

Analisis Pengambilan Keputusan dalam Menyikapi Isu Keamanan Digital (Notifikasi "No System is Safe") di PT Telkomsel

**Hilma Harmen¹, Mhd. Syaikh Nazri Limbong², Stefhani Gresia Simare-mare³,
Dita Agustina Bintang⁴, Karin Rimina Bangun⁵, Nesah Sartika Harahap⁶, Helon
Hibri Harahap⁷**

Universitas Negeri Medan, Indonesia
limbongnazri18@gmail.com

Submitted: 17th August 2025 | **Edited:** 25th September 2025 | **Issued:** 01st October 2025

Cited on: Harmen, H., Limbong, M. S. N., Simare-mare, S. G., Bintang, D. A., Bangun, K. R., Harahap, N. S., & Harahap, H. H. (2025). Analisis Pengambilan Keputusan dalam Menyikapi Isu Keamanan Digital (Notifikasi "No System is Safe") di PT Telkomsel. *SCIENTIFIC JOURNAL OF REFLECTION: Economic, Accounting, Management and Business*, 8(4), 1646-1652.

ABSTRACT

This study examines the decision-making process of PT Telkomsel in addressing digital security challenges, particularly in the context of the alert "No System is Safe." The main problem lies in the increasing cyber threats that jeopardize customer data, corporate reputation, and regulatory compliance, which cannot be mitigated solely by adopting international security standards. The research aims to analyze how decision-making theories, especially bounded rationality, are applied by Telkomsel when responding to uncertain and high-risk situations. Using a qualitative descriptive approach with a literature review method, data were obtained from scholarly journals, corporate policy documents, institutional reports, and media coverage related to digital security and organizational decision-making. The findings reveal that Telkomsel employs a combination of directive, analytical, conceptual, and behavioral decision-making styles, supported by rational, intuitive, participative, and bounded rationality approaches. This integration enables the company to balance speed, accuracy, and adaptability in managing cyber incidents. The study contributes by highlighting that effective digital security management in a large-scale telecommunication company depends not only on technical safeguards but also on the quality of organizational decision-making under uncertainty.

Keywords: Digital Security, Decision-Making, Bounded Rationality, Telkomsel, Cyber Risk Management

PENDAHULUAN

PT Telekomunikasi Selular (Telkomsel) merupakan anak perusahaan dari PT Telkom Indonesia yang sejak berdiri pada tahun 1995 berkembang menjadi operator telekomunikasi seluler terbesar di Indonesia, dengan lebih dari 150 juta pelanggan aktif. Perusahaan tidak hanya menyediakan layanan jaringan, tetapi juga menjadi pemain utama dalam ekosistem digital nasional melalui layanan hiburan, finansial, dan solusi bisnis (PT Telekomunikasi Selular, 2023). Namun, posisi strategis ini menempatkan Telkomsel pada risiko tinggi terkait keamanan digital yang semakin kompleks.

Dalam era transformasi digital, ancaman keamanan siber tidak lagi terbatas pada serangan tradisional seperti virus, tetapi mencakup ransomware, phishing, dan serangan

DDoS yang dapat mengganggu layanan maupun merugikan pelanggan (Adisty, 2024). Prinsip “No System is Safe” menekankan bahwa setiap sistem selalu memiliki celah yang dapat dimanfaatkan oleh penyerang, meskipun sudah diperkuat dengan standar keamanan seperti ISO 27001 (Wijoyo, Abdillah, Khalbi, Saputra, & Khoiriyah, 2024). Bagi Telkomsel, hal ini berimplikasi serius: kebocoran data pelanggan, kerugian finansial, gangguan operasional, hingga kerusakan reputasi perusahaan (Siponen, Mahmood, & Pahnla, 2014; Maalem Lahcen, Caulkins, Mohapatra, & Kumar, 2020).

Penelitian sebelumnya menunjukkan bahwa keberhasilan respons terhadap insiden keamanan tidak hanya ditentukan oleh faktor teknis, melainkan juga oleh kualitas pengambilan keputusan manajerial (Li, He, Xu, & Ash, 2023). Teori bounded rationality menyatakan bahwa pengambil keputusan sering kali menghadapi keterbatasan informasi, waktu, dan kognitif, sehingga solusi yang dipilih lebih bersifat memadai (satisficing) daripada optimal (Hidayat, 2016). Dengan demikian, memahami bagaimana organisasi besar seperti Telkomsel mengambil keputusan dalam kondisi ketidakpastian menjadi penting.

Sebagian besar studi tentang keamanan digital di Indonesia masih berfokus pada aspek teknis dan regulasi (Sutra & Haryanto, 2023; Sudarmadi, Indonesia, Josias, & Runturambi, 2019), sementara kajian tentang dinamika pengambilan keputusan strategis dalam merespons isu keamanan relatif terbatas. Hal ini menimbulkan research gap, yaitu minimnya pemahaman empiris mengenai proses internal pengambilan keputusan pada perusahaan telekomunikasi dalam menghadapi isu keamanan digital yang berdampak luas.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis proses pengambilan keputusan PT Telkomsel dalam menghadapi isu keamanan digital dengan mengintegrasikan teori pengambilan keputusan, khususnya pendekatan rasional, intuitif, partisipatif, dan bounded rationality. Penelitian ini diharapkan dapat memperluas diskursus akademik mengenai manajemen keamanan digital sekaligus memberikan kontribusi praktis bagi pengelolaan risiko siber di sektor telekomunikasi.

LANDASAN TEORI

Teori Pengambilan Keputusan

Pengambilan keputusan merupakan proses fundamental dalam organisasi yang berhubungan dengan pemilihan alternatif terbaik untuk menyelesaikan masalah atau mencapai tujuan. Menurut Suganda, Hendriawan, Saefurridjal, dan Muchtarom (2023), pengambilan keputusan melibatkan pertimbangan rasional, evaluasi risiko, dan penentuan arah yang paling efektif untuk kepentingan organisasi. Dalam konteks organisasi besar, pengambilan keputusan tidak hanya dipengaruhi faktor logis, tetapi juga oleh pengalaman, intuisi, dan keterlibatan berbagai pemangku kepentingan (Marsyela, Marsyeli, & Maidiana, 2023).

Pendekatan dalam Pengambilan Keputusan

Berbagai pendekatan digunakan dalam proses pengambilan keputusan. Pendekatan rasional menekankan penggunaan data dan analisis sistematis sebelum memilih alternatif (Fuadah & Kolis, 2023). Sebaliknya, pendekatan intuitif lebih mengandalkan pengalaman dan insting pengambil keputusan dalam situasi yang penuh ketidakpastian (Solin et al., 2024). Pendekatan partisipatif melibatkan berbagai pihak dalam organisasi untuk memastikan keputusan diterima secara kolektif (Sutrisno & Lucitasari, 2019). Sementara itu, teori bounded rationality menjelaskan bahwa

keterbatasan informasi, waktu, dan kognisi membuat pengambil keputusan cenderung memilih solusi yang memadai (satisficing) daripada optimal (Hidayat, 2016).

Keamanan Digital dan Risiko Siber

Keamanan digital adalah upaya sistematis melindungi data, jaringan, dan sistem dari ancaman yang dapat merusak integritas, kerahasiaan, maupun ketersediaan informasi. Menurut Radanliev (2024), keamanan digital berperan penting dalam menjaga kepercayaan publik dan kontinuitas bisnis. Ancaman keamanan kini semakin kompleks, termasuk phishing, ransomware, dan serangan Distributed Denial of Service (DDoS) yang menargetkan sistem layanan publik (Wijoyo, Abdillah, Khalbi, Saputra, & Khoiriyah, 2024). Dalam konteks perusahaan telekomunikasi, risiko keamanan digital tidak hanya mengancam operasional, tetapi juga kepercayaan pelanggan dan reputasi organisasi (Cains, Flora, Taber, King, & Henshel, 2022).

Keterkaitan Keputusan Manajerial dengan Keamanan Digital

Keamanan digital tidak bisa dilepaskan dari kualitas proses pengambilan keputusan. Li, He, Xu, dan Ash (2023) menekankan bahwa efektivitas kebijakan keamanan sangat ditentukan oleh iklim organisasi dan kepatuhan karyawan terhadap arahan manajerial. Dalam situasi krisis keamanan siber, keputusan cepat dan tepat menjadi kunci mencegah kerugian yang lebih besar (Saputra, Situmorang, Kusumasari, & Hidayat, 2024). Oleh karena itu, pengambilan keputusan dalam menghadapi isu “No System is Safe” pada PT Telkomsel harus dipahami sebagai kombinasi pendekatan rasional, intuitif, partisipatif, dan bounded rationality yang saling melengkapi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur. Pendekatan ini dipilih karena fokus penelitian adalah memahami makna, konteks, serta dinamika pengambilan keputusan dalam menghadapi isu keamanan digital, bukan pada perhitungan numerik (Haki, Prahastiwi, & Selatan, 2024). Data penelitian bersumber dari literatur sekunder, yang mencakup artikel jurnal internasional dan nasional, buku akademik, laporan lembaga resmi, dokumen kebijakan perusahaan, serta pemberitaan media.

Proses pengumpulan data dilakukan melalui tahap literature search menggunakan kata kunci seperti “digital security,” “decision-making,” “bounded rationality,” dan “cybersecurity risk management.” Pencarian difokuskan pada publikasi dalam rentang tahun 2019–2024 agar relevan dengan perkembangan terbaru di bidang manajemen keamanan digital (Snyder, 2019). Literatur yang dipilih memenuhi kriteria inklusi berupa: (1) membahas isu keamanan digital dan pengambilan keputusan organisasi, (2) relevan dengan konteks perusahaan telekomunikasi atau sektor teknologi, dan (3) dipublikasikan dalam jurnal bereputasi, laporan institusional, atau buku akademik. Sementara itu, literatur dikecualikan apabila tidak terkait dengan isu manajerial atau bersifat opini populer yang tidak melalui proses peninjauan akademik.

Analisis data dilakukan dengan menggunakan teknik analisis isi (content analysis), yaitu mengidentifikasi, mengelompokkan, dan membandingkan tema-tema utama dari setiap literatur. Tahap analisis mencakup: (1) identifikasi konsep utama pengambilan keputusan dan keamanan digital, (2) pengkategorian berdasarkan pendekatan rasional, intuitif, partisipatif, dan bounded rationality, serta (3) penarikan kesimpulan dengan menghubungkan teori dan praktik yang terjadi di PT Telkomsel (Krippendorff, 2019). Validitas hasil dijaga dengan melakukan triangulasi sumber, yaitu membandingkan data dari jurnal akademik, dokumen resmi perusahaan, dan laporan

institusi keamanan siber, sehingga diperoleh gambaran yang lebih komprehensif (Bowen, 2019).

Dengan metode ini, penelitian tidak hanya menyajikan kerangka konseptual mengenai pengambilan keputusan dalam menghadapi isu “No System is Safe”, tetapi juga memberikan pemahaman yang aplikatif tentang bagaimana keputusan strategis Telkomsel diambil dalam kondisi ketidakpastian dan risiko tinggi.

HASIL PENELITIAN

Hasil penelitian menunjukkan bahwa proses pengambilan keputusan di PT Telkomsel dalam menghadapi isu keamanan digital “No System is Safe” mencerminkan kombinasi dari berbagai teori, dasar, gaya, dan pendekatan pengambilan keputusan.

Pertama, gaya direktif terlihat saat manajemen Telkomsel segera menutup akses sistem yang dianggap bermasalah untuk mencegah eskalasi risiko. Hal ini sejalan dengan temuan Tika Widiyan, Muli Prima, dan Rafi (2025) yang menekankan bahwa gaya direktif digunakan dalam situasi dengan toleransi rendah terhadap ketidakpastian.

Kedua, gaya analitis tampak melalui investigasi forensik digital dan analisis log sistem oleh tim CSIRT. Pendekatan ini mendukung proses pengambilan keputusan berbasis data sebagaimana dikemukakan Dina dan Rusmiwari (2017), bahwa metode rasional melibatkan identifikasi masalah, pencarian alternatif, dan pemilihan solusi yang objektif.

Ketiga, gaya konseptual tercermin dari langkah Telkomsel menjadikan isu keamanan sebagai peluang untuk memperkuat kolaborasi dengan vendor global serta lembaga pengawas nasional. Hal ini selaras dengan pendekatan partisipatif, di mana keputusan melibatkan berbagai pemangku kepentingan agar lebih komprehensif (Sutrisno & Lucitasari, 2019).

Keempat, gaya perilaku diterapkan melalui edukasi dan pelatihan keamanan digital bagi karyawan serta sosialisasi kepada pelanggan. Penerapan ini menunjukkan prinsip bounded rationality (Hidayat, 2016), di mana organisasi memilih solusi memadai di tengah keterbatasan informasi dan ancaman yang terus berubah.

Dengan demikian, hasil penelitian memperlihatkan bahwa pengambilan keputusan Telkomsel tidak bersifat tunggal, melainkan adaptif dengan menggabungkan rasionalitas, intuisi, partisipasi, dan rasionalitas terbatas dalam merespons dinamika risiko siber.

Pembahasan

Hasil penelitian ini mengonfirmasi bahwa efektivitas pengelolaan keamanan digital di Telkomsel tidak hanya ditentukan oleh kesiapan teknis, tetapi juga oleh kualitas proses pengambilan keputusan manajerial. Pendekatan multi-gaya (direktif, analitis, konseptual, dan perilaku) yang diterapkan Telkomsel menunjukkan adanya upaya adaptasi terhadap situasi ketidakpastian, sesuai dengan teori bounded rationality yang dikemukakan Simon (dalam Hidayat, 2016).

Temuan ini sejalan dengan penelitian Siponen, Mahmood, dan Pahnla (2014), yang menegaskan bahwa kepatuhan terhadap kebijakan keamanan informasi sangat dipengaruhi oleh keputusan manajerial dan iklim organisasi, bukan semata oleh sistem teknis. Hal serupa diungkapkan oleh Li, He, Xu, dan Ash (2023), bahwa kejelasan komunikasi dan iklim keamanan organisasi merupakan faktor penentu keberhasilan kebijakan keamanan informasi.

Di sisi lain, hasil ini memperkaya kajian keamanan digital di Indonesia yang sebelumnya lebih banyak menekankan aspek teknis. Penelitian Sudarmadi, Indonesia, Josias, dan Runturambi (2019) menekankan pentingnya strategi BSSN dalam menghadapi ancaman siber, sedangkan penelitian Sutra dan Haryanto (2023) menekankan regulasi nasional. Penelitian ini memberikan perspektif berbeda dengan menyoroti aspek pengambilan keputusan strategis di dalam organisasi, khususnya dalam konteks operator telekomunikasi besar.

Lebih jauh, temuan ini juga mengindikasikan bahwa implementasi keamanan digital Telkomsel menghadapi kendala berupa keterbatasan informasi, potensi human error, serta tekanan reputasi. Hal ini sejalan dengan studi Maalem Lahcen, Caulkins, Mohapatra, dan Kumar (2020) yang menekankan faktor perilaku dan psikologis dalam manajemen risiko keamanan siber.

Dengan menghubungkan temuan empiris Telkomsel dengan penelitian terdahulu, dapat disimpulkan bahwa keputusan manajerial yang cepat, partisipatif, dan adaptif merupakan faktor kritis dalam menjaga kepercayaan publik serta keberlanjutan operasional perusahaan telekomunikasi di era digital.

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa keamanan digital merupakan kebutuhan strategis bagi PT Telkomsel dalam menjaga kepercayaan pelanggan, melindungi data pribadi, serta memastikan keberlangsungan operasional perusahaan di tengah meningkatnya ancaman siber. Proses pengambilan keputusan terbukti memainkan peran krusial, karena respon yang cepat, tepat, dan adaptif mampu meminimalisasi dampak kerugian finansial maupun reputasi.

Penelitian ini menunjukkan bahwa Telkomsel tidak hanya mengandalkan standar teknis seperti ISO 27001, tetapi juga menerapkan kombinasi berbagai gaya dan pendekatan pengambilan keputusan mulai dari direktif, analitis, konseptual, hingga perilaku dengan landasan rasional, intuitif, partisipatif, serta bounded rationality. Integrasi ini memungkinkan perusahaan menyeimbangkan kebutuhan akan kecepatan, akurasi, partisipasi, dan fleksibilitas dalam menghadapi ketidakpastian keamanan digital.

Secara teoretis, penelitian ini memperkaya kajian pengambilan keputusan organisasi dengan menunjukkan bagaimana teori bounded rationality relevan dalam konteks keamanan digital pada perusahaan telekomunikasi besar. Secara praktis, temuan ini memberikan gambaran bahwa efektivitas manajemen risiko siber tidak hanya ditentukan oleh aspek teknologi, tetapi juga oleh kualitas keputusan manajerial dan keterlibatan seluruh pemangku kepentingan.

Adapun keterbatasan penelitian ini terletak pada penggunaan data sekunder yang bersumber dari literatur dan dokumen publik, sehingga belum sepenuhnya menggambarkan dinamika internal organisasi secara empiris. Oleh karena itu, penelitian selanjutnya disarankan untuk melakukan pendekatan studi kasus dengan wawancara mendalam terhadap manajemen dan praktisi keamanan digital di perusahaan telekomunikasi, agar diperoleh pemahaman yang lebih holistik dan aplikatif.

Dengan demikian, penelitian ini menegaskan bahwa pengambilan keputusan yang efektif, adaptif, dan berbasis kolaborasi menjadi faktor kunci dalam menjaga ketahanan digital Telkomsel, serta dapat dijadikan referensi bagi perusahaan lain di industri telekomunikasi maupun sektor strategis lainnya di era digital.

DAFTAR PUSTAKA

- Adisty, P. C. (2024). *Digital security*. Jakarta: Prenada Media.
- Bowen, G. A. (2019). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40.
- Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42(8), 1643–1669.
- Dina, & Rusmiwari, S. (2017). Pengambilan keputusan rasional dan bounded terhadap kinerja pegawai. *Jurnal Ilmu Sosial dan Ilmu Politik*, 6(2), 103–112.
- Fuadah, L., & Kolis, N. (2023). Gaya pengambilan keputusan dalam lembaga pendidikan Islam: Studi atas perilaku pengelola lembaga pendidikan Islam. *Excelencia: Journal of Islamic Education & Management*, 3(1), 37–50.
- Haki, U., Prahastiwi, E. D., & Selatan, U. T. (2024). Strategi pengumpulan dan analisis data dalam penelitian kualitatif pendidikan. *Jurnal Inovasi dan Teknologi Pendidikan*, 3(1), 1–19.
- Hidayat, R. (2016). Rasionalitas: Overview terhadap pemikiran dalam 50 tahun terakhir. *Buletin Psikologi*, 24(2), 101–122.
- Krippendorff, K. (2019). *Content analysis: An introduction to its methodology* (4th ed.). Thousand Oaks, CA: Sage Publications.
- Li, Y., He, W., Xu, H., & Ash, I. (2023). Information security policy compliance and the role of security climate. *Journal of Information Security*, 30(1), 1–12.
- Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(1), 1–14.
- Marsyela, Marsyeli, & Maidiana. (2023). Pengambilan keputusan dalam perilaku organisasi. *Jurnal Bahasa Indonesia*, 1(2), 56–62.
- PT Telekomunikasi Selular. (2023). *Perjalanan 28 tahun evolusi teknologi Telkomsel menuju perusahaan telekomunikasi digital terdepan*. Jakarta: PT Telkomsel.
- Radanliev, P. (2024). Digital security by design. *Security Journal*, 37(2), 215–230.
- Saputra, A., Situmorang, G., Kusumasari, I., & Hidayat, R. (2024). Proses pengambilan keputusan yang diterapkan dalam organisasi dan manajemen. *Journal of Indonesian Management*, 4(3), 8–16.
- Siponen, M., Mahmood, M., & Pahlila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, 51(2), 217–224.
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.
- Solin, T., Munthe, A., Harahap, A., Sitorus, S., Harahap, S., Angkat, D., & Ginting, S. (2024). Penerapan teori pengambilan keputusan dalam lingkungan bisnis. *Relevan: Jurnal Pendidikan*, 4(4), 6–14.
- Sudarmadi, D. A., Indonesia, U., Josias, A., & Runturambi, S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) dalam menghadapi ancaman siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, 2(2), 45–60.
- Suganda, N., Hendriawan, E., Saefurridjal, A., & Muchtarom, M. (2023). Konsep dasar-dasar pertimbangan dan strategi pengambilan keputusan dalam kepemimpinan pendidikan. *Jurnal Ilmiah Mandala Education*, 9(2), 134–145.
- Sutra, S. M., & Haryanto, A. (2023). Upaya peningkatan keamanan siber Indonesia oleh BSSN tahun 2017–2020. *Global Political Studies Journal*, 7(1), 56–69.

- Sutrisno, S., & Lucitasari, D. (2019). Pengembangan model pengambilan keputusan multi kriteria dalam menentukan trade-off tujuan berkonflik menggunakan global criterion method. *Jurnal Matematika*, 9(2), 101–110.
- Tika Widiyan, M., Muli Prima, A. M., & Muhammad, R. (2025). Etika pengambilan keputusan dalam Islam: Relevansi dan aplikasinya dalam praktik manajerial kontemporer. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(2), 948–959.
- Wijoyo, A., Abdillah, B., Khalbi, F., Saputra, R. A., & Khoiriyah, W. (2024). Keamanan cyber dalam sistem informasi manajemen: Ancaman dan solusi terbaru. *Jurnal Ilmiah Wahana Pendidikan*, 10(23), 1–23.