Inovan Publisher

Fibonacci: Jurnal Ilmu Ekonomi, Manajemen dan Keuangan

| ISSN (Online) 3064-5883 |
https://creativecommons.org/licenses/by/4.0/
DOI: 10.63217/fibonacci.v2i1.253

Manajemen Krisis dan Respons Insiden Keamanan dalam Era Digital

Nazwa Salsabila[1], Achmad Fauzi[2], Lina Ramadani[3], Annisa Novita Sari[4]
[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, salsabilanazwa69@gmail.com
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, linarmdn02@gmail.com
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, novitasariannisa8@gmail.com

Corresponding Author: salsabilanazwa69@gmail.com[1]

Abstract: *This study discusses crisis management and cybersecurity incident response in an increasingly complex digital era. Digital transformation developments improve organizational efficiency, but also increase the risk of data leaks and cyber attacks that can threaten reputation, public trust, and business continuity. This study uses a literature review method sourced from scientific journals, books, and proceedings, and is reinforced by a case study analysis of the 2020 Tokopedia data breach and the 2023 ransomware attack on Bank Syariah Indonesia (BSI). The results show that most organizations in Indonesia still take a reactive approach to handling digital security crises, with limited integration between technical preparedness, crisis communication, and business continuity planning. Although internal recovery and coordination systems are able to keep operations running, delays in communicating information to the public have the potential to undermine stakeholder trust. This research emphasizes that successful digital crisis management requires synergy between technical preparedness, transparent internal and external communication, and an organizational culture that supports post-crisis learning and evaluation.*

Keywords: *Crisis Management, Cybersecurity, Incident Response, Disaster Recovery Plan (DRP)*

Abstrak: Penelitian ini membahas manajemen krisis dan respons insiden keamanan siber di era digital yang semakin kompleks. Perkembangan transformasi digital meningkatkan efisiensi organisasi, namun juga memperbesar risiko kebocoran data dan serangan siber yang dapat mengancam reputasi, kepercayaan publik, serta keberlanjutan bisnis. Penelitian ini menggunakan metode studi literatur yang bersumber dari jurnal ilmiah, buku, dan prosiding, serta diperkuat dengan analisis studi kasus kebocoran data Tokopedia tahun 2020 dan serangan ransomware pada Bank Syariah Indonesia (BSI) tahun 2023. Hasil kajian menunjukkan bahwa sebagian besar organisasi di Indonesia masih menerapkan pendekatan reaktif dalam menangani krisis keamanan digital, dengan keterbatasan integrasi antara kesiapan teknis, komunikasi krisis, dan perencanaan keberlanjutan bisnis. Meskipun sistem pemulihan dan koordinasi internal mampu menjaga operasional tetap berjalan, keterlambatan penyampaian informasi kepada publik berpotensi menurunkan kepercayaan pemangku kepentingan. Penelitian ini menegaskan bahwa keberhasilan manajemen krisis digital memerlukan sinergi

antara kesiapan teknis, komunikasi internal dan eksternal yang transparan, serta budaya organisasi yang mendukung pembelajaran dan evaluasi pascakrisis.

Kata Kunci: Manajemen Krisis, Keamanan Siber, Respons Insiden, *Disaster Reovery Plan (DRP)*

PENDAHULUAN

Transformasi digital merupakan proses strategis yang melibatkan pemanfaatan teknologi digital untuk mengubah cara organisasi beroperasi, menciptakan nilai, dan berinteraksi dengan para pemangku kepentingan (Ramdani, 2025). Transformasi digital menciptakan perubahan dalam tata kelola perusahaan modern. Kemajuan teknologi informasi, sistem berbasis cloud, dan platform digital telah meningkatkan efisiensi bisnis,tetapi juga memperluas risiko terhadap ancaman keamanan siber (Asrul, 2025).

Fenomena kebocoran data, serangan ransomware, dan gangguan operasional bukan hanya masalah teknis, tetapi juga ancaman strategis terhadap reputasi dan keberlanjutan bisnis suatu perusahaan (Nathania *et al,* 2025) Peran manajemen krisis dan respons insiden keamanan menjadi sangat penting dalam hal ini. Menurut Yuliastina (2017) manajemen krisis bukan hanya langkah reaktif, tetapi merupakan sebuah sistem terpadu yang mengantisipasi, mengendalikan, dan memulihkan kondisi perusahaan saat terjadi gangguan besar. Dalam dunia digital manajemen krisis memerlukan koordinasi antara unit teknologi informasi, komunikasi publik, serta pimpinan eksekutif untuk memastikan keputusan yang cepat dan akurat.

Saat ekosistem perusahaan sudah banyak beralih ke digital, maka dari itu diperlukan keamanan lebih terkait dengan data dan sistem perusahan. Perusahaan turut memberikan awareness berupa Cyber Security Awareness'. Dalam hal ini, Humas turut mensosialisasikan bahwa tugas menjaga keamanan data tidak hanya dari divisi IT, namun dari semua divisi perusahaan. Perusahaan juga menekankan untuk mematikan komputer setelah selesai bekerja, melakukan penggantian kata sandi secara berkala untuk akun yang terafiliasi dengan akun perusahaan seperti akun PEO, lalu menggunakan perangkat lunak yang resmi, tidak meng-klik tautan yang mencurigakan seperti link phising yang dikemas seperti surat undangan (Malika, 2024). Siregar *et al,* (2024) menegaskan bahwa kecepatan dan ketepatan dalam memberikan informasi selama krisis terjadi menjadi penentu persepsi publik.

Perusahaan yang memiliki respon lambat cenderung akan kehilangan kepercayaan pelanggan dan menghadapi tekanan media. Sementara itu, Irawan (2024) dalam bahwa keamanan informasi menjadi perhatian utama bagi bisnis di seluruh dunia, dengan manajemen keamanan informasi menjadi tantangan penting. Faktor-faktor yang mempengaruhi performa keamanan siber suatu negara meliputi ketersediaan tenaga ahli, proses pengambilan keputusan yang terstruktur, manajemen infrastruktur, solusi keamanan yang dirancang khusus, konvergensi OT/TI, respons insiden cepat, dan pelatihan staf. Upaya edukasi dan kesadaran pengguna juga penting dalam mengurangi kerentanan sistem. Setiawan (2024) mengatakan Peraturan pemerintah semakin menekankan pentingnya memiliki rencana pemulihan bencana bagi organisasi, terutama BUMN Temuan ini selaras dengan riset Kedua dan Zebua (2024) yang menyebut bahwa banyak perusahaan masih menghadapi tantangan dalam melindungi data pelanggan, mengelola risiko serangan siber, dan mematuhi regulasi keamanan data. Selain itu, kesadaran akan pentingnya keamanan informasi juga perlu ditingkatkan di kalangan karyawan. Penelitian ini diharapkan dapat memberikan rekomendasi praktis untuk meningkatkan keamanan sistem informasi di perusahaan e-commerce di Indonesia.

Kasus kebocoran data berskala besar yang terjadi pada salah satu platform digital nasional pada tahun 2020 menjadi momentum penting yang menguji kesiapan manajemen krisis siber di Indonesia. Pada insiden tersebut, puluhan juta data pengguna dilaporkan terekspos akibat serangan peretas. Pihak perusahaan segera mengaktifkan rencana penanganan insiden (Incident Response Plan/IRP) dan melakukan komunikasi resmi kepada publik. Meskipun sempat menuai kritik karena klarifikasi dinilai terlambat, langkah cepat untuk mengumumkan

insiden serta koordinasi dengan pemerintah membantu meredam kepanikan masyarakat.

Berdasarkan konteks tersebut, analisis ini berupaya mengintegrasikan temuan dari berbagai penelitian terdahulu yang membahas manajemen krisis, keamanan informasi, strategi komunikasi perusahaan, serta business continuity, kemudian mengaitkannya dengan contoh kasus nyata kebocoran data digital di Indonesia. Dengan demikian, esai ini diharapkan dapat memperkuat landasan teoritis dan empiris mengenai urgensi tata kelola krisis siber di era ekonomi digital.

Oleh karena itu, penelitian ini bertujuan untuk mengkaji peran pemahaman cybersecurity dalam menjaga keamanan akun Instagram pada mahasiswa, serta mengidentifikasi faktor-faktor yang memengaruhi tingkat kesadaran mereka terhadap berbagai ancaman siber yang berkembang di era digital.

Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Jenis ancaman kejahatan siber apa saja yang berpotensi memicu konflik siber, seperti peretasan akun, sabotase siber, serta penggunaan perangkat mata-mata digital?
2. Manfaat apa saja yang dapat diperoleh mahasiswa dari penggunaan media sosial, khususnya Instagram, secara bijak dan aman?
3. Strategi apa saja yang dapat diterapkan untuk membangun dan meningkatkan kesadaran masyarakat, khususnya mahasiswa, mengenai pentingnya keamanan siber?

METODE

Metode dalam penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi pustaka. Data penelitian diperoleh melalui penelusuran dan kajian terhadap berbagai sumber ilmiah yang relevan, seperti jurnal akademik, buku teks di bidang keamanan informasi, serta laporan resmi dari lembaga nasional yang berkaitan dengan keamanan siber. Proses pengumpulan data dilakukan dengan mengidentifikasi dan memilih artikel serta publikasi yang membahas topik social engineering, ancaman terhadap komunikasi bisnis, serta kebijakan dan tata kelola keamanan informasi. Setiap sumber yang terpilih dibaca secara menyeluruh untuk memahami konteks dan substansi pembahasan, kemudian informasi yang relevan dicatat dan dikelompokkan sesuai dengan fokus penelitian.

Data yang telah dikumpulkan selanjutnya dianalisis menggunakan teknik analisis tematik. Analisis dilakukan dengan membandingkan temuan dari berbagai sumber untuk mengidentifikasi kesamaan konsep, pola ancaman social engineering, serta efektivitas kebijakan keamanan informasi yang dilaporkan dalam literatur. Hasil analisis ini digunakan untuk membangun pemahaman yang komprehensif mengenai dampak social engineering terhadap komunikasi bisnis dan peran kebijakan keamanan dalam memitigasi ancaman tersebut.

HASIL DAN PEMBAHASAN

Berdasarkan latar belakang masalah dan rumusan masalah diatas, maka hasil penelitian ini adalah sebagai berikut:

Social Engineering sebagai Ancaman terhadap Komunikasi Bisnis

Social engineering adalah bentuk ancaman siber yang semakin banyak ditemui di zaman digital saat ini. Berbeda dengan serangan teknis yang mencari celah dalam sistem, rekayasa sosial lebih memfokuskan pada aspek manusia dengan menggunakan manipulasi psikologis. Dalam dunia komunikasi bisnis, metode ini sering dimanfaatkan untuk menipu pegawai agar memberikan data sensitif atau mengambil langkah-langkah tertentu yang merugikan perusahaan.

Komunikasi bisnis menjadi target utama karena dianggap resmi dan dipercaya oleh banyak orang. Email, pesan instan, dan komunikasi internal di perusahaan biasanya berisi informasi penting seperti data pelanggan, instruksi terkait keuangan, hingga akses ke sistem internal. Para pelaku rekayasa sosial memanfaatkan kepercayaan ini dengan berpura-pura

menjadi atasan, kolega, atau mitra bisnis, sehingga korban tidak menyadari bahwa mereka menjadi sasaran. Situasi ini menunjukkan bahwa keamanan dalam komunikasi bisnis tidak hanya bergantung pada teknologi, tetapi juga pada sikap dan kewaspadaan penggunanya.

Bentuk-Bentuk Ancaman Social Engineering yang Relevan bagi Organisasi

Ancaman dari rekayasa sosial adalah salah satu jenis serangan dalam dunia siber yang mengeksploitasi kelemahan manusia sebagai target utama. Dengan meningkatnya ketergantungan organisasi pada teknologi digital dan sistem informasi, jenis-jenis rekayasa sosial pun ikut berkembang dan menjadi lebih rumit. Serangan ini tidak hanya menimbulkan risiko kehilangan data, tetapi juga bisa menyebabkan krisis dalam organisasi, baik dari aspek operasional, finansial, maupun reputasi. Oleh karena itu, penting untuk memahami berbagai bentuk ancaman rekayasa sosial sebagai dasar untuk mencegah dan merespons insiden keamanan.

Berbagai bentuk ancaman rekayasa sosial yang relevan bagi organisasi adalah sebagai berikut:

1. Phishing
   Usaha penipuan lewat email, pesan singkat, atau platform digital lainnya yang dirancang untuk menyerupai komunikasi resmi dengan tujuan mendapatkan informasi sensitif seperti kata sandi, data pribadi, atau kredensial akun organisasi.
2. Spear Phishing
   Serangan yang ditujukan secara spesifik pada individu atau unit tertentu di dalam organisasi dengan pesan yang lebih personal dan kontekstual, sehingga meningkatkan kemungkinan keberhasilan penipuan.
3. Vishing
   Metode rekayasa sosial yang dilakukan melalui telepon, berpura-pura menjadi pihak berwenang atau bagian internal organisasi untuk memanipulasi korban agar memberikan informasi penting.
4. Pretexting
   Penciptaan skenario atau identitas palsu untuk membangun kepercayaan korban sebelum mendapatkan akses kepada informasi atau sistem dalam organisasi.

Dampak Social Engineering terhadap Keamanan Informasi dan Operasional Organisasi

Serangan social engineering dapat memberikan konsekuensi yang signifikan untuk perusahaan, baik dari segi keamanan data maupun operasi bisnis. Salah satu hasil utama adalah kebocoran informasi, di mana data sensitif seperti informasi pelanggan atau kata sandi sistem bisa jatuh ke tangan yang salah. Kebocoran ini tidak hanya merugikan organisasi dari sisi keuangan, tetapi juga dapat mengurangi kepercayaan masyarakat.

Selain itu, social engineering dapat mengakibatkan gangguan dalam operasi, contohnya ketika sistem internal diserang atau ada penyalahgunaan akses oleh individu luar. Dalam beberapa situasi, perusahaan harus menghentikan layanan sementara untuk memulihkan sistem, yang tentunya berdampak pada produktivitas dan citra. Oleh karena itu, ancaman dari rekayasa sosial perlu dilihat sebagai risiko serius yang harus ditangani dengan cara yang terencana.

Strategi Pencegahan dan Peningkatan Kesadaran Keamanan Informasi

Upaya pencegahan ancaman social engineering tidak hanya bisa bergantung pada teknologi, tetapi juga perlu mencakup peningkatan kesadaran mengenai keamanan informasi di antara sumber daya manusia. Pelatihan keamanan yang dilakukan secara rutin, latihan serangan phishing, serta kampanye internal tentang keamanan informasi bisa membantu meningkatkan kewaspadaan di kalangan karyawan.

Selain itu, mengintegrasikan kebijakan keamanan dengan budaya organisasi adalah langkah yang krusial agar praktik keamanan menjadi bagian dari rutinitas sehari-hari. Dengan cara ini,

karyawan tidak hanya mengetahui aturan yang ada, tetapi juga memiliki kesadaran terhadap potensi risiko yang mungkin muncul. Pendekatan ini diharapkan dapat memperkuat posisi manusia sebagai garis pertahanan utama dalam menjaga keamanan komunikasi bisnis dalam organisasi.

Tabel 1. Hasil Penelitian Terdahulu

No	Judul dan Penulis	Perbedaan	Persamaan
1.	**Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT** – (Ade Irawan dkk. 2024)	Penelitian ini lebih menekankan pada manajemen keamanan siber berbasis IoT serta strategi teknis dan kebijakan pada level sistem dan nasional.	Sama-sama memandang keamanan digital sebagai isu strategis serta menekankan pentingnya respons insiden yang cepat dan terstruktur.
2.	**Transformasi Bisnis di Era Digital: Peluang, Tantangan, dan Strategi Inovasi** – (Asrul. 2025)	Fokus penelitian terletak pada transformasi bisnis dan inovasi organisasi, dengan keamanan siber sebagai bagian dari tantangan digital.	Sama-sama menyoroti bahwa perkembangan teknologi digital membawa peluang sekaligus risiko bagi organisasi.
3.	**Manajemen Krisis Public Relations BPWS** – (Roos Yulistiana. 2017)	Penelitian ini membahas krisis sosial dengan pendekatan komunikasi public relations secara langsung dan interpersonal.	Sama-sama menggunakan konsep manajemen krisis yang mencakup tahapan pra-krisis, krisis, dan pasca-krisis.
4.	**Analisis Strategi Komunikasi Krisis dalam Mempertahankan Reputasi Perusahaan** – (Nasaruddin Siregar dkk. 2024)	Penelitian lebih berfokus pada strategi komunikasi krisis dan upaya mempertahankan reputasi perusahaan.	Sama-sama menekankan pentingnya kecepatan dan ketepatan respons organisasi dalam situasi krisis.
5.	**Strategi Komunikasi Krisis di Era Digital** – (Aqida Nuril Salma. 2018)	Penelitian ini menitikberatkan pada peran internet dan media digital dalam praktik komunikasi krisis public relations.	Sama-sama membahas krisis di era digital serta perlunya respons yang cepat dan adaptif.
6.	**Komunikasi Krisis di Era Digital** – (Topan Setiawan dkk. 2019)	Fokus penelitian pada pengelolaan media relations dan pembentukan citra organisasi saat krisis.	Sama-sama menekankan pentingnya strategi komunikasi yang tepat dalam menghadapi krisis digital.
7.	**Strategi Manajemen Krisis Komunikasi Perusahaan di Era Disinformasi Media Sosial** – (Mere, K. 2025)	Penelitian ini menitikberatkan pada pengaruh disinformasi media sosial terhadap eskalasi krisis perusahaan.	Sama-sama membahas perlunya strategi manajemen krisis yang terencana dan terkoordinasi.
8.	**Ancaman Penyalahgunaan Data Pribadi sebagai Dampak Sistem Informasi Manajemen** – (Nugraha & Nasution. 2024)	Fokus utama penelitian pada perlindungan data pribadi dan keamanan sistem informasi.	Sama-sama menyoroti risiko digital yang dapat memicu krisis kepercayaan publik.
9.	**Penerapan BCP/DRP pada BUMN** – (Yulhendri. 2016)	Penelitian berfokus pada perencanaan keberlanjutan bisnis dan pemulihan bencana.	Sama-sama membahas kesiapan organisasi dalam menghadapi gangguan dan krisis.
10.	**Analisis Krisis Organisasi Berdasarkan Model Anatomi Krisis** – (Suharyanti & Sutawidjaya. 2013)	Penelitian menggunakan pendekatan public relations dan model anatomi krisis.	Sama-sama menekankan pentingnya perencanaan dan pengelolaan krisis organisasi.
11.	**Strategi Manajemen Krisis Gojek** – (Jeconiah, C. 2025)	Penelitian difokuskan pada perusahaan teknologi dengan karakteristik digital yang	Sama-sama membahas strategi manajemen krisis dalam konteks organisasi

		spesifik.	modern.
12.	**Collaboration Engineering for Incident Response Planning** – (Kamal et al. 2007)	Penelitian menitikberatkan pada perencanaan respons insiden berbasis kolaborasi lintas fungsi.	Sama-sama menekankan pentingnya koordinasi dan kesiapsiagaan dalam menghadapi krisis.

Berdasarkan tabel literature review, dapat disimpulkan bahwa studi-studi sebelumnya mengupas berbagai aspek terkait manajemen krisis, keamanan siber, dan cara organisasi bereaksi terhadap insiden di zaman digital. Topik yang dibahas bervariasi, mulai dari strategi komunikasi saat krisis, perlindungan data serta sistem informasi, perencanaan kelangsungan bisnis, hingga kesiapan organisasi dalam menghadapi ancaman di dunia maya. Beberapa kajian menekankan pada pentingnya respons yang cepat dan akurat serta peran komunikasi dan media dalam mengurangi dampak krisis, sementara studi lainnya lebih mengedepankan aspek pengelolaan, kebijakan, dan koordinasi internal dalam menangani insiden terkait keamanan.

Perbedaan utama di antara penelitian-penelitian tersebut terletak pada perspektif dan konteks yang diangkat. Sebagian dari studi tersebut lebih menyoroti komunikasi krisis dan reputasi organisasi, sementara penelitian lain lebih menfokuskan pada manajemen keamanan, respons terhadap insiden, serta kelangsungan operasional organisasi. Meskipun demikian, semua penelitian memiliki kesamaan dalam menekankan pentingnya kesiapan, pengambilan keputusan yang strategis, serta respons yang cepat dan terkoordinasi dalam menghadapi krisis di dunia digital, demi menjaga stabilitas organisasi dan kepercayaan publik.

KESIMPULAN

Social engineering merupakan ancaman terbesar dalam komunikasi bisnis saat ini karena memanfaatkan kelemahan dari aspek manusia, bukan dari sisi teknologi. Serangan seperti phishing, spear phishing, vishing, dan pretexting telah terbukti dapat merusak integritas komunikasi bisnis dan menyebabkan kerugian yang signifikan dalam hal finansial, operasional, dan reputasi organisasi, terutama di era ketika ketergantungan pada sistem digital semakin tinggi. Kebijakan keamanan informasi berfungsi sebagai alat mitigasi yang efektif jika disusun dengan jelas, relevan, dan didukung oleh sistem pengelolaan keamanan yang solid. Pelatihan untuk meningkatkan kesadaran tentang keamanan menjadi komponen penting dalam mencegah serangan, mengingat bahwa sumber daya manusia adalah titik lemah utama. Selain itu, mengaitkan kebijakan keamanan dengan budaya organisasi, didukung oleh komitmen dari manajemen, melakukan audit secara rutin, dan menerapkan kontrol teknis yang tepat, telah terbukti dapat memperkuat ketahanan serta kesiapan organisasi dalam menghadapi ancaman rekayasa sosial secara terus-menerus.

REFERENSI

Asrul. (2025). Transformasi bisnis di era digital: Peluang, tantangan, dan strategi inovasi. *Jurnal Minfo Polgan*, 13(2).

Irawan, A., Fadholi, W. H. N., Erikamaretha, Z., & Sinlae, F. (2024). Tantangan dan strategi manajemen keamanan siber di Indonesia berbasis IoT. *Zetroem*, 6(1), 114–124.

Jeconiah, C. (2025). Strategi manajemen krisis Gojek: Peran komunikasi, media, dan implikasi bagi perusahaan teknologi. *Triwikrama: Jurnal Multidisiplin Ilmu Sosial*, 7(5).

Kamal, M., Davis, A. J., Pietron, L. R., Nabukenya, J., de Vreede, G.-J., & Schoonover, T. V. (2007). Collaboration engineering for incident response planning: Process development and validation. *Proceedings of the 40th Hawaii International Conference on System Sciences*.

Komal, K., Mulia, M. H., & Rudianto, R. (2025). Audit keamanan sistem informasi menggunakan standar ISO/IEC 27001:2013 pada Unit Sistem Informasi PT Kereta Api Indonesia Persero Daop 1 Jakarta. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 8(2).

Mere, K. (2025). Strategi manajemen krisis komunikasi perusahaan di era disinformasi media sosial. *Community Engagement & Emergence Journal*, 6(3), 1327–1335.

Nathania, A. B., Azam, M. A., & Voll, R. R. E. (2025). Menanggulangi ancaman keamanan siber di sektor perbankan: Upaya melindungi data nasabah di zaman digital. *Jurnal Ilmiah Wahana Pendidikan*, 11(6.D), 34–39.

Nirmalasari, A. (2020). Manajemen krisis dalam public relations: Analisis meta-sintesis aktivisme online. *Jurnal Penelitian Komunikasi dan Opini Publik*, 24(2), 98–112.

Nugraha, R. A., & Nasution, M. I. P. (2024). Ancaman penyalahgunaan data pribadi sebagai dampak penggunaan sistem informasi manajemen. *Journal of Informatics and Business*, 2(2), 197–201.

Pamungkas, W. C., & Saputra, F. T. (2020). Analisa mobile phishing dengan Incident Response Plan dan incident handling. *Jurnal Riset Komputer*, 7(4).

Salma, A. N. (2018). Strategi komunikasi krisis di era digital: Penggunaan internet dari sebelum hingga sesudah krisis. *Jurnal Penelitian Pers dan Komunikasi Pembangunan*, 22(1).

Setiawan, T., Kurniawati, J., & Saputro, E. (2019). Komunikasi krisis di era digital. *Jurnal Ilmu Komunikasi*, 17(2).

Siregar, N., Nursyamsi, S. E., & Dewi, N. K. (2024). Analisis strategi komunikasi krisis dalam mempertahankan reputasi perusahaan di situasi darurat. *Harmoni: Jurnal Ilmu Komunikasi dan Sosial*, 2(4), 142–154.

Suharyanti, & Sutawidjaya, A. H. (2013). Analisis krisis pada organisasi berdasarkan model anatomi krisis dan perspektif public relations. *Communication Spectrum*, 2(2).

Utomo, B. S., Diponegoro, R. A. M. P., Alfarizi, M. A. H., & Hibatullah, F. (2023). Manajemen krisis pandemi COVID-19 di Indonesia. *Jurnal Ilmiah Dinamika Sosial*, 7(2), 130–142.

Wahyuningsih, R. S. H. (2020). Krisis organisasi, budaya, dan kepemimpinan etis: Sebuah tinjauan literatur. *Sudut Pandang*, 1(2).

Yulhendri. (2016). Penerapan Business Continuity Plan / Disaster Recovery Plan (BCP/DRP) pada BUMN dalam rangka sustainability. *Jurnal Ilmu Komputer*, 12(1).

Yuliastina, R. (2017). Manajemen krisis public relations (Studi kasus BPWS). *Jurnal Komunikasi*, 11(1), 29–38.

Zein, A. (2023). Analisa penyerangan untuk cyber security social engineering. *Jurnal Informatika Universitas Pamulang*, 8(4), 642–648.

Wibowo, B. S. A., & Hermawan, A. (2023). Faktor dan rencana aksi implementasi BCMS pada sektor publik. *Jurnal Akademi Akuntansi*, 6(3), 323–344