International Civic Enggagement Studies (ICES)
p-ISSN : 00000 | e-ISSN : 0000
Vol. … No. … (2025) | p. … - …
DOI : ……

ANCAMAN TERHADAP KOMUNIKASI BISNIS DAN KEBIJAKAN SEKURITI SERTA TATA KELOLA

***Keisha Najwa Khairana*[1], *Naqinni Azhara*[2], *Sasikirana Azalia Rahmadhani*[3], *Syalu Aulia Hakim*[4]**
[1] Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia
202310415011@mhs.ubharajaya.ac.id
[2] Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia
202310415241@mhs.ubharajaya.ac.id
[3] Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia
202310415274@mhs.ubharajaya.ac.id
[4] Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia
202310415158@mhs.ubharajaya.ac.id

*Correspondence: E-mail:: naqinazhr@gmail.com

A B S T R A C T S

Social engineering menjadi salah satu ancaman siber paling berbahaya dalam komunikasi bisnis karena memanfaatkan manipulasi psikologis untuk memperoleh akses ilegal. Serangan seperti phishing, pretexting, baiting, dan whaling terus meningkat, terutama di organisasi yang belum memiliki budaya keamanan kuat. Penelitian ini bertujuan menganalisis bagaimana social engineering mengancam komunikasi bisnis serta mengkaji efektivitas kebijakan keamanan dan tata kelola informasi dalam menekan risiko tersebut. Metode yang digunakan adalah analisis deskriptif kualitatif dengan menggabungkan literatur akademik dan data empiris dari lembaga nasional seperti BSSN. Hasil penelitian menunjukkan bahwa kebijakan keamanan hanya efektif jika didukung kontrol teknis, edukasi pengguna, mekanisme audit, dan leadership keamanan yang konsisten. Temuan ini menegaskan bahwa faktor manusia tetap menjadi titik paling rentan dan membutuhkan strategi mitigasi yang berkelanjutan.

A R T I C L E I N F O

Article History:
Received:xxxxxxx
Accepted:xxxxxxx
Publish:xxxxxxx

Keyword:
social engineering, komunikasi bisnis, keamanan informasi, tata kelola informasi, phishing, faktor manusia

1. PENDAHULUAN

Transformasi digital membawa perubahan signifikan pada cara organisasi berkomunikasi dan menjalankan proses bisnis. Namun, kemudahan tersebut juga membuka ruang bagi ancaman siber. Salah satu ancaman yang terus meningkat adalah social engineering, yaitu teknik manipulasi psikologis untuk menipu individu agar memberikan informasi atau akses yang seharusnya tidak boleh dibagikan. BSSN (2022) mencatat bahwa insiden yang melibatkan social engineering meningkat hampir setiap tahun, terutama melalui phishing dan penyalahgunaan kredensial email bisnis.

Komunikasi bisnis menjadi target utama karena jalur ini mengandung informasi kritis seperti data pelanggan, transaksi, rencana bisnis, hingga akses sistem internal. Serangan berbasis social engineering sering berhasil bukan karena kelemahan teknologi, melainkan karena kelengahan manusia. Oleh sebab itu, kebijakan keamanan informasi memainkan peran penting sebagai pagar struktural dalam mengurangi risiko.

Jurnal ini mengulas secara mendalam:

1. bagaimana social engineering mengganggu komunikasi bisnis,

2. bentuk-bentuk ancaman yang paling relevan bagi organisasi,

3. bagaimana kebijakan keamanan dan tata kelola dapat memitigasi ancaman tersebut secara efektif.

Menurut kelompok studi keamanan informasi, social engineering bekerja dengan mengeksploitasi prinsip psikologis seperti otoritas, urgensi, rasa percaya, serta kepatuhan (Cialdini, 2006; Mouton et al., 2016). Di Indonesia, Putra dan Rochim (2021) menemukan bahwa rendahnya kesadaran keamanan dan budaya organisasi yang permisif memudahkan pelaku melakukan manipulasi.

Kebijakan keamanan informasi didefinisikan sebagai seperangkat aturan formal yang mengatur bagaimana informasi dikelola, dilindungi, dan digunakan (Whitman & Mattord, 2018). Tata kelola keamanan (information security governance) melibatkan integrasi kebijakan, struktur organisasi, proses audit, dan komitmen manajemen (Von Solms & Van Niekerk, 2013).

DOI: xxxxxxxxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

2. METHODS

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi pustaka. Seluruh data diperoleh melalui penelusuran dan pembacaan berbagai sumber ilmiah yang relevan, seperti jurnal akademik, buku teks keamanan informasi, laporan resmi lembaga nasional.

Proses pengumpulan data dilakukan dengan cara mengidentifikasi artikel dan publikasi yang membahas social engineering, ancaman terhadap komunikasi bisnis, serta kebijakan dan tata kelola keamanan informasi. Setiap sumber dibaca secara menyeluruh, kemudian informasi yang berkaitan dengan topik penelitian dicatat dan diklasifikasikan.

Data yang diperoleh dari berbagai sumber tersebut kemudian digabungkan dan dianalisis secara tematik. Analisis dilakukan dengan membandingkan temuan antarjurnal untuk melihat kesamaan konsep, pola ancaman, serta efektivitas kebijakan keamanan yang dilaporkan. Hasil penggabungan ini digunakan untuk membangun pemahaman yang lebih komprehensif mengenai bagaimana social engineering menjadi ancaman bagi komunikasi bisnis dan bagaimana kebijakan keamanan dapat merespons ancaman tersebut.

Metode studi pustaka ini dipilih karena topik penelitian bersifat konseptual dan sangat bergantung pada pemahaman teori serta temuan akademik yang sudah ada. Dengan menggabungkan berbagai sumber terpercaya, penelitian ini menghasilkan kajian yang kuat secara ilmiah dan relevan dengan konteks keamanan informasi di organisasi modern.

Hasil Penelitian Terdahulu

No	Peneliti & Tahun	Judul Penelitian	Metode	Temuan Utama
1	Putra & Rochim (2021)	Analisis Kerentanan Social Engineering pada Organisasi Sektor Publik	Kualitatif — Studi kasus	Rendahnya kesadaran keamanan dan budaya organisasi yang permisif membuat pegawai mudah dimanipulasi.

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

2	Bullee et al. (2017)	Spear Phishing in Organisations Explained	Mixed methods	Spear phishing berhasil karena memanfaatkan konteks pekerjaan dan psikologi korban.
3	Mouton et al. (2016)	Social Engineering Attack Examples, Templates and Scenarios	Literatur studi	Social engineering memanfaatkan prinsip otoritas, urgensi, dan kepercayaan.
4	Abawajy (2014)	User Preference of Cyber Security Awaren ess Delivery Methods	Survei	Pengguna membutuhkan edukasi keamanan yang interaktif untuk mencegah phishing.
5	Whitman & Mattord (2018)	Principles of Information Security	Literatur akademik	Kebijakan keamanan harus jelas, relevan, dan didukung audit serta manajemen.
6	Von Solms & Van Niekerk (2013)	From Information Security to Cyber Security	Teoretis	Tata kelola keamanan penting untuk mencegah ancaman manusia.

DOI: xxxxxxxxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

7	Hidayat et al. (2022)	Tingkat Literasi Keamanan Digital Pengguna Internet Indonesia	Kuantitatif	Literasi digital masyarakat Indonesia masih rendah meningkatkan risiko social engineering.
8	Conti et al. (2016)	A Survey of Man-in-the-Middle Attacks	Systematic review	Serangan MITM sering berawal dari social engineering untuk mencuri kredensial.
9	Nurse et al. (2014)	Trustworthy and Effective Communication of Cyber Security Risks	Survei & analisis	Organisasi sering gagal mengkomunikasikan risiko keamanan dengan baik.

3. PEMBAHASAN

1. Social Engineering sebagai Ancaman Utama Komunikasi Bisnis

1.1 Phishing dan Spear Phishing

Phishing merupakan serangan paling umum yang menargetkan komunikasi bisnis karena memanfaatkan email sebagai media utama. Pelaku mendesain pesan seolah berasal dari pihak resmi, misalnya divisi keuangan, HR, atau vendor. Spear phishing lebih berbahaya karena pesan dirancang berdasarkan profil korban sehingga tingkat keberhasilannya tinggi (Bullee et al., 2017). Di perusahaan Indonesia, spear phishing sering digunakan untuk mengalihkan pembayaran vendor melalui manipulasi invoice (BSSN, 2022).

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

1.2 Whaling dan Penipuan Eksekutif

Whaling menargetkan eksekutif dengan pesan yang meniru gaya komunikasi internal perusahaan. Pelaku memanfaatkan kultur hierarki, di mana permintaan dari atasan sering dieksekusi tanpa verifikasi. Serangan ini banyak terjadi pada permintaan transfer dana mendesak atau akses data sensitif.

1.3 Pretexting: Rekayasa Identitas

Pretexting dilakukan dengan membuat skenario palsu, misalnya menyamar sebagai staf IT yang meminta kode OTP atau password "untuk pembaruan sistem". Kasus di Indonesia menunjukkan bahwa pretexting sering berhasil karena pelaku memahami konteks organisasi yang ditargetkan (Wibowo & Santoso, 2022).

1.4 Dampak pada Komunikasi Bisnis

Serangan social engineering dapat:

1. mengubah isi komunikasi (fraud),
2. mencuri kredensial email bisnis,
3. menyebarkan malware,
4. mengakibatkan kebocoran data, dan
5. merusak kepercayaan antarunit bisnis maupun dengan mitra eksternal.

2. Efektivitas Kebijakan Keamanan Informasi dalam Mengatasi Social Engineering

2.1 Kualitas Kebijakan dan Relevansi Operasional

Kebijakan keamanan yang ideal tidak hanya berisi larangan dan prosedur teknis, tetapi juga panduan perilaku. Kebijakan yang efektif memiliki ciri:

1. jelas,
2. mudah dipahami,
3. relevan dengan proses bisnis,
4. mendukung pengambilan keputusan harian, dan
5. diperbarui secara berkala (Whitman & Mattord, 2018).

Kebijakan yang hanya bersifat administratif terbukti tidak mampu menahan serangan social engineering.

2.2 Pelatihan Kesadaran Keamanan sebagai Kunci Utama

Kesadaran pengguna merupakan faktor paling penting dalam mencegah social engineering. Pelatihan yang efektif mencakup:

DOI: xxxxxxxxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

1. simulasi phishing,
2. praktik verifikasi dua langkah,
3. pembelajaran berbasis kasus nyata,
4. pelaporan insiden tanpa sanksi.

Di Indonesia, BSSN dan Kominfo menekankan pentingnya peningkatan literasi digital karena sebagian besar insiden bermula dari kelengahan pengguna, bukan kegagalan sistem.

2.3 Tata Kelola Keamanan dan Peran Manajemen Puncak

Tata kelola keamanan memastikan kebijakan berjalan melalui struktur yang jelas, audit rutin, dan mekanisme evaluasi. Jika manajemen tidak menunjukkan komitmen, kebijakan hanya menjadi dokumen tanpa fungsi. Organisasi yang berhasil menekan social engineering biasanya memiliki:

1. unit keamanan khusus,
2. SOP komunikasi aman,
3. alur eskalasi insiden yang jelas,
4. budaya “cek dulu sebelum klik”.

2.4 Pengendalian Teknis Pendukung

Walau fokus utama social engineering ada pada manusia, kontrol teknis tetap penting, seperti:

1. email filtering,
2. verifikasi domain,
3. multi-factor authentication,
4. endpoint protection,
5. enkripsi komunikasi.

Kontrol teknis berperan sebagai second layer jika pengguna gagal mendeteksi manipulasi.

4. CONCLUSION

Social engineering merupakan ancaman paling kritis dalam komunikasi bisnis modern karena memanfaatkan kelemahan manusia, bukan teknologi. Serangan seperti phishing, spear phishing, whaling, dan pretexting terbukti mampu merusak integritas komunikasi serta menyebabkan kerugian finansial dan reputasi organisasi.

Kebijakan keamanan informasi dapat menjadi alat mitigasi yang efektif jika dirancang dengan jelas, relevan, dan didukung oleh tata kelola yang kuat. Pelatihan kesadaran keamanan menjadi elemen paling penting dalam mencegah serangan karena manusia adalah titik rawan utama. Kombinasi antara edukasi, komitmen manajemen, audit, dan kontrol teknis terbukti meningkatkan ketahanan organisasi terhadap social engineering.

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

5. References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237–248.

Alshehri, M., Alabdulmohsin, I., & Algalil, S. (2023). Detecting phishing emails using deep learning techniques. Journal of Cybersecurity and Digital Forensics, 5(2), 77–92.

Badan Siber dan Sandi Negara. (2022). Laporan Tahunan Keamanan Siber Indonesia. BSSN RI.

Bullee, J. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information & Computer Security, 25(5), 593–613.

Cherdantseva, Y., & Hilton, J. (2013). Information security and information assurance: The discussion about the meaning, scope, and goals. International Journal of Computer Science and Engineering, 7(1), 36–43.

Cialdini, R. B. (2006). Influence: The psychology of persuasion (Rev. ed.). Harper Collins.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027–2051.

Firmansyah, A., & Suryanto, W. (2022). Analisis risiko keamanan jaringan WiFi publik di kawasan perkotaan. Jurnal Teknologi Informasi dan Keamanan, 10(1), 45–54.

Fruhlinger, J. (2020). Whaling attack definition and examples. CSO Online.

Harris, A. J., Patten, K., & Regan, E. (2012). The need for BYOD mobile device security awareness. Information Security Journal, 21(3), 123–131.

Hidayat, R., Fadhilah, N., & Yuliana, D. (2022). Tingkat literasi keamanan digital pengguna internet di Indonesia. Jurnal Ilmu Komunikasi Digital Indonesia, 4(2), 101–114.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. Wiley.

Mouton, F., Leenen, L., & Venter, H. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209.

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2014). Trustworthy and effective communication of cyber security risks. ACM Computing Surveys, 47(4), 1–44.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). The human aspects of information security questionnaire (HAIS-Q): Measuring security awareness. Computers & Security, 42, 165–176.

Putra, B. S., & Rochim, A. F. (2021). Analisis kerentanan social engineering pada organisasi sektor publik. Jurnal Keamanan Siber Nusantara, 3(2), 89–102.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

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

Wibowo, E., & Santoso, I. (2022). Evaluasi risiko insider threat pada sistem informasi perusahaan. Jurnal Sistem Informasi Indonesia, 8(1), 55–63.

DOI: xxxxxxxxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx