DAMPAK *INSIDER THREAT* TERHADAP KEAMANAN OBJEK VITAL: LITERATURE REVIEW

Aurell Kartika Reswara

Universitas Budi Luhur
E-mail : 2343500282@studentbudiluhur.ac.id

ABSTRAK

Objek vital merupakan aset strategis yang berperan penting dalam mendukung pelayanan publik, stabilitas ekonomi, dan keamanan nasional. Seiring meningkatnya pemanfaatan teknologi informasi, objek vital menghadapi ancaman *insider threat* yang berasal dari individu internal dengan hak akses sah terhadap sistem organisasi. Penelitian ini bertujuan menganalisis dampak *insider threat* terhadap objek vital melalui metode *literature review* dengan pendekatan kualitatif. Data diperoleh dari sepuluh artikel ilmiah yang relevan, kemudian dianalisis melalui proses identifikasi, evaluasi, dan sintesis temuan penelitian. Hasil kajian menunjukkan bahwa *insider threat* memberikan empat dampak utama, yaitu kebocoran informasi strategis, gangguan operasional objek vital, peningkatan risiko dan kerugian organisasi, serta ancaman terhadap keamanan infrastruktur kritis dan keamanan nasional. Dampak tersebut dipengaruhi oleh akses sah dan pemahaman pelaku terhadap sistem organisasi sehingga tindakan yang dilakukan cenderung sulit dideteksi. Oleh karena itu, perlindungan objek vital memerlukan pendekatan pengamanan yang mengintegrasikan aspek manusia, teknologi, dan tata kelola organisasi guna meminimalkan risiko yang ditimbulkan oleh *insider threat.*

Kata Kunci : *Insider Threat, Objek Vital, Keamanan Nasional, Literature Review*

ABSTRACT

Critical infrastructure constitutes strategic assets that support public services, economic stability, and national security. Along with the increasing adoption of information technology, critical infrastructure faces the growing risk of insider threats, originating from authorized individuals with legitimate access to organizational systems. This study aims to analyze the impacts of insider threats on critical infrastructure using a qualitative literature review approach. Data were collected from ten relevant scientific articles and analyzed through identification, evaluation, and synthesis of previous research findings. The results indicate that insider threats generate four major impacts: the compromise of sensitive information, disruption of critical infrastructure operations, increased organizational risks and losses, and threats to critical infrastructure and national security. These impacts are exacerbated by insiders' legitimate access and extensive knowledge of organizational systems, making malicious activities difficult to detect. Therefore, protecting critical infrastructure requires an integrated security approach that combines human factors, technological controls, and organizational governance to reduce the risks posed by insider threats.

Keywords : *Insider Threat, Critical Infrastructure, National Security, Information Security, Literature Review*

PENDAHULUAN

Sebagai infrastruktur strategis dan aset milik negara, objek vital memegang peranan penting dalam menjamin kelangsungan hidup masyarakat serta mendukung pelaksanaan fungsi pemerintahan. Oleh karena itu, adanya hambatan pada aspek keamanan maupun operasional objek vital dapat memicu dampak yang meluas terhadap stabilitas sosial, kondisi ekonomi, penyediaan pelayanan publik, hingga sistem keamanan nasional. Menurut Cybersecurity and Infrastructure Security Agency (2024), infrastruktur kritis merupakan aset dan sistem yang sangat penting, sehingga kelumpuhan atau kerusakan di dalamnya akan memberikan implikasi besar terhadap keamanan, ekonomi, kesehatan masyarakat, dan keselamatan umum. Di Indonesia, objek vital nasional didefinisikan sebagai kawasan, lokasi, bangunan, instalasi, dan/atau usaha yang menyangkut hajat hidup orang banyak, kepentingan negara, serta sumber pendapatan negara yang bersifat strategis sehingga memerlukan sistem pengamanan khusus (Kepolisian Negara Republik Indonesia, 2019). Seiring dengan perkembangan teknologi informasi yang ada, manajemen objek vital di sektor energi, transportasi, kesehatan, industri, telekomunikasi, dan lembaga pemerintahan kini tidak hanya bertumpu pada pengamanan fisik saja, melainkan sudah terintegrasi dengan sistem digital yang mengatur operasional lembaga. Integrasi digital ini di satu sisi memang berhasil meningkatkan efisiensi dan efektivitas layanan, tetapi di sisi lain juga melahirkan berbagai bentuk kerentanan keamanan baru yang berisiko mengganggu keberadaan objek vital.

Dalam lingkup pengamanan objek vital, *insider threat* kini menjadi salah satu bentuk ancaman yang kian mendapatkan perhatian serius. Berbeda dari ancaman eksternal yang dipicu oleh pihak luar, *insider threat* berasal dari individu internal yang memiliki hak akses sah terhadap sistem, informasi, maupun fasilitas organisasi. Al-Mhiqani et al. (2024) memaparkan bahwa *insider threat* ini dapat dikategorikan dalam tiga bentuk, yakni *malicious insider*, *compromised insider*, serta *careless insider*. Tingkat bahaya dari ancaman ini tergolong tinggi karena pelaku sudah memahami alur prosedur kerja organisasi, mengetahui celah kelemahan sistem, dan memegang legitimasi akses yang membuat aktivitas mereka menjadi sangat sulit untuk dideteksi. Jika ditinjau dari perspektif kriminologi, fenomena *insider threat* dapat dikategorikan sebagai bentuk penyalahgunaan kesempatan oleh oknum yang telah mendapatkan kepercayaan serta wewenang di dalam organisasi, namun justru memanfaatkannya untuk melancarkan tindakan yang merugikan. Berbagai karakteristik inilah yang pada akhirnya menempatkan *insider threat* sebagai salah satu risiko kejahatan dengan tingkat kompleksitas yang tinggi dalam manajemen pengamanan objek vital.

Dampak yang ditimbulkan oleh *insider threat* di lingkungan objek vital umumnya memiliki konsekuensi yang jauh lebih serius apabila dibandingkan dengan organisasi komersial biasa. Ancaman internal yang menyerang *Cyber Physical Systems* (CPS) berpotensi besar mengacaukan operasional berbagai infrastruktur kritis, termasuk sektor energi, transportasi, kesehatan, dan industri (Al-Mhiqani et al., 2024). Dampak dari gangguan pada sektor-sektor strategis tersebut tidak hanya berdampak pada organisasi melainkan juga meluas hingga mempengaruhi masyarakat luas yang menggantungkan aktivitasnya pada layanan tersebut. Secara konkret, hambatan pada sistem energi dapat mengganggu proses distribusi listrik, kendala di sektor transportasi akan membatasi mobilitas publik, sedangkan gangguan pada sektor kesehatan dapat menurunkan mutu pelayanan medis. Atas dasar itulah, fenomena *insider threat* pada objek vital nasional tidak boleh hanya dinilai sebagai persoalan teknis keamanan informasi saja, melainkan

harus dipandang sebagai ancaman nyata yang mampu menggoyahkan stabilitas sosial, roda perekonomian, hingga ketahanan nasional.

Besarnya tingkat risiko yang ditimbulkan oleh *insider threat* ini juga diperkuat oleh berbagai temuan data terkini. Merujuk pada laporan *Cybersecurity and Infrastructure Security Agency (2024)* tercatat sebanyak 83% organisasi mengkonfirmasi telah mengalami minimal satu kali insiden *insider threat* dalam kurun waktu satu tahun terakhir, sementara hampir separuh dari jumlah organisasi tersebut menegaskan bahwa intensitas insiden ini terus menunjukkan tren peningkatan dari tahun ke tahun. Di samping itu rata-rata biaya yang harus dikeluarkan untuk menangani insiden kebocoran data di skala global telah menembus angka USD 4,88 juta(IBM, 2024). Statistik tersebut membuktikan bahwa ancaman dari pihak internal tidak sekadar mengakibatkan kerugian finansial dalam skala besar, melainkan juga berisiko tinggi mengganggu stabilitas operasional serta keberlangsungan organisasi yang menjadi target. Dampak ini tentunya berpotensi menjadi jauh lebih masif apabila menimpa sektor objek vital, sebab eksistensinya berhubungan langsung dengan aspek pelayanan publik, pemenuhan kepentingan strategis negara, serta jaminan keamanan masyarakat luas.

Salah satu contoh nyata yang menunjukkan besarnya dampak *insider threat* adalah kasus Edward Snowden pada tahun 2013. Snowden yang bekerja sebagai kontraktor di *National Security Agency* (NSA) Amerika Serikat membocorkan sejumlah besar dokumen rahasia yang berisi informasi mengenai program pengawasan dan kegiatan intelijen pemerintah Amerika Serikat. Pihak NSA memperkirakan bahwa Snowden telah membocorkan antara 50.000 hingga 200.000 dokumen rahasia kepada media. Keberhasilan Snowden memperoleh dokumen-dokumen rahasia tidak dilakukan melalui serangan eksternal terhadap sistem, melainkan melalui akses legitim yang dimilikinya sebagai personel internal organisasi(Mark Hosenball, 2013). Kasus ini menunjukkan bahwa ancaman terhadap objek vital dapat berasal dari individu yang memiliki kewenangan dan akses sah, sehingga penyalahgunaan hak akses menjadi salah satu risiko keamanan yang perlu diantisipasi oleh organisasi pengelola objek vital. Dampak yang ditimbulkan bahkan meluas hingga mempengaruhi keamanan nasional, hubungan diplomatik, serta kepercayaan publik terhadap institusi negara. Oleh karena itu, kasus Snowden sering dijadikan salah satu contoh paling signifikan mengenai bagaimana ancaman dari orang dalam dapat menimbulkan konsekuensi yang jauh lebih besar dibandingkan serangan eksternal terhadap organisasi yang memiliki fungsi strategis bagi negara.

Meskipun penelitian mengenai *insider threat* telah berkembang pesat, sebagian besar kajian masih berfokus pada pengembangan metode deteksi, autentikasi, prediksi, dan mitigasi ancaman (Inayat et al., 2024). Sementara itu, kajian yang secara khusus membahas dampak *insider threat* terhadap objek vital dan infrastruktur kritis masih relatif terbatas. Padahal, pemahaman mengenai dampak ancaman merupakan bagian penting dalam proses identifikasi risiko dan penyusunan strategi pengamanan objek vital. Oleh karena itu, penelitian ini bertujuan untuk menganalisis dampak *insider threat* terhadap objek vital melalui pendekatan *literature review*. Fokus penelitian diarahkan pada dampak ancaman terhadap kerahasiaan informasi, operasional objek vital, kerugian organisasi, serta keamanan infrastruktur kritis dan keamanan nasional. Hasil penelitian diharapkan dapat memberikan pemahaman yang lebih komprehensif mengenai risiko kejahatan yang berasal dari orang dalam sekaligus menjadi dasar dalam memperkuat sistem pengamanan objek vital.

METODE

Penelitian ini menggunakan metode literature review dengan pendekatan kualitatif untuk mengkaji dampak *insider threat* terhadap objek vital dan infrastruktur kritis. Literature review merupakan metode penelitian yang digunakan untuk mengidentifikasi, mengevaluasi, dan mensintesis hasil penelitian terdahulu guna memperoleh pemahaman yang komprehensif mengenai suatu topik penelitian (Snyder, 2019). Data yang digunakan berupa data sekunder yang diperoleh melalui penelusuran literatur menggunakan Google Scholar dengan kata kunci *insider threat*, *critical infrastructure*, *information security*, *cyber physical systems*, dan objek vital. Artikel yang digunakan berasal dari berbagai jurnal ilmiah nasional dan internasional serta dokumen pendukung yang relevan. Pemilihan artikel didasarkan pada relevansi topik, ketersediaan naskah lengkap dan kesesuaiannya dengan tujuan penelitian, sehingga diperoleh 10 artikel yang digunakan sebagai sumber utama dalam penelitian ini.

Analisis data dilakukan melalui tahapan identifikasi, evaluasi, pengelompokan, dan sintesis terhadap temuan dari setiap artikel yang telah dipilih. Setiap artikel dianalisis berdasarkan fokus penelitian, metode yang digunakan, serta dampak *insider threat* yang dilaporkan. Selanjutnya, temuan-temuan tersebut dikelompokkan ke dalam beberapa tema yang memiliki kesamaan untuk memperoleh gambaran yang lebih komprehensif mengenai dampak *insider threat* terhadap keamanan objek vital dan infrastruktur kritis. Hasil sintesis tersebut kemudian digunakan sebagai dasar dalam pembahasan penelitian.

Tabel 1. Daftar Jurnal yang Digunakan dalam *Literature Review*

No	Judul, Penulis, Tahun	Fokus Penelitian	Hasil Penelitian
1.	*Insider Threat Mitigation: Systematic Literature Review* (Inayat et al., 2024)	Berbagai penelitian mengenai strategi pencegahan *insider threat*.	Penelitian menemukan bahwa pencegahan *insider threat* dapat dilakukan melalui pendekatan berbasis jaringan, perilaku, anomali, analisis, kontrol akses, dan identifikasi niat pelaku. Ancaman internal dapat menyebabkan kebocoran data, sabotase, hingga pencurian kredensial sehingga diperlukan pengelolaan hak akses dan analisis perilaku pengguna secara berkelanjutan.
2.	*Insider Threat Detection in Cyber-Physical Systems: A Systematic Literature Review* (Al-Mhiqani et al., 2024)	*Cyber-Physical Systems* (CPS) pada sektor infrastruktur kritis.	Hasil penelitian menunjukkan bahwa *insider threat* merupakan ancaman serius pada CPS karena pelaku memiliki

			akses yang sah terhadap sistem. Dampaknya meliputi kerugian finansial, gangguan operasional, penurunan reputasi organisasi, serta terganggunya layanan pada infrastruktur kritis.
3.	*Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses* (Saxena et al., 2020)	Organisasi dan bisnis kritis yang menghadapi ancaman *insider threat.*	Penelitian mengidentifikasi tiga jenis *insider threat,* yaitu *malicious insider, compromised insider*, dan *careless insider*. Ancaman ini dipengaruhi oleh faktor teknis maupun faktor manusia seperti kepribadian, budaya organisasi, dan kondisi psikologis yang dapat mendorong terjadinya pencurian informasi, sabotase, dan keuntungan finansial ilegal.
4.	Analisis Keamanan Sistem Informasi terhadap Ancaman *Insider Threat (Rahman et al., 2026)*	Sistem informasi organisasi yang dianalisis menggunakan MITRE ATT & CK dan NIST SP 800-30.	Penelitian menunjukkan bahwa *insider threat* sulit dideteksi karena pelaku memiliki akses yang sah terhadap sistem. Risiko meningkat akibat lemahnya pengelolaan hak akses, kurangnya pemantauan aktivitas pengguna, dan rendahnya kesadaran keamanan informasi sehingga diperlukan pendekatan keamanan yang mengintegrasikan aspek manusia, proses, dan teknologi.
5.	Analisis Ancaman Serangan Siber Pada Infrastruktur Informasi	Menganalisis ancaman serangan siber terhadap Infrastruktur Informasi	Hasil penelitian menunjukkan bahwa serangan siber terhadap

	Vital Terhadap Stabilitas Keamanan Nasional (Anggaini Puspita et al., 2025)	Vital (IIV) di Indonesia serta dampaknya terhadap stabilitas keamanan nasional melalui studi kasus serangan siber pada Pusat Data Nasional Sementara (PDNS).	Infrastruktur Informasi Vital dapat mengganggu penyelenggaraan layanan publik, melemahkan keamanan nasional, serta menimbulkan kerugian bagi masyarakat dan pemerintah. Penelitian juga menekankan pentingnya penguatan tata kelola keamanan siber, manajemen risiko, deteksi dini, peningkatan kapasitas sumber daya manusia, serta kolaborasi antarinstansi untuk melindungi objek vital dan infrastruktur informasi vital di Indonesia.
6.	*Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis* (Gheyas & Abdallah, 2016)	Tiga puluh tujuh penelitian mengenai deteksi dan prediksi *insider threat.*	Penelitian menemukan bahwa aktivitas pengguna seperti akses file, email, database, dan jaringan merupakan indikator utama dalam deteksi *insider threat.* Pendekatan *anomaly detection* dan *Bayesian Network* dinilai efektif karena mampu mendeteksi pola ancaman baru yang belum pernah teridentifikasi sebelumnya.
7.	*Toward an Insider Threat Education Platform: A Theoretical Literature Review* (Gelman et al., 2024)	Literatur mengenai *insider threat* dari perspektif psikologis, teknologi, dan pendidikan.	Hasil penelitian menunjukkan bahwa *insider threat* dipengaruhi oleh faktor psikologis, motivasi, tekanan organisasi, dan peluang yang dimiliki pelaku. Oleh karena itu, program pelatihan keamanan yang menggabungkan aspek

			teknologi dan perilaku manusia diperlukan untuk meningkatkan kemampuan pencegahan ancaman internal.
8.	*A systematic Literature Review On Insider Threat* (Singh & Sharma, 2022)	Tiga puluh tujuh studi terkait *insider threat* dalam keamanan siber.	Penelitian menunjukkan bahwa pencurian data, penyalahgunaan hak akses, dan sabotase merupakan bentuk *insider threat* yang paling sering terjadi. Deteksi yang efektif dapat dilakukan melalui analisis perilaku pengguna, *machine learning,* pemantauan aktivitas sistem, dan penerapan kebijakan keamanan yang ketat
9.	*The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures* (Moore et al., 2008)	Tiga puluh kasus insider IT sabotage pada infrastruktur kritis Amerika Serikat.	Penelitian menemukan bahwa sebagian besar pelaku menunjukkan tanda-tanda perilaku mencurigakan sebelum melakukan sabotase, seperti ketidakpuasan kerja dan aktivitas teknis yang tidak wajar. Lemahnya pengawasan dan kontrol akses menjadi faktor utama yang mempermudah terjadinya serangan dari orang dalam
10.	*The Urgency of Defining Indonesia's National Critical Infrastructure* (Setiyawan, 2019)	Menganalisis urgensi penetapan dan definisi Infrastruktur Vital Nasional di Indonesia dalam menghadapi ancaman siber terhadap keamanan, pertahanan, dan kepentingan nasional melalui penelitian hukum normatif dengan pendekatan komparatif.	Hasil penelitian menunjukkan bahwa Indonesia masih menggunakan perspektif konvensional dalam menentukan objek vital nasional sebagaimana diatur dalam Peraturan Presiden Nomor 63 Tahun 2004 sehingga belum sepenuhnya mampu

	mengantisipasi ancaman siber modern. Oleh karena itu, pemerintah perlu mengevaluasi kebijakan yang ada serta menetapkan dan mendefinisikan Infrastruktur Vital Nasional secara lebih komprehensif sebagai dasar penguatan perlindungan terhadap kepentingan nasional di domain siber.

HASIL PENELITIAN DAN PENELITIAN

Dalam penelitian ini, sebanyak 10 artikel ilmiah yang relevan dengan topik *insider threat* pada objek vital dan infrastruktur kritis telah ditinjau menggunakan pendekatan *literature review*. Artikel-artikel tersebut membahas berbagai aspek *insider threat*, mulai dari karakteristik ancaman, faktor penyebab, dampak yang ditimbulkan, hingga metode deteksi dan strategi mitigasi yang dapat diterapkan. Hasil telaah menunjukkan bahwa *insider threat* menjadi salah satu ancaman yang paling kompleks karena berasal dari individu yang memiliki akses dan pemahaman terhadap sistem organisasi. Ancaman ini berpotensi menyebabkan kebocoran informasi, gangguan operasional, kerugian organisasi, serta risiko terhadap keamanan infrastruktur kritis. Berdasarkan artikel-artikel yang telah dianalisis, diperoleh temuan sebagai berikut:

1. Penelitian pertama dilakukan untuk mengidentifikasi berbagai teknik pencegahan *insider threat* yang telah dikembangkan dalam literatur. Melalui metode *systematic literature review*, penelitian ini mengelompokkan strategi mitigasi *insider threat* ke dalam enam kategori utama, yaitu *network based methods, behavior based methods, anomaly based methods, analysis based methods, access based methods*, dan *intention based methods*. Hasil penelitian menunjukkan bahwa *insider threat* dapat menyebabkan berbagai bentuk serangan seperti *data breach, sabotage, data loss, credential attack,* dan *data exfiltration* yang berdampak pada kerahasiaan, integritas, serta ketersediaan informasi organisasi. Selain itu, pengelolaan hak akses, analisis perilaku pengguna, dan deteksi anomali dinilai sebagai langkah penting dalam mencegah ancaman yang berasal dari orang dalam organisasi (Inayat et al., 2024).
2. Penelitian kedua membahas ancaman *insider threat* pada *Cyber Physical Systems* (CPS) yang banyak diterapkan pada sektor infrastruktur kritis seperti energi, transportasi, kesehatan, dan industri. Hasil penelitian menunjukkan bahwa pelaku *insider threat* memiliki tingkat risiko yang tinggi karena memperoleh akses yang sah terhadap sistem sehingga lebih sulit dideteksi dibandingkan ancaman eksternal. Ancaman tersebut berpotensi menyebabkan kerugian finansial, gangguan operasional, penurunan reputasi organisasi, hingga mengancam keberlangsungan layanan pada infrastruktur kritis. Oleh

karena itu, penelitian ini menekankan pentingnya pengembangan metode deteksi yang mampu mengidentifikasi aktivitas mencurigakan dalam lingkungan *Cyber Physical Systems (Al-Mhiqani et al., 2024).*

3. Penelitian ketiga dilakukan untuk mengidentifikasi karakteristik, jenis, dan tantangan utama *insider threat* pada organisasi dan infrastruktur kritis. Hasil penelitian menunjukkan bahwa *insider threat* dapat berasal dari *malicious insider, compromised insider,* maupun *careless insider*. Ancaman tersebut umumnya dipicu oleh motif pencurian informasi, sabotase sistem, pencurian kekayaan intelektual, serta keuntungan finansial. Penelitian ini juga menemukan bahwa faktor manusia seperti kepribadian, budaya organisasi, perilaku pengguna, dan kondisi psikologis memiliki pengaruh besar terhadap munculnya ancaman internal. Oleh karena itu, strategi mitigasi *insider threat* tidak cukup hanya mengandalkan teknologi, tetapi juga perlu memperhatikan aspek perilaku dan organisasi secara menyeluruh (Saxena et al., 2020).
4. Penelitian keempat bertujuan menganalisis keamanan sistem informasi terhadap ancaman *insider threat* dengan menggunakan kerangka MITRE ATT & CK *for Insider Threat* dan NIST SP 800-30. Hasil penelitian menunjukkan bahwa *insider threat* merupakan salah satu ancaman yang paling kompleks karena pelaku memiliki akses sah terhadap sistem sehingga aktivitasnya sulit dibedakan dari perilaku pengguna normal. Penelitian ini mengidentifikasi lemahnya pengelolaan hak akses, kurangnya pemantauan aktivitas pengguna, dan rendahnya kesadaran keamanan informasi sebagai faktor utama yang meningkatkan risiko *insider threat*. Oleh karena itu, penelitian merekomendasikan penguatan kontrol akses, peningkatan monitoring aktivitas pengguna, dan program peningkatan kesadaran keamanan untuk mengurangi resiko ancaman internal (Rahman et al., 2026).
5. Penelitian kelima bertujuan menganalisis ancaman serangan siber terhadap Infrastruktur Informasi Vital (IIV) serta dampaknya terhadap stabilitas keamanan nasional di Indonesia. Penelitian menggunakan pendekatan kualitatif melalui studi literatur dan wawancara ahli dengan menganalisis kasus serangan siber pada Pusat Data Nasional Sementara (PDNS). Hasil penelitian menunjukkan bahwa serangan siber terhadap IIV memiliki tingkat ancaman yang kritis akibat lemahnya tata kelola keamanan, kurangnya cadangan data, serta rendahnya kesadaran keamanan informasi. Penelitian juga menegaskan bahwa gangguan pada infrastruktur informasi vital dapat melumpuhkan layanan publik, mengganggu penyelenggaraan pemerintahan, serta berdampak terhadap stabilitas keamanan nasional. Oleh karena itu, diperlukan penguatan manajemen risiko, strategi intelijen, peningkatan deteksi dini, serta kolaborasi antarinstansi dalam menghadapi ancaman siber terhadap objek vital (Anggaini Puspita et al., 2025).
6. Penelitian keenam meninjau 37 studi terkait deteksi dan prediksi *insider threat* untuk mengidentifikasi tren penelitian, tantangan utama, serta algoritma yang paling efektif dalam mendeteksi ancaman dari orang dalam. Hasil penelitian menunjukkan bahwa aktivitas pengguna seperti akses file, penggunaan *database*, email, dan jaringan merupakan indikator yang paling banyak digunakan dalam proses deteksi. Selain itu, penelitian menemukan bahwa pendekatan *anomaly detection* dan algoritma berbasis *Bayesian Network* memiliki kemampuan yang baik dalam mendeteksi pola serangan yang belum pernah teridentifikasi sebelumnya. Penelitian juga menekankan pentingnya menggabungkan analisis perilaku individu, perilaku kelompok, penggunaan sumber daya

sistem, dan faktor psikologis pengguna untuk meningkatkan akurasi deteksi ancaman (Gheyas & Abdallah, 2016).

7. Penelitian ketujuh mengkaji *insider threat* dari perspektif psikologis, teknologi, dan pendidikan untuk mengembangkan platform pelatihan yang efektif dalam mendeteksi dan mencegah ancaman internal. Hasil penelitian menunjukkan bahwa *insider threat* tidak hanya dipengaruhi oleh faktor teknis, tetapi juga berkaitan dengan motivasi, karakteristik psikologis, tekanan organisasi, dan peluang yang dimiliki pelaku. Penelitian ini menemukan bahwa metode deteksi yang efektif perlu menggabungkan analisis perilaku pengguna, *machine learning*, *user behavior analytics*, serta identifikasi indikator psikologis seperti stres dan ketidakpuasan kerja. Selain itu, edukasi dan pelatihan keamanan dinilai memiliki peran penting dalam meningkatkan kesadaran karyawan terhadap ancaman dari orang dalam (Gelman et al., 2024).
8. Penelitian kedelapan melakukan kajian sistematis terhadap berbagai penelitian mengenai *insider threat* untuk mengidentifikasi bentuk ancaman, dampak, metode deteksi, dan strategi mitigasi yang digunakan dalam keamanan siber. Hasil penelitian menunjukkan bahwa pencurian data, penyalahgunaan hak akses, dan sabotase merupakan bentuk ancaman yang paling sering terjadi. Ancaman tersebut berpotensi menimbulkan kerugian finansial yang besar serta mengganggu operasional organisasi. Penelitian ini juga menegaskan bahwa kombinasi antara teknologi deteksi, analisis perilaku pengguna, dan manajemen keamanan organisasi merupakan pendekatan yang paling efektif dalam mengurangi risiko *insider threat* (Singh & Sharma, 2022).
9. Penelitian kesembilan menganalisis 30 kasus *insider IT sabotage* yang terjadi pada berbagai infrastruktur kritis di Amerika Serikat. Hasil penelitian menunjukkan bahwa sebagian besar pelaku melakukan tindakan sabotase setelah mengalami ketidakpuasan kerja, konflik organisasi, atau peristiwa negatif lainnya yang memicu keinginan untuk melakukan balas dendam. Selain itu, penelitian menemukan bahwa pelaku seringkali memanfaatkan akun tersembunyi, akses jarak jauh, maupun celah pengawasan yang tidak diketahui manajemen untuk melancarkan aksinya. Temuan tersebut menunjukkan bahwa lemahnya pengawasan dan kontrol akses dapat meningkatkan peluang terjadinya ancaman dari orang dalam pada infrastruktur kritis (Moore et al., 2008).
10. Penelitian kesepuluh bertujuan menganalisis urgensi penetapan dan definisi National Critical Infrastructure di Indonesia dalam menghadapi perkembangan ancaman siber terhadap kepentingan nasional. Penelitian menggunakan metode hukum normatif dengan pendekatan komparatif melalui analisis peraturan perundang-undangan dan konsep critical infrastructure yang diterapkan di berbagai negara. Hasil penelitian menunjukkan bahwa Indonesia masih menggunakan pendekatan konvensional dalam menetapkan objek vital nasional sehingga belum sepenuhnya mampu mengantisipasi ancaman siber yang semakin kompleks. Penelitian merekomendasikan perlunya penetapan definisi Infrastruktur Vital Nasional yang lebih komprehensif, penguatan regulasi, serta penerapan strategi perlindungan yang berorientasi pada ketahanan siber untuk menjaga keberlangsungan layanan publik dan kepentingan nasional (Setiyawan, 2019).

Pembahasan

Dampak terhadap Kerahasiaan Informasi pada Objek Vital

Berdasarkan hasil telaah literatur, kerahasiaan informasi menjadi salah satu aspek yang paling rentan dan dominan terdampak oleh insider threat. Sebagian besar studi menunjukkan

bahwa individu yang memiliki akses sah terhadap sistem organisasi berpotensi besar menyalahgunakan kewenangan tersebut untuk memperoleh, menyalin, maupun menyebarluaskan informasi yang bersifat sensitif dan rahasia. Kondisi ini menjadikan insider threat sebagai ancaman yang sangat sulit dideteksi pada tahap awal karena aktivitas pelaku cenderung menyerupai pola aktivitas pengguna normal yang sah di dalam sistem.

Penelitian yang dilakukan oleh Inayat et al. (2024) mengungkapkan bahwa *insider threat* dapat menimbulkan berbagai bentuk serangan, seperti *data breach*, *data loss*, *credential attack*, dan *data exfiltration* yang berpotensi mengganggu kerahasiaan, integritas, serta ketersediaan informasi organisasi. Temuan tersebut menunjukkan bahwa individu yang memiliki akses resmi terhadap sistem berada pada posisi yang memungkinkan untuk menyalahgunakan kewenangannya dalam mengakses, mengambil, maupun menyebarluaskan informasi penting organisasi. Keberadaan akses yang sah ini menjadikan aktivitas pelaku cenderung sulit dikenali karena sering kali tidak berbeda secara signifikan dengan aktivitas pengguna normal di dalam sistem.

Pencurian informasi serta pencurian kekayaan intelektual merupakan bentuk *insider threat* yang paling sering ditemukan dalam berbagai organisasi yang mengidentifikasi penyalahgunaan hak akses dan pencurian data sebagai risiko utama yang ditimbulkan oleh ancaman dari orang dalam (Moore et al., 2008). Tingginya risiko tersebut tidak terlepas dari posisi pelaku yang telah memahami struktur organisasi, alur kerja, serta lokasi penyimpanan aset informasi yang bernilai strategis. Pengetahuan dan akses yang dimiliki memungkinkan pelaku melakukan tindakan yang merugikan organisasi dengan tingkat kerahasiaan yang tinggi, sehingga aktivitasnya sering kali tidak terdeteksi pada tahap awal.

Dalam konteks objek vital, kebocoran informasi memiliki konsekuensi yang lebih serius dibandingkan organisasi pada umumnya. Objek vital umumnya menyimpan informasi yang berkaitan dengan operasional layanan, prosedur pengamanan, konfigurasi sistem, hingga data strategis yang mendukung fungsi organisasi. Apabila informasi tersebut berhasil diakses oleh pihak yang tidak berwenang, maka informasi tersebut dapat dimanfaatkan untuk merencanakan tindakan kriminal lanjutan seperti sabotase, pencurian aset, maupun serangan terhadap sistem yang mendukung operasional objek vital. Dengan demikian, kebocoran informasi tidak hanya menjadi masalah keamanan data, tetapi juga dapat meningkatkan kerentanan objek vital terhadap berbagai bentuk ancaman keamanan lainnya.

Salah satu contoh nyata dampak *insider threat* terhadap kerahasiaan informasi terjadi pada kasus Edward Snowden pada tahun 2013. Snowden yang bekerja sebagai kontraktor di National Security Agency (NSA) Amerika Serikat membocorkan ribuan dokumen rahasia yang berisi informasi mengenai program pengawasan dan intelijen pemerintah Amerika Serikat (Mark Hosenball, 2013). Kasus tersebut menunjukkan bahwa individu yang memiliki akses sah terhadap sistem dapat menjadi ancaman yang sangat besar bagi organisasi. Kebocoran informasi yang dilakukan Snowden tidak hanya berdampak pada keamanan informasi NSA, tetapi juga menimbulkan konsekuensi terhadap hubungan diplomatik, kepercayaan publik, serta keamanan nasional Amerika Serikat. Kasus tersebut menunjukkan bahwa penyalahgunaan akses oleh individu internal dapat menimbulkan dampak yang sangat besar, terutama pada organisasi yang mengelola informasi strategis dan memiliki fungsi vital bagi negara.

Berdasarkan berbagai temuan tersebut, dapat dipahami bahwa kerahasiaan informasi merupakan salah satu aspek yang paling rentan terdampak oleh *insider threat*. Dalam konteks objek vital, kebocoran informasi tidak hanya merugikan organisasi secara internal, tetapi juga berpotensi membuka peluang terjadinya ancaman lanjutan yang dapat mengganggu keamanan, operasional,

dan keberlangsungan fungsi objek vital. Oleh karena itu, penguatan perlindungan informasi strategis melalui pengelolaan hak akses, pemantauan aktivitas pengguna, dan peningkatan kesadaran keamanan menjadi bagian penting dalam sistem pengamanan objek vital.

Dampak terhadap Operasional Objek Vital

Berdasarkan hasil kajian literatur, *insider threat* tidak hanya menimbulkan risiko terhadap keamanan informasi, tetapi juga dapat mengganggu keberlangsungan operasional objek vital. Tingkat ancaman ini menjadi lebih tinggi karena pelaku umumnya memiliki akses yang sah terhadap sistem dan infrastruktur yang mendukung aktivitas organisasi. Kondisi tersebut memungkinkan tindakan yang dilakukan oleh pelaku secara langsung mempengaruhi proses operasional serta kualitas layanan yang diselenggarakan oleh objek vital.

Insider threat pada *Cyber Physical Systems* (CPS) berpotensi menimbulkan gangguan terhadap operasional berbagai sektor strategis, seperti energi, transportasi, kesehatan, dan industri (Al-Mhiqani et al., 2024). Sektor-sektor tersebut termasuk ke dalam kategori infrastruktur kritis yang memiliki peran penting dalam menunjang aktivitas masyarakat dan keberlangsungan pelayanan publik. Oleh karena itu, gangguan yang terjadi tidak hanya berdampak pada sistem teknologi yang digunakan, tetapi juga dapat menghambat proses layanan, menurunkan efektivitas operasional, serta memengaruhi aktivitas masyarakat yang bergantung pada sektor-sektor tersebut.

Sabotase merupakan salah satu bentuk serangan yang paling sering dikaitkan dengan *insider threat*. Bentuk serangan ini dapat diwujudkan melalui penghapusan data, manipulasi sistem, perubahan pengaturan keamanan, maupun penghentian layanan yang dilakukan secara sengaja. Temuan tersebut diperkuat oleh (Moore et al., 2008) yang menunjukkan bahwa pelaku *insider IT sabotage* pada berbagai infrastruktur kritis di Amerika Serikat memanfaatkan akses resminya untuk merusak sistem teknologi informasi organisasi. Kondisi ini mengindikasikan bahwa akses yang dimiliki oleh orang dalam dapat menjadi sarana untuk melakukan tindakan yang mengganggu stabilitas operasional dan fungsi layanan pada objek vital.

Dalam konteks objek vital, gangguan operasional yang disebabkan oleh *insider threat* dapat menimbulkan konsekuensi yang lebih signifikan dibandingkan pada organisasi non strategis. Gangguan pada sektor energi berpotensi menghambat distribusi listrik, sementara gangguan pada sektor transportasi dapat mempengaruhi mobilitas masyarakat dan distribusi barang. Di sisi lain, gangguan pada sektor kesehatan dapat menurunkan efektivitas serta kualitas pelayanan medis yang diberikan kepada masyarakat. Oleh karena itu, dampak *insider threat* tidak hanya terbatas pada aspek keamanan informasi, tetapi juga dapat mengganggu fungsi utama objek vital dalam menyediakan layanan yang mendukung kepentingan publik.

Temuan tersebut menunjukkan bahwa ancaman terhadap operasional objek vital tidak dapat dipandang sebagai persoalan teknis semata, melainkan sebagai risiko strategis yang berpotensi mempengaruhi keberlangsungan fungsi organisasi. Seiring meningkatnya ketergantungan objek vital terhadap sistem digital, penyalahgunaan akses oleh pihak internal dapat menimbulkan dampak yang semakin luas terhadap pelayanan dan operasional organisasi. Dengan demikian, penguatan mekanisme pengawasan, penerapan prinsip *least privilege*, serta pembangunan budaya keamanan yang kuat menjadi langkah penting dalam menjaga kontinuitas layanan dan ketahanan objek vital terhadap ancaman *insider threat*.

Dampak terhadap Risiko dan Kerugian Objek Vital

Berdasarkan hasil telaah literatur, *insider threat* tidak hanya menimbulkan gangguan terhadap keamanan informasi dan operasional organisasi, tetapi juga meningkatkan risiko serta kerugian yang harus ditanggung oleh objek vital. Kerugian tersebut dapat berupa kerugian

finansial, biaya pemulihan sistem, hilangnya aset informasi strategis, hingga menurunnya tingkat kepercayaan publik terhadap organisasi. Oleh karena itu, insider threat merupakan ancaman yang dapat mempengaruhi keberlangsungan organisasi dalam jangka pendek maupun jangka panjang.

Serangan yang dilakukan oleh orang dalam dapat menyebabkan kerugian finansial akibat terganggunya operasional organisasi, biaya pemulihan sistem, serta kebutuhan untuk meningkatkan sistem keamanan setelah terjadinya insiden (Al-Mhiqani et al., 2024)Kerugian tersebut menjadi semakin besar apabila ancaman terjadi pada objek vital yang memiliki ketergantungan tinggi terhadap teknologi informasi dalam menjalankan fungsi operasionalnya. Ketika sistem yang mendukung operasional terganggu, organisasi harus mengalokasikan sumber daya tambahan untuk melakukan pemulihan serta memastikan layanan dapat kembali berjalan secara normal.

Selain itu, penelitian pada berbagai infrastruktur kritis di Amerika Serikat menunjukkan bahwa pencurian informasi, sabotase sistem, dan pencurian kekayaan intelektual dapat memberikan dampak ekonomi yang signifikan bagi organisasi (Moore et al., 2008) Selain kehilangan aset informasi yang bernilai strategis, organisasi juga harus menanggung biaya investigasi, pemulihan sistem, serta penguatan keamanan untuk mencegah kejadian serupa di masa mendatang. Hal ini menunjukkan bahwa dampak insider threat tidak berhenti pada saat insiden terjadi, tetapi dapat terus dirasakan dalam jangka waktu yang panjang.

Selain kerugian finansial, Saxena et al. (2020) menjelaskan bahwa *insider threat* juga berpotensi menurunkan reputasi organisasi. Kebocoran data dan kegagalan dalam menjaga keamanan informasi dapat mengurangi tingkat kepercayaan masyarakat terhadap organisasi yang mengelola objek vital. Padahal, kepercayaan publik merupakan salah satu faktor penting dalam penyelenggaraan layanan yang berkaitan dengan kepentingan masyarakat. Ketika terjadi insiden keamanan yang melibatkan orang dalam, masyarakat dapat mempertanyakan kemampuan organisasi dalam melindungi aset dan informasi yang dimilikinya.

Temuan dari berbagai penelitian tersebut menunjukkan bahwa kerugian akibat *insider threat* bersifat multidimensional karena tidak hanya mempengaruhi kondisi keuangan organisasi, tetapi juga berdampak pada reputasi, kepercayaan publik, dan efektivitas penyelenggaraan layanan. Dalam konteks objek vital nasional, kerugian yang ditimbulkan tidak hanya dirasakan oleh organisasi pengelola, tetapi juga dapat berdampak pada masyarakat yang bergantung pada layanan tersebut. Gangguan pada objek vital dapat menghambat pelayanan publik, meningkatkan biaya operasional negara, serta mengurangi efektivitas penyelenggaraan fungsi strategis organisasi. Oleh karena itu, *insider threat* perlu dipandang sebagai risiko strategis yang memerlukan pendekatan pengelolaan risiko secara menyeluruh dengan memperhatikan aspek manusia, teknologi, dan tata kelola organisasi.

Dampak terhadap Keamanan Infrastruktur Kritis dan Keamanan Nasional

Hasil telaah literatur menunjukkan bahwa dampak *insider threat* pada objek vital tidak hanya dirasakan oleh organisasi secara internal, tetapi juga dapat memengaruhi keamanan infrastruktur kritis dan kepentingan nasional. Hal ini disebabkan karena objek vital memiliki keterkaitan langsung dengan penyediaan layanan publik, stabilitas ekonomi, dan keberlangsungan fungsi negara. Oleh sebab itu, setiap gangguan yang terjadi pada objek vital berpotensi menimbulkan konsekuensi yang lebih luas dibandingkan gangguan pada organisasi biasa.

Al-Mhiqani et al. (2024) menjelaskan bahwa sektor energi, transportasi, kesehatan, dan industri merupakan bagian dari infrastruktur kritis yang mendukung berbagai aktivitas masyarakat dan perekonomian negara. Gangguan yang terjadi pada sektor-sektor tersebut berpotensi

menyebabkan terhambatnya aktivitas publik, terganggunya distribusi layanan, hingga menurunnya produktivitas ekonomi. Kondisi tersebut menunjukkan bahwa ancaman *insider threat* tidak hanya berdampak pada organisasi yang menjadi target, tetapi juga dapat mempengaruhi stabilitas sistem yang lebih luas.

Temuan tersebut diperkuat oleh Moore et al., (2008) yang menunjukkan bahwa sabotase yang dilakukan oleh orang dalam dapat menyebabkan kerusakan serius terhadap sistem teknologi informasi yang mendukung operasional infrastruktur kritis. Ancaman tersebut menjadi semakin berbahaya karena pelaku umumnya memahami sistem yang digunakan, mengetahui kelemahan organisasi, serta memiliki akses yang memungkinkan mereka melakukan tindakan tanpa menimbulkan kecurigaan pada tahap awal. Karakteristik inilah yang menjadikan *insider threat* sebagai salah satu ancaman dengan tingkat risiko tinggi terhadap keberlangsungan layanan publik dan fungsi strategis negara.

Kasus Edward Snowden pada tahun 2013 menunjukkan bahwa ancaman dari orang dalam dapat berkembang menjadi persoalan keamanan nasional. Kebocoran dokumen rahasia yang dilakukan Snowden tidak hanya mempengaruhi keamanan informasi National Security Agency (NSA), tetapi juga menimbulkan konsekuensi politik, diplomatik, dan keamanan pada tingkat internasional. Kasus tersebut memperlihatkan bahwa penyalahgunaan akses oleh individu internal dapat menghasilkan dampak yang jauh melampaui organisasi tempat pelaku bekerja. Ketika ancaman serupa terjadi pada institusi yang memiliki fungsi strategis, dampaknya dapat mempengaruhi kepentingan nasional secara keseluruhan.

Dalam konteks Indonesia, ancaman *insider threat* perlu mendapatkan perhatian khusus mengingat banyaknya objek vital nasional yang telah bergantung pada sistem digital dalam menjalankan operasionalnya. Sektor energi, transportasi, telekomunikasi, perbankan, hingga lembaga penegak hukum merupakan contoh objek vital yang menyimpan informasi strategis dan mendukung pelayanan publik. Penyalahgunaan akses oleh individu internal pada sektor-sektor tersebut berpotensi mengganggu stabilitas layanan, menimbulkan kerugian ekonomi, serta mempengaruhi keamanan nasional apabila tidak dikelola dengan baik.

Gangguan pada satu objek vital juga berpotensi menimbulkan *cascading effect* atau efek berantai terhadap sektor lain yang saling terhubung. Sebagai contoh, gangguan pada sektor energi dapat memengaruhi sektor transportasi, komunikasi, dan industri yang bergantung pada pasokan listrik. Oleh karena itu, *insider threat* perlu dipandang sebagai ancaman strategis yang tidak hanya mengancam organisasi secara internal, tetapi juga berpotensi mengganggu stabilitas layanan publik, aktivitas ekonomi, serta keamanan nasional secara keseluruhan. Pandangan ini didukung oleh (Setiyawan, 2019) yang menyatakan bahwa kegagalan melindungi infrastruktur kritis nasional dapat berdampak pada terganggunya fungsi-fungsi strategis negara dan kepentingan nasional.

Secara keseluruhan, hasil telaah literatur menunjukkan bahwa *insider threat* memiliki dampak multidimensional terhadap objek vital. Dampak tersebut tidak hanya berupa kebocoran informasi, tetapi juga meliputi gangguan operasional, peningkatan risiko dan kerugian organisasi, serta ancaman terhadap keamanan infrastruktur kritis dan keamanan nasional. Temuan ini menunjukkan bahwa ancaman dari orang dalam harus dipandang sebagai risiko strategis yang memerlukan pendekatan pengamanan yang mengintegrasikan aspek manusia, teknologi, dan organisasi. Dengan demikian, penguatan sistem keamanan internal menjadi langkah penting untuk menjaga keberlangsungan fungsi objek vital dan melindungi kepentingan masyarakat maupun negara.

KESIMPULAN

Literature review ini mengkaji sepuluh artikel ilmiah yang membahas *insider threat* pada organisasi, infrastruktur kritis, dan objek vital. Berdasarkan hasil telaah terhadap artikel-artikel tersebut, diperoleh temuan bahwa insider threat memberikan empat dampak utama terhadap objek vital, yaitu kebocoran informasi strategis, gangguan terhadap operasional objek vital, peningkatan risiko dan kerugian organisasi, serta ancaman terhadap keamanan infrastruktur kritis dan keamanan nasional. Dampak tersebut muncul karena pelaku memiliki hak akses yang sah, memahami prosedur operasional organisasi, serta mengetahui kelemahan sistem sehingga tindakan yang dilakukan cenderung lebih sulit dideteksi dibandingkan ancaman dari pihak eksternal.

Hasil kajian juga menunjukkan bahwa ancaman dari orang dalam tidak hanya berdampak pada organisasi pengelola objek vital, tetapi dapat memengaruhi keberlangsungan pelayanan publik, stabilitas ekonomi, hingga keamanan nasional. Oleh karena itu, pengamanan objek vital perlu dilakukan secara menyeluruh dengan mengintegrasikan aspek manusia, teknologi, dan tata kelola organisasi melalui penguatan pengendalian hak akses, pemantauan aktivitas pengguna, serta peningkatan budaya dan kesadaran keamanan. *Literature review* ini diharapkan dapat menjadi referensi bagi pengelola objek vital, aparat penegak hukum, maupun peneliti dalam memahami dampak *insider threat* sehingga dapat mendukung penyusunan strategi pengamanan yang lebih efektif. Selain itu, penelitian selanjutnya diharapkan dapat mengembangkan kajian ini melalui penelitian empiris atau studi kasus pada objek vital di Indonesia agar diperoleh gambaran yang lebih komprehensif mengenai karakteristik dan penanganan *insider threat*.

DAFTAR PUSTAKA

Al Hammadi, A. Y., Lee, D., Yeun, C. Y., Damiani, E., Kim, S. K., Yoo, P. D., & Choi, H. J. (2020). Novel EEG Sensor-Based Risk Framework for the Detection of Insider Threats in Safety Critical Industrial Infrastructure. *IEEE Access*, *8*, 206222–206234. https://doi.org/10.1109/ACCESS.2020.3037979

Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W., Hassan, A., Abdulkareem, K. H., Ali, N. S., & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. In *Applied Sciences (Switzerland)* (Vol. 10, Number 15). MDPI AG. https://doi.org/10.3390/app10155208

Al-Mhiqani, M. N., Alsboui, T., Al-Shehari, T., Abdulkareem, K. hameed, Ahmad, R., & Mohammed, M. A. (2024). Insider threat detection in cyber-physical systems: a systematic literature review. *Computers and Electrical Engineering*, *119*. https://doi.org/10.1016/j.compeleceng.2024.109489

Budžys, A., Kurasova, O., & Medvedev, V. (2024). Deep learning-based authentication for insider threat detection in critical infrastructure. *Artificial Intelligence Review*, *57*(10). https://doi.org/10.1007/s10462-024-10893-1

Cybersecurity and Infrastructure Security Agency. (2024). *Critical Infrastructure Security And Resilience*.

Gelman, H., Hastings, J. D., Kenley, D., & Loiacono, E. (2024). *Toward an Insider Threat Education Platform: A Theoretical Literature Review*. https://doi.org/10.1109/ICCA62237.2024.10928083

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1). https://doi.org/10.1186/s41044-016-0006-0

IBM. (2024). *Cost Of a Data Breach Report 2024*.

Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal*, *15*(12). https://doi.org/10.1016/j.asej.2024.103068

Kepolisian Negara Republik Indonesia. (2019). *Peraturan Kepolisian Negara Republik Indonesia Nomor 7 Tahun 2019 tentang Perubahan Kedua atas Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 13 Tahun 2017 tentang Pemberian Bantuan Pengamanan pada Objek VItal Nasional dan Objek Tertentu*.

Mark Hosenball. (2013). NSA chief says Snowden leaked up to 200,000 secret documents. *Reuters*.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*. http://www.sei.cmu.edu

Rahman, R., Lestari, D., & Lestari, C. I. (2026). *Analisis Keamanan Sistem Informasi Terhadap Serangan Insider Threat* (Vol. 01, Number 03). Online.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. In *Electronics (Switzerland)* (Vol. 9, Number 9, pp. 1–29). MDPI AG. https://doi.org/10.3390/electronics9091460

Singh, A. P., & Sharma, A. (2022). *A systematic literature review on insider threats*. http://arxiv.org/abs/2212.05347

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039