INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 215-221, ISSN: 3123-5573 (Online)

Analisis Keamanan Sistem Informasi Terhadap Serangan *Insider Threat*

Rakhamdi Rahman[1], Drahayu Lestari[2], Citra Indah Lestari[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie
rakhmadi.rahman@ith.ac.id[1], drahayulestarii.0420@gmail.com[2], citraindahlm@gmail.com[3]

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:
information system security, insider threat, risk management, MITRE ATT&CK, NIST SP 800-30

ABSTRACT

Information system security has become a critical aspect for organizations due to the increasing reliance on digital technology in managing data and business processes. One of the most complex and high-risk security threats is the insider threat, which originates from internal individuals who possess legitimate access to information systems. This type of threat is difficult to detect because malicious activities often resemble normal authorized user behavior. This study aims to analyze information system security against insider threats and to identify their characteristics, risks, and effective mitigation strategies. The research adopts a qualitative approach by utilizing the MITRE ATT&CK for Insider Threat framework to identify threat patterns and the NIST Special Publication 800-30 framework for risk assessment. The results indicate that weak access control management, insufficient user activity monitoring, and low information security awareness are the main factors contributing to insider threat risks. Therefore, a holistic security approach that integrates people, processes, and technology is essential to effectively mitigate insider threats and ensure the resilience of information systems.

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
keamanan sistem informasi, insider threat, manajemen risiko, MITRE ATT & CK, NIST SP 800-30

ABSTRAK

Keamanan sistem informasi merupakan aspek penting bagi organisasi seiring meningkatnya ketergantungan terhadap teknologi digital dalam pengelolaan data dan proses bisnis. Salah satu ancaman yang paling kompleks dan berisiko tinggi adalah *insider threat*, yaitu ancaman yang berasal dari individu internal organisasi yang memiliki akses sah terhadap sistem informasi. Ancaman ini sulit dideteksi karena aktivitas pelaku sering menyerupai perilaku normal pengguna yang berwenang. Penelitian ini bertujuan untuk menganalisis keamanan sistem informasi terhadap ancaman *insider threat* serta mengidentifikasi karakteristik, risiko, dan strategi mitigasi yang efektif. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan mengacu pada kerangka MITRE ATT&CK for *Insider Threat* untuk identifikasi pola ancaman dan NIST SP 800-30 untuk penilaian risiko. Hasil analisis menunjukkan bahwa lemahnya pengelolaan hak akses, kurangnya pemantauan aktivitas pengguna, serta rendahnya kesadaran keamanan informasi menjadi faktor utama yang meningkatkan risiko *insider threat*. Oleh karena itu, diperlukan pendekatan keamanan yang holistik dengan mengintegrasikan aspek manusia, proses, dan teknologi guna meningkatkan perlindungan sistem informasi dari ancaman internal.

INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 215-221, ISSN: 3123-5573 (Online)

Corresponding Author:
Rakhamdi Rahman
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie
rakhmadi.rahman@ith.ac.id

PENDAHULUAN

Kemajuan teknologi informasi yang berkembang pesat telah membawa perubahan signifikan dalam pelaksanaan kegiatan operasional dan manajerial pada berbagai organisasi. Sistem Informasi kini tidak hanya berfungsi sebagai sarana pendukung, tetapi telah menjadi komponen krusial dalam pengelolaan data, proses pengambilan keputusan strategis, serta peningkatan efisiensi dan efektivitas kinerja organisasi. Beragam informasi penting, mulai dari data pengguna, data keuangan, hingga data operasional dan strategis lainnya, disimpan dan diolah melalui sistem informasi berbasis teknologi digital. Oleh karena itu, keberlangsungan operasional dan keamanan sistem informasi menjadi faktor penting yang menentukan kelangsungan hidup suatu organisasi (Whitman & Mattord, 2018). Seiring meningkatnya ketergantungan organisasi terhadap sistem informasi, risiko terhadap keamanan informasi juga semakin besar. Ancaman keamanan dapat mengganggu aspek kerahasiaan, integritas, dan ketersediaan data, yang berpotensi menimbulkan kerugian finansial, gangguan terhadap aktivitas operasional, serta penurunan tingkat kepercayaan publik. Selama ini, upaya pengamanan sistem informasi umumnya lebih difokuskan pada serangan yang berasal dari pihak eksternal. Namun, berbagai penelitian menunjukkan bahwa ancaman juga dapat muncul dari dalam organisasi, yang dikenal sebagai *insider threat*. Ancaman ini dapat berasal dari karyawan aktif, mantan karyawan, kontraktor, maupun pihak ketiga yang memiliki akses resmi terhadap sistem informasi. Insider threat dapat terjadi secara sengaja dengan tujuan merugikan organisasi, seperti pencurian data sensitif, manipulasi informasi, maupun tindakan perusakan sistem. Selain itu, ancaman internal juga dapat muncul secara tidak disengaja akibat kelalaian pengguna, rendahnya tingkat kesadaran terhadap keamanan informasi, serta kesalahan dalam penggunaan sistem informasi (Peltier, 2016). Tingkat kompleksitas *insider threat* menjadikannya sulit untuk diidentifikasi, mengingat pelaku memiliki hak akses yang sah dan pemahaman mendalam terhadap proses kerja serta celah keamanan sistem. Aktivitas yang dilakukan sering kali tampak sebagai aktivitas normal pengguna, sehingga menyulitkan proses pendeteksian perilaku berbahaya (Cappelli, Moore, & Trzeciak, 2012).

Di samping aspek teknis, kemunculan *insider threat* juga dipengaruhi oleh faktor manusia dan organisasi, seperti tingkat kepuasan kerja, budaya organisasi, lemahnya pengawasan internal, serta kurang efektifnya kebijakan dan prosedur keamanan informasi. Pengelolaan hak akses yang tidak optimal, keterbatasan sistem pemantauan, serta minimnya program edukasi keamanan informasi bagi pengguna dapat meningkatkan potensi terjadinya ancaman internal. Oleh sebab itu, pengamanan sistem informasi tidak dapat hanya mengandalkan solusi teknologi semata, tetapi harus didukung oleh penguatan kebijakan, prosedur, serta pengelolaan sumber daya manusia secara menyeluruh. Berdasarkan kondisi tersebut, analisis keamanan sistem informasi terhadap ancaman *insider threat* menjadi langkah penting untuk memahami karakteristik ancaman, mengidentifikasi potensi risiko, serta merumuskan strategi pencegahan dan mitigasi yang efektif. Dengan penerapan sistem keamanan yang komprehensif, organisasi diharapkan

mampu melindungi aset informasinya dari ancaman internal serta menjaga keberlangsungan operasional sistem informasi secara optimal.

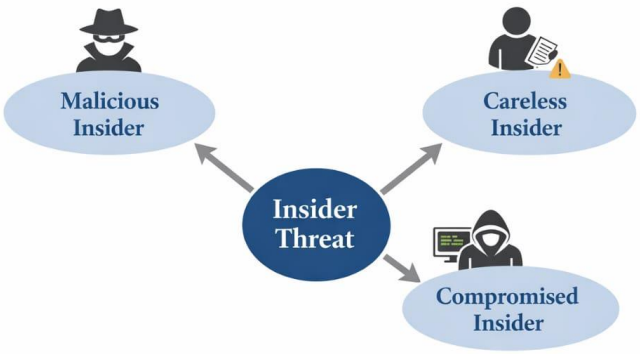
TINJAUAN PUSTAKA

2.1 Konsep Keamanan Sistem Informasi

Keamanan sistem informasi merupakan upaya terstruktur yang bertujuan untuk melindungi aset informasi dari berbagai ancaman yang dapat menggnggu proses penyimpanan, pengolahan, dan distribusi data. Tujuan utama dari keamanan sistem informasi adalah menjaga kerahasiaan, integritas data, dan ketersediaan informasi agar dapat digunakan secara andal oleh pihak yang berwenang. Dalam organisasi modern, informasi memiliki nilai strategis yang tinggi sehingga perlindungan terhadap sistem informasi menjdi aspek yang sangat krusial (Whitman & Mattord, 2018). Prinsip dasar keamanan sistem informasi dikenal sebagai CIA Triad yang terdiri dari *confidentiality, integrity, dan availability,* yang menjadi fondasi dalam perancangan serta evaluasi sistem keamanan informasi (Stallings, 2017). Selain itu, penerapan model keamanan seperti Bell-LaPadula, Biba, Clark-Wilson, dan *Defense in Depth* membantu organisasi dalam menerapkan keamanan informasi secara sistematis dan berlapis sesuai dengan kebutuhan dan risiko yang dihadapi.

2.2 Insider Threat: Definisi dan Jenis

Insider threat merupakan ancaman keamanan sistem informasi yang berasal dari individu internal organisasi yang memiliki akses sah terhadap sistem dan data. Ancaman ini tergolong berbahaya karena pelaku insider memiliki pemahaman terhadap struktur sistem, kebijakan keamanan, serta potesi celah yang ada, sehingga sulit untuk dideteksi (Capelli, Moore & Trzeciak, 2012). *Insider threat* tidak selalu dilakukan dengan niat jahat, tetapi juga dapat terjadi akibat kelalaia pengguna atau kompromi akuun oleh pihak eksternal.Berdasarkan karakteristiknya, *insider threat* dapat diklasifikasikan enjadi *malicious insider* yang bertindak secara sengaja, *careless insider* yang menimbulkan ancaman akibat kelalaian, serta *compromised insider* yang terjadi ketika akun internal diambil alih oleh pihak eksternal (Whitman & Mattord, 2018; Peltier,2016).



Gambar 1. Klasifikasi Insider Threat dalam sistem informasi

2.3 Karakteristik dan Motif Insider Threat

Insider threat memiliki karakteristik utama berupa kepemilikan akses sah terhadap sistem informasi serta pemahaman mendalam terhadap proses bisnis organisasi. Kondisi ini menyebabkan aktivitas normal pengguna yang berwenang (Capelli et. al., 2012). Selain aspek teknis *insider threat* juga dipengaruhi oleh faktor manusia dan organisasi, seperti budaya kerja, tingkat kepuasan kerja, tekanan kerja, serta lemahnya pengawasan internal. Motif *insider threat* umumnya meliputi motif finansial, balas dendam, kelalaian, dan tekanan kerja, yang masing-masing dapat mendorong individu untuk menyalahgunakan atau mengabaikan kebijakan keamanan informasi (Whitman & Mattord, 2018; Stallings, 2017).

2.4 Dampak Insider Threat terhadap Organisasi

Insider threat dapat menimbulkan dampak signifikan bagi organisasi, baik dari sisi finansial, hukum, reputasi, maupun operasional. Kebocoran data dan manipulasi sistem dapat menyebabkan kerugian ekonomi yang besar serta meningkatkan biaya pemulihan dan pengamanan sistem. Selain itu, insiden *insider threat* dapat memicu konsekuensi hukum akibat pelanggaran regulasi perlindungan data serta menurunkan kepercayaan publik dan mitra bisnis terhadap organisasi. Dari sisi operasional, *insider threat* juga berpotensi mengganggu layanan sistem dan menurunkan produktivitas kerja organisasi (Capell et. al., 2012; Peltier, 2016).

2.5 Teknik Deteksi dan Mitigasi Insider Threat

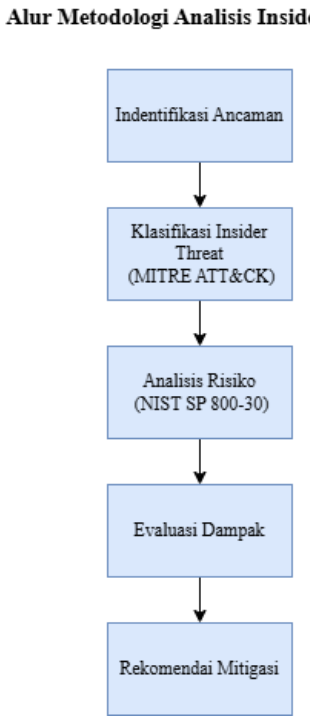
Untuk mengurangi risiko *insider threat*, organisasi perlu menerapkan teknik deteksi dan mitigasi yang mencakup aspek teknis dan non-teknis. Beberapa pendekatan yang umum digunakan antara lain *User and Entity Behavior Analytics* (UEBA) untuk mendeteksi anomali perilaku pengguna, *Security Information and Event Management* (SIEM) untuk memantau dan menganalisis log keamanan, serta *Role-Based Access Control* (RBAC) guna membatasi hak akses sesuai peran pengguna. Selain itu, penerapan *audit trail* dan program *awareness training* juga bereperan penting dalam mendeteksi aktivitas mencurigakan serta meningkatkan kesadaran keamanan informasi di lingkungan organisasi (Whitman & Mattord, 2018; Peltier, 2016).

METODE ANALISIS DATA

Metode analisis data dalam penelitian ini menggunakan pendekatan kualitatif untuk mengkaji ancaman *insider threat* terhadap keamanan sistem informasi secara sistematis. Analisis dilakukan dengan mengacu pada kerangka kerja keamanan informasi yang diakui secara internasional guna menghasilkan rekomendasi mitigasi yang relevan bagi organisasi. Tahap awal analisis dilakukan melalui identifiksi dan kategorisasi ancaman *insider threat* menggunakan kerangka *MITRE ATT&CK for Insider Threat.* Kerangka ini digunakan untuk memetakan taktik, teknik, dan prosedur (*tactics, techniques, and procedures*) yang umum dilakukan oleh pelaku insider, sehingga pola perilaku ancaman dapat dipahami secara lebih terstruktur (MITRE, 2023).

Selanjutnya, penilaian risiko dilakukan menggunakan kerangka *NIST Special Publication 800-30* dengan pendekatan kualitatif. Analisis risiko mencakup identifikasi sumber ancaman, kerentanan sistem, dampak yang ditimbulkan, serta kemungkinan

terjadinya ancaman. Hasil penilaian ini digunakan untuk menentukan tingkat risiko *insider threat* dan menetapkan prioritas mitigasi (NIST, 2012). Tahap akhir dilakukan melalui analisis komparatif terhadap strategi mitigasi *insider threat*, baik dari aspek tekns seperti UEBA, SIEM, dan kontrol akses, maupun aspek non-teknis seperti kebijakan keamanan dan pelatihan kesadaran keamanan. Analisis ini bertujuan untuk merumuskan rekomendasi mitigasi yang efektif dan sesuai dengan kebutuhan organisasi (Whitman & Mattord, 2018).



Gambar 2. Alur Metodologi Analisis Insider Threat

PEMBAHASAN

Hasil analisis menunjukkan bahwa *insider threat* merupakan ancaman yang kompleks dan sulit didetksi karena pelaku memiliki hak akses sah serta pemahaman terhadap sistem informasi organisasi. Aktivitas insider cenderung dilakukan secara bertahap dan tidak mencolok (*low and slow*), seperti pengumpulan data secara perlahan atau penggunaan akses di lua jam kerja normal, sehingga sulit teridentifikasi oleh mekanisme keamanan konvensional (Capelli et. al., 2012; Greitzer & Hohimer, 2011). Selain itu, lemahnya kebijakan internal, pengelolaan hak akses yang tidak optial, serta kurangnya monitoring dan logging memperbesar peluang terjadinya penyalahgunaan sistem oleh pihak internal yang menegaskan bahwa *insider threat* tidak hanya bersifat teknis, tetapi juga berkaitan erat dengan aspek manajerial dan organisasi.

Temuan peneltian ini sejalan dengan hasil penelitian nasional yang menunjukkan bahwa tata kelola akses internal memiliki peran penting dalam mitigasi *insider threat*. Laksono dan Sari(2025) menegaskan bahwa penerapan kerangka tata kelola akses yag mempertimbangkan konteks dan perilaku pengguna mampu meningkatkan efektivitas deteksi ancaman internal dibandingkan kontrol akses tradisional. Selain itu, penelitian

nasional lainnya menyoroti bahwa keterbatassan kapasitas dan kesadaran pegawai dalam pengelolaan keamanan jaringan menjadi faktor signifikan yang meningkatkan kerentanan organisasi terhadap *insider threat*, meskipun standar keamanan informasi telah diterapkan (Sitorus & Harwahyu, 2025). Hal ini memperkuat pandangan bahwa faktor manusia merupakan elemen kritis dalam keamanan sistem informasi.

Implikasi praktis dari temuan ini menunjukkan bahwa organisasi perlu mengadopsi pendekatan keamanan yang holistik dengan mengombinasikan teknologi deteksi lanjutan, seperti *User and Entity Behavior Analytics* (UEBA), dengan penguatan kebijakan manajemen akses serta peningkatan kesadaran keamanan informasi bagi pengguna. Pendekatan ini sejalan dengan model *People-Process-Technology* yang menekankan bahwa kegagalan pada salah satu elemen dapat melemahkan keseluruhan sistem keamanan. Oleh karena itu, pengelolaan risiko *insider threat* yang efektif tidak hanya bergantung pada teknologi, tetapi juga pada kebijakan organisasi dan pengelolaan sumber daya manusia secara berkelanjutan (Peltier, 2016; NIST, 2018).

KESIMPULAN

Berdasarkan hasil analisis keamanan sistem informasi terhadap ancaman *insider threat* yang telah dilakukan, dapat disimpulkan bahwa insider threat merupakan salah satu bentuk ancaman yang paling kompleks dan berisiko tinggi bagi organisasi. Tingginya tingkat risiko ini disebabkan oleh karakteristik pelaku insider yang memiliki akses sah serta pemahaman mendalam terhadap sistem, proses, dan kebijakan internal organisasi, sehingga aktivitas berbahaya yang dilakukan sering kali sulit terdeteksi oleh mekanisme keamanan konvensional. Hasil analisis menunjukkan bahwa aset informasi kritis, seperti basis data pelanggan, data keuangan, dan informasi strategis organisasi, memiliki tingkat kerentanan yang tinggi terhadap penyalahgunaan oleh pihak internal, yang berpotensi menimbulkan dampak signifikan terhadap kerahasiaan, integritas, dan ketersediaan informasi.

Selain itu, identifikasi celah keamanan menunjukkan bahwa pengelolaan hak akses yang tidak optimal,kurangnya pemisahan tugas, serta lemahnya pencatatan dan pemantauan aktivitas pengguna menjadi faktor utama yang meningkatkan risiko terjadinya *insider threat*. Penerapan kerangka *MITRE ATT&CK for Insider Threat* dan *NIST SP 800-30* terbukti membantu dalam memberikan gambaran yang sistematis mengenai pola ancaman, tingkat risiko, dan potensi dampak terhadap sistem informasi organisasi. Namun demikian, hasil analisis juga menunjukkan bahwa tidak seluruh skenario *insider threat* dapat dideteksi secara optimal oleh sistem yang ada. Hal ini menegaskan bahwa pengelolaan risiko *insider threat* memerlukan pendekatan yang komprehensif dengan mengintegrasikan aspek manusia, proses, dan teknologi guna meningkatkan efektivitas keamanan sistem informasi secara keseluruhan.

DAFTAR PUSTAKA

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes*. Addison-Wesley. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=31681

Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security*, 4(2), 25–48. https://scholarcommons.usf.edu/jss/vol4/iss2/2/

Laksono, A. C., & Sari, B. W. (2025). Pengembangan framework tata kelola akses multi-tenant untuk mitigasi ancaman insider di cloud publik. *Jurnal Informatika Teknologi dan Sains (JINTEKS)*. https://jurnal.uts.ac.id/index.php/JINTEKS

MITRE. (2023). *MITRE ATT&CK® for insider threat*. MITRE Corporation. https://attack.mitre.org/

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. https://www.nist.gov/cyberframework

Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management*. CRC Press. https://doi.org/10.1201/b19505

Sitorus, F. N., & Harwahyu, R. (2025). Analysis of employee capacity gap in managing network security and its implementation towards insider threat prevention. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*. https://journal.irpi.or.id/index.php/malcom

Stallings, W. (2017). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley. https://www.pearson.com/en-us/subject-catalog/p/effective-cybersecurity/P200000003296

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning. https://www.cengage.com/c/principles-of-information-security-6e-whitman/