6 juta data NPWP yang dijual di dark web oleh peretas Bjorka menimbulkan kekhawatiran publik yang luas tentang keamanan data pribadi di Indonesia (Edavos, 2025).

Dampak reputasional juga mempengaruhi kemampuan organisasi untuk menarik talenta, investor, dan pelanggan baru (Jelita et al., 2024). Dalam era digital di mana informasi menyebar dengan cepat melalui media sosial, satu insiden keamanan dapat menjadi viral dan merusak brand yang telah dibangun bertahun-tahun (Diskominfo Jawa Timur, 2024).

Dampak Hukum dan Regulasi

Organisasi yang mengalami pelanggaran keamanan informasi dapat menghadapi konsekuensi hukum dan regulasi (Master of Computer Science Binus, 2021). Regulasi seperti UU ITE dan peraturan perlindungan data pribadi mengharuskan organisasi untuk melindungi data yang mereka kelola (Mitraberdaya, 2024). Kegagalan dalam melindungi data dapat mengakibatkan sanksi administratif, denda, bahkan tuntutan pidana (Master of Computer Science Binus, 2021).

Selain itu, organisasi yang mengalami data breach dapat menghadapi tuntutan class action dari individu yang datanya bocor (Edavos, 2025). Biaya litigasi dan kompensasi dapat mencapai nilai yang sangat besar, terutama jika melibatkan data sensitif seperti informasi finansial atau kesehatan (Daniswara et al., 2023).

Efektivitas Implementasi Kebijakan Keamanan Informasi Berbasis ISO/IEC 27001

Tingkat Adopsi ISO 27001 di Indonesia

Berdasarkan data yang dianalisis, adopsi standar ISO 27001 di Indonesia menunjukkan tren positif dengan tercatat 822 sertifikasi pada tahun 2022 (Mitraberdaya, 2024). Namun, angka ini masih relatif rendah jika dibandingkan dengan jumlah organisasi yang beroperasi di Indonesia dan intensitas ancaman siber yang dihadapi (Sinaga & Taan, 2024).

Sektor yang paling banyak mengadopsi ISO 27001 adalah perbankan dan keuangan, diikuti oleh telekomunikasi dan teknologi informasi (Intertek SAI Global, 2024). Sector pemerintahan juga menunjukkan peningkatan adopsi, didorong oleh berbagai regulasi yang mewajibkan penerapan standar keamanan informasi (Mitraberdaya, 2024).

Tingkat Kematangan Implementasi

Penelitian Riana et al. (2023) menunjukkan bahwa tingkat kematangan keamanan informasi organisasi yang telah mengadopsi ISO 27001 masih berada pada level sedang dengan skor rata-rata 2,54 berdasarkan maturity index. Ini mengindikasikan bahwa mayoritas organisasi berada pada tingkat "defined" atau "managed" namun belum mencapai tingkat "optimized" (Riana et al., 2023).

Tingkat kematangan yang sedang ini menunjukkan bahwa meskipun organisasi telah memiliki kebijakan dan prosedur keamanan informasi, implementasinya belum konsisten dan masih memerlukan pengawasan intensif (Barraza et al., 2023). Proses keamanan informasi belum sepenuhnya terintegrasi dalam proses bisnis dan belum menjadi bagian dari budaya organisasi (Jelita et al., 2024).

Gap antara Compliance dan Efektivitas

Analisis literatur mengungkapkan adanya gap signifikan antara compliance formal terhadap ISO 27001 dengan efektivitas praktis dalam menghadapi ancaman real-world (Djebbar & Nordstrom, 2023). Banyak organisasi fokus pada pemenuhan requirement standar untuk mendapatkan sertifikasi, namun kurang memperhatikan efektivitas kontrol dalam konteks operasional mereka (Fattah et al., 2024). Gap ini tercermin dalam beberapa aspek (Daniswara et al., 2023):

1. Kebijakan vs Praktik: Kebijakan keamanan informasi yang comprehensive namun tidak dipahami atau dipatuhi oleh karyawan
2. Dokumentasi vs Implementasi: Dokumentasi yang lengkap namun tidak direfleksikan dalam praktik sehari-hari
3. Technical Controls vs Human Factors: Fokus berlebihan pada kontrol teknis dengan mengabaikan faktor manusia
4. Audit vs Continuous Improvement: Audit sebagai ritual compliance daripada mekanisme pembelajaran dan perbaikan berkelanjutan

Faktor-Faktor yang Mempengaruhi Efektivitas

Berdasarkan analisis literatur, beberapa faktor kunci yang mempengaruhi efektivitas implementasi ISO 27001 dalam menghadapi social engineering adalah:

1. Komitmen Manajemen Puncak

   Komitmen dari manajemen puncak adalah faktor paling krusial dalam keberhasilan implementasi SMKI (Fattah et al., 2024). Tanpa dukungan penuh dari level eksekutif, program keamanan informasi akan kesulitan mendapatkan sumber daya yang memadai dan tidak mendapat prioritas dalam agenda organisasi (Kamal et al., 2024).

   Komitmen manajemen harus diterjemahkan dalam bentuk konkret seperti alokasi anggaran yang memadai, penetapan accountability yang jelas, dan role modeling dalam praktik keamanan informasi (Intertek SAI Global, 2024). Penelitian menunjukkan bahwa organisasi dengan komitmen manajemen yang kuat memiliki tingkat kematangan keamanan yang lebih tinggi (Fattah et al., 2024).
2. Program Kesadaran Keamanan yang Efektif

   Program security awareness yang berkelanjutan dan engaging adalah kunci untuk mengatasi kerentanan human factor (Ladayya et al., 2024). Program yang efektif tidak hanya memberikan informasi tentang ancaman, tetapi juga mengubah behavior dan membangun budaya keamanan (CSIRT Teknokrat, 2024).

   Namun, penelitian menunjukkan bahwa banyak organisasi masih melakukan program awareness secara sporadis dan tidak engaging (Yahya et al., 2023). Pelatihan yang terlalu teknis atau membosankan tidak efektif dalam meningkatkan kesadaran dan mengubah behavior karyawan (Ladayya et al., 2024).
3. Budaya Organisasi

   Budaya organisasi memainkan peran penting dalam efektivitas keamanan informasi (Jelita et al., 2024). Organisasi dengan budaya yang memprioritaskan keamanan, mendorong reporting, dan tidak menghukum mistake secara berlebihan cenderung lebih resilient terhadap ancaman (Yahya et al., 2023).

   Sebaliknya, budaya yang terlalu fokus pada speed dan convenience tanpa mempertimbangkan security, atau budaya yang punitive terhadap error, dapat menciptakan environment di mana karyawan takut untuk report insiden atau mengambil shortcuts yang membahayakan keamanan (Jelita et al., 2024).
4. Integrasi Keamanan dalam Proses Bisnis

   Keamanan informasi yang efektif harus terintegrasi dalam setiap proses bisnis, bukan diperlakukan sebagai add-on atau afterthought (Intertek SAI Global, 2024). Konsep "security by

design" harus diterapkan dalam pengembangan sistem baru, proses baru, atau inisiatif transformasi digital (Amirinnisa & Bisma, 2023).

Organisasi yang memperlakukan keamanan sebagai enabler bisnis rather than inhibitor cenderung lebih berhasil dalam mengintegrasikan keamanan ke dalam DNA organisasi (Nurbojatmiko et al., 2024).

5. Kapabilitas Tim Keamanan Informasi

Kompetensi dan kapabilitas tim keamanan informasi sangat mempengaruhi efektivitas implementasi (Haikal et al., 2019). Tim yang memiliki pemahaman mendalam tentang ancaman terkini, teknologi yang berkembang, dan business context organisasi dapat merancang dan mengimplementasikan kontrol yang lebih efektif (Kamal et al., 2024).

Tantangan yang dihadapi banyak organisasi di Indonesia adalah kelangkaan talenta keamanan informasi yang qualified dan cost yang tinggi untuk merekrut dan mempertahankan mereka (Haikal et al., 2019). Ini mendorong banyak organisasi untuk menggunakan jasa Managed Security Service Provider (MSSP) atau membangun program training internal (Intertek SAI Global, 2024).

Strategi Peningkatan Efektivitas Kebijakan Keamanan Informasi

Berdasarkan hasil analisis literatur pada subbab sebelumnya, dapat disimpulkan bahwa ancaman social engineering tidak dapat diatasi hanya melalui pendekatan teknis atau pemenuhan kepatuhan formal terhadap standar ISO/IEC 27001. Oleh karena itu, diperlukan strategi yang bersifat holistik, adaptif, dan berorientasi pada manusia (human-centered security) untuk meningkatkan ketahanan organisasi terhadap ancaman tersebut. Strategi dan rekomendasi yang dirumuskan dalam penelitian ini mencakup aspek kebijakan, teknologi, sumber daya manusia, serta tata kelola organisasi.

Pertama, penguatan program kesadaran dan pelatihan keamanan informasi berbasis perilaku menjadi strategi prioritas. Literatur menunjukkan bahwa sebagian besar insiden social engineering berhasil karena lemahnya kesadaran dan kewaspadaan karyawan dalam mengenali pola serangan (Ladayya et al., 2024). Oleh karena itu, organisasi disarankan untuk mengembangkan program security awareness yang berkelanjutan, kontekstual, dan interaktif, seperti simulasi phishing, tabletop exercise, serta pembelajaran berbasis studi kasus nyata. Program pelatihan tidak hanya berfokus pada transfer pengetahuan, tetapi juga diarahkan pada perubahan perilaku (behavioral change) dan pembentukan kebiasaan aman dalam komunikasi bisnis digital

Kedua, integrasi keamanan informasi ke dalam seluruh proses bisnis (security by design) perlu diperkuat. Hasil penelitian menunjukkan bahwa organisasi yang memposisikan keamanan sebagai bagian integral dari proses bisnis memiliki tingkat ketahanan yang lebih tinggi dibandingkan organisasi yang menjadikan keamanan sebagai fungsi tambahan (Intertek SAI Global, 2024). Implementasi ISO/IEC 27001 sebaiknya tidak hanya difokuskan pada pemenuhan dokumen dan audit, tetapi juga pada integrasi kontrol keamanan sejak tahap perencanaan sistem, pengembangan aplikasi, hingga operasional sehari-hari. Pendekatan ini memungkinkan organisasi untuk mengantisipasi risiko social engineering secara lebih proaktif dan sistematis

Ketiga, penguatan peran kepemimpinan dan tata kelola keamanan informasi menjadi faktor kunci dalam keberhasilan strategi mitigasi social engineering. Komitmen manajemen puncak perlu diwujudkan dalam bentuk kebijakan yang jelas, alokasi sumber daya yang memadai, serta dukungan terhadap budaya pelaporan insiden tanpa rasa takut disalahkan (non-punitive culture). Literatur menegaskan bahwa kepemimpinan yang aktif dalam keamanan informasi mampu mendorong internalisasi nilai-nilai keamanan di seluruh level organisasi (Fattah et al., 2024)

Keempat, pemanfaatan teknologi pendukung secara adaptif dan risk-based juga direkomendasikan untuk memperkuat pertahanan organisasi. Teknologi seperti email security gateway, multi-factor authentication (MFA), endpoint protection, dan sistem deteksi anomali berbasis perilaku dapat membantu mengurangi keberhasilan serangan social engineering. Namun,

penelitian menekankan bahwa teknologi harus dipilih dan diimplementasikan berdasarkan hasil penilaian risiko yang kontekstual, bukan sekadar mengikuti tren atau tuntutan compliance (Djebbar & Nordstrom, 2023)

Kelima, evaluasi dan peningkatan berkelanjutan (continuous improvement) dalam implementasi ISO/IEC 27001 perlu menjadi fokus utama organisasi. Audit internal dan eksternal sebaiknya tidak hanya dipandang sebagai kewajiban administratif, tetapi sebagai sarana pembelajaran organisasi untuk mengidentifikasi kelemahan dan peluang perbaikan. Pendekatan risk-based compliance yang menitikberatkan pada efektivitas kontrol dalam menghadapi ancaman nyata dinilai lebih relevan dibandingkan pendekatan compliance-oriented semata (Djebbar & Nordstrom, 2023)

Secara keseluruhan, strategi dan rekomendasi yang dirumuskan dalam penelitian ini menegaskan bahwa peningkatan ketahanan organisasi terhadap social engineering membutuhkan kombinasi antara kebijakan yang matang, kepemimpinan yang kuat, budaya keamanan yang positif, serta integrasi teknologi dan proses bisnis yang selaras. Pendekatan holistik ini diharapkan dapat membantu organisasi modern di Indonesia dalam menghadapi dinamika ancaman social engineering yang semakin kompleks di era komunikasi bisnis digital.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada Bab IV, dapat disimpulkan bahwa social engineering merupakan ancaman paling dominan dan berbahaya dalam konteks komunikasi bisnis digital di organisasi modern Indonesia. Ancaman ini berkembang seiring dengan meningkatnya ketergantungan organisasi terhadap teknologi digital, khususnya email bisnis, aplikasi pesan instan, media sosial, dan platform kolaborasi daring. Berbeda dengan serangan teknis yang menargetkan sistem, social engineering mengeksploitasi faktor manusia sebagai titik terlemah dalam sistem keamanan informasi.

Hasil analisis menunjukkan bahwa phishing, smishing, vishing, dan pretexting menjadi teknik social engineering yang paling sering digunakan, dengan tingkat keberhasilan yang tinggi karena memanfaatkan kepercayaan, rasa takut, tekanan waktu, serta budaya kepatuhan dalam organisasi. Selain itu, perkembangan AI-powered social engineering, seperti deepfake dan email phishing berbasis generative AI, menambah kompleksitas ancaman dan memperbesar risiko kebocoran informasi serta penipuan finansial.

Penelitian ini juga menyimpulkan bahwa dampak serangan social engineering bersifat multidimensional, mencakup kerugian finansial, gangguan operasional, kerusakan reputasi organisasi, serta konsekuensi hukum dan regulasi. Dalam banyak kasus, serangan social engineering menjadi pintu masuk awal bagi serangan lanjutan seperti ransomware, pencurian identitas, dan kebocoran data berskala besar, yang berpotensi melumpuhkan aktivitas organisasi dalam jangka pendek maupun jangka panjang.

Terkait efektivitas kebijakan keamanan informasi, penelitian ini menemukan bahwa implementasi standar ISO/IEC 27001 memberikan kerangka kerja yang sistematis dan komprehensif dalam mengelola risiko keamanan informasi, termasuk ancaman social engineering. Namun demikian, efektivitas penerapannya di Indonesia masih belum optimal. Tingkat kematangan keamanan informasi organisasi yang berada pada level sedang menunjukkan adanya kesenjangan antara kepatuhan formal (compliance) dengan efektivitas praktis di lapangan.

Kesenjangan tersebut terutama disebabkan oleh kurangnya integrasi kebijakan keamanan ke dalam budaya organisasi, rendahnya kesadaran keamanan karyawan, serta kecenderungan organisasi untuk memandang ISO 27001 sebagai alat sertifikasi semata, bukan sebagai sistem manajemen berkelanjutan. Dengan demikian, penelitian ini menegaskan bahwa keberhasilan kebijakan keamanan informasi tidak hanya ditentukan oleh keberadaan standar dan kontrol teknis, tetapi sangat bergantung pada faktor manusia, kepemimpinan, dan budaya keamanan organisasi.

REFERENSI

Amirinnisa, R., & Bisma, A. (2023). Strategi pengelolaan keamanan informasi dalam transformasi digital organisasi. *Jurnal Manajemen Informasi, 7*(2), 115–128.

Ardius, M., & Syamsuar, D. (2023). Assessment risk terhadap penggunaan sistem informasi akademik menggunakan metode ISO/IEC 27001. *Jurnal Sistem Informasi dan Keamanan, 5*(1), 45–56.

Arini, F. (2019). Dampak work from home terhadap keamanan informasi organisasi. *Jurnal Manajemen Informatika*.

Arumdiya, S., & Rudianto, H. (2025). Reorganisasi kontrol ISO/IEC 27001:2022 dan implikasinya terhadap manajemen risiko keamanan informasi. *Jurnal Keamanan Siber Indonesia, 4*(1), 1–14.

Bakri, M., & Irmayana, A. (2017). Ancaman keamanan informasi dalam era internet of things. *Jurnal Teknologi Informasi*.

Bank BSI. (2024). *Laporan keamanan siber dan tren social engineering di Indonesia*. Jakarta: Bank Syariah Indonesia.

Barraza, J., Gomez, L., & Hernandez, R. (2023). Cybersecurity maturity model untuk organisasi modern. *International Journal of Cybersecurity*.

Budi, S., Rahmawati, N., & Pratama, R. (2021). Social engineering sebagai ancaman utama dalam keamanan informasi organisasi. *Jurnal Teknologi Informasi dan Komunikasi, 9*(3), 201–213.

CSIRT Cirebon. (2025). *Analisis tren serangan social engineering berbasis media sosial*. Cirebon: CSIRT Cirebon.

CSIRT Teknokrat. (2024). *Laporan insiden keamanan siber dan business email compromise*. Bandar Lampung: CSIRT Teknokrat.

Daniswara, A., Nugroho, B., & Putri, S. (2023). Evaluasi keamanan informasi di lingkungan rumah sakit menggunakan pendekatan audit ISO 27001. *Jurnal Kesehatan Digital, 6*(2), 89–102.

Djebbar, M., & Nordstrom, L. (2023). Compliance challenges in information security management: ISO 27001 perspective. *International Journal of Information Security Management, 12*(4), 233–247.

Edavos. (2025). Serangan siber terhadap pusat data nasional dan implikasinya terhadap layanan publik. *Jurnal Keamanan Nasional, 3*(1), 1–10.

Fattah, R., Siregar, M., & Utami, L. (2024). Evaluasi efektivitas kebijakan keamanan informasi berbasis ISO 27001 di organisasi modern. *Jurnal Manajemen Risiko Siber, 8*(1), 55–69.

Intertek SAI Global. (2024). *ISO/IEC 27001:2022 information security management systems overview*. London: Intertek Group.

ISOCENTER Indonesia. (2015). *Panduan sistem manajemen keamanan informasi ISO/IEC 27001*. Jakarta: ISOCENTER Indonesia.

ITGID. (2025). *Collaboration tools vulnerabilities and security challenges*. Jakarta: ITGID Research.

Jelita, A., Prakoso, T., & Handayani, D. (2024). Budaya organisasi dan efektivitas keamanan informasi berbasis ISO 27001. *Jurnal Ilmu Komunikasi dan Teknologi, 11*(2), 134–148.

Justyna, K., & Abbas, R. (2021). Digital business communication: Opportunities and security challenges. *Journal of Business Communication*.

Kamal, M., Hidayat, R., & Saputra, A. (2024). Information technology security audit at the YDSF national zakat institution using the ISO 27001 framework. *Journal of Information Systems Audit, 5*(2), 77–90.

Kurii, S., & Opirskyy, I. (2023). Information security management systems and human factors. *Cybersecurity Review, 14*(1), 21–35.

Ladayya, R., Putra, A., & Hidayah, N. (2024). Kesadaran keamanan informasi atas phishing, smishing, dan vishing pada masyarakat perkotaan. *Jurnal Keamanan Informasi, 6*(3), 210–224.

Maulana, F. (2025). *Metodologi systematic literature review dalam penelitian keamanan informasi*. Bandung: Pustaka Akademik.

Master of Computer Science BINUS. (2021). *Keamanan informasi dan sistem manajemen keamanan informasi*. Jakarta: BINUS University Press.

Media Indonesia. (2024). Lonjakan serangan phishing di Indonesia sepanjang 2024. *Media Indonesia*.

Mitraberdaya. (2024). *Regulasi penerapan ISO/IEC 27001 di Indonesia*. Jakarta: Mitraberdaya Consulting.

Nurbojatmiko, A., Wibowo, H., & Lestari, S. (2024). Keamanan informasi dalam era society 5.0. *Jurnal Transformasi Digital, 5*(1), 1–15.

Riana, D., Kurniawan, F., & Lestari, S. (2023). Analisis maturity level dan PDCA dalam penerapan audit sistem manajemen keamanan informasi. *Jurnal Audit Sistem Informasi*.

Rochmadi, T., & Pasa, I. (2021). Pengukuran risiko dan evaluasi keamanan informasi menggunakan indeks KAMI berdasarkan ISO 27001. *Jurnal Sistem Pemerintahan Digital, 4*(2), 98–111.

Sinaga, R., & Taan, A. (2024). Penerapan ISO/IEC 27001:2022 dalam tata kelola keamanan sistem informasi. *Jurnal Tata Kelola Teknologi Informasi, 10*(1), 33–47.

Yahya, F., Suryani, D., & Rahmat, A. (2023). Program kesadaran keamanan informasi dan perubahan perilaku karyawan. *Jurnal Psikologi Organisasi, 7*(2), 120–134.