Inovan Publisher

Orbit: Jurnal Ilmu Multidisplin Nusantara

| ISSN (Online) 3064-5883 |
https://creativecommons.org/licenses/by/4.0/
DOI: 10.63217/orbit.v2i3.212

Keamanan Komunikasi di Lingkungan Hybrid dan Remote

Mohammad Fayruz[1], Zalfa Fhaerunnisa Ahmad[2], Syafiqoh Syaqurani[3], Silvania Aldian Cahyani[4], Putri Aulia Febriyanti[5]
[1]STIE Ganesha, Tangerang Selatan, Indonesia, Mfayruz@gmail.com
[2]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, fhaerunissa@gmail.com
[3]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, syafiqoh.syaqurani04@gmail.com
[4] Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, silvaniaaldian76@gmail.com
[5] Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, putriauliafebriyanti4@gmail.com

Corresponding Author: fhaerunissa@gmail.com[2]

Abstract: *The implementation of hybrid and remote work models has become increasingly prevalent alongside accelerated digital transformation, while simultaneously presenting significant challenges to organizational communication security. The disappearance of physical network boundaries, the growing use of personal devices, and reliance on digital communication platforms require more adaptive and integrated security management approaches. This study aims to analyze communication security risks in hybrid and remote work environments, particularly those related to the use of personal devices, network connectivity, and communication activity monitoring mechanisms. The method employed is a literature review examining relevant scholarly sources on security management, personal device policies, secure network architectures, and digital communication monitoring practices. The findings indicate that the use of personal devices increases the risk of data leakage if not supported by adequate policies and controls, while the implementation of secure network technologies strengthens data protection in remote communications. Furthermore, communication monitoring and activity logging play a crucial role in supporting accountability and early threat detection, provided they are applied transparently and balanced with privacy protection. This study concludes that communication security in hybrid and remote work environments requires the integration of organizational policies, security technologies, and ethical awareness of human resources to establish a sustainable and trustworthy security system.*

Keywords: *Communication Security, Hybrid Work, Remote Work, Security Management, Information Security Risk.*

Abstrak: Penerapan model kerja hybrid dan remote telah menjadi praktik yang semakin umum seiring dengan percepatan transformasi digital, namun kondisi ini turut menghadirkan tantangan serius terhadap keamanan komunikasi organisasi. Hilangnya batas fisik jaringan, meningkatnya penggunaan perangkat pribadi, serta ketergantungan pada platform komunikasi digital menuntut pendekatan manajemen sekuriti yang lebih adaptif dan terintegrasi. Penelitian ini bertujuan untuk menganalisis risiko keamanan komunikasi dalam lingkungan kerja hybrid

dan remote, khususnya yang berkaitan dengan penggunaan perangkat pribadi, konektivitas jaringan, serta mekanisme pengawasan aktivitas komunikasi. Metode yang digunakan adalah studi literatur dengan menelaah berbagai sumber ilmiah yang relevan mengenai manajemen keamanan, kebijakan perangkat pribadi, arsitektur jaringan aman, serta praktik monitoring komunikasi digital. Hasil pembahasan menunjukkan bahwa penggunaan perangkat pribadi meningkatkan potensi kebocoran data apabila tidak disertai kebijakan dan pengendalian yang memadai, sementara penerapan teknologi jaringan aman mampu memperkuat perlindungan data dalam komunikasi jarak jauh. Selain itu, monitoring dan pencatatan aktivitas komunikasi berperan penting dalam mendukung akuntabilitas dan deteksi dini ancaman keamanan, asalkan diterapkan secara transparan dan berimbang dengan perlindungan privasi. Simpulan penelitian ini menegaskan bahwa keamanan komunikasi di lingkungan kerja hybrid dan remote memerlukan integrasi antara kebijakan organisasi, teknologi keamanan, dan kesadaran etis sumber daya manusia untuk menciptakan sistem keamanan yang berkelanjutan dan terpercaya.

Kata Kunci: Keamanan Komunikasi, Kerja Hybrid, Kerja Jarak Jauh, Manajemen Sekuriti, Risiko Keamanan Informasi.

PENDAHULUAN

Transformasi digital yang dipercepat oleh pandemi global telah mendorong perubahan signifikan dalam pola kerja organisasi, di mana model kerja hybrid dan remote kini menjadi praktik yang semakin umum dan berkelanjutan. Perubahan ini membawa implikasi besar terhadap pola komunikasi organisasi yang bergantung pada teknologi digital dan Computer Mediated Communication (CMC), sehingga batas fisik dan teknis jaringan organisasi menjadi semakin kabur. Ketergantungan pada perangkat pribadi atau Bring Your Own Device (BYOD) dalam mendukung fleksibilitas dan produktivitas kerja di satu sisi memberikan efisiensi, namun di sisi lain memperluas permukaan risiko keamanan informasi, termasuk potensi kebocoran data, akses tidak sah, serta meningkatnya ancaman siber.

Berdasarkan teori manajemen sekuriti informasi, perlindungan aset informasi tidak hanya menekankan pada pengamanan teknis, tetapi juga pada pengelolaan risiko, kebijakan organisasi, serta perilaku pengguna sebagai faktor krusial dalam sistem keamanan. Selain itu, pendekatan Zero Trust menegaskan bahwa tidak ada pengguna maupun perangkat yang dapat dipercaya secara default, sehingga setiap akses harus diverifikasi secara berkelanjutan. Dalam konteks ini, teknologi seperti Virtual Private Network (VPN), Secure Access Service Edge (SASE), serta sistem monitoring dan logging menjadi instrumen penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Namun, efektivitas teknologi tersebut sangat bergantung pada integrasi dengan teori etika profesi dan akuntabilitas, yang menekankan tanggung jawab individu dalam menjaga keamanan data organisasi.

Oleh karena itu, penelitian ini berfokus pada analisis keamanan komunikasi di lingkungan kerja hybrid dan remote dengan menelaah keterkaitan antara risiko komunikasi digital, penerapan teknologi keamanan, serta peran etika dan tata kelola manajemen sekuriti sebagai upaya membangun sistem keamanan informasi yang holistik dan berkelanjutan.

METODE

Menurut Sugiyono (2019), metode penulisan adalah cara ilmiah untuk mendapatkan data dengan tujuan dan manfaat tertentu untuk menjawab rumusan masalah penelitian, sehingga data dapat dianalisis secara sistematis dan objektif untuk menghasilkan kesimpulan yang valid. Metode penulisan juga diartikan sebagai teknik yang dipakai dalam menyusun makalah agar penyampaian informasi menjadi jelas dan sistematis. Metode ini bisa berupa metode kualitatif, kuantitatif, campuran, deskriptif, atau eksperimental, tergantung pada tujuan dan jenis data yang dikumpulkan. Metode ini berfungsi agar penulisan dapat dilakukan secara

logis, sistematis, dan mudah dipahami oleh pembaca. Dalam konteks karya ilmiah, metode penulisan meliputi langkah-langkah seperti perumusan masalah, pengumpulan data, analisis, dan penyajian hasil yang didukung oleh teori dan fakta.

Penulis menggunakan metode studi pustaka (library research) sebagai pendekatan utama. Metode ini dilakukan dengan cara mengumpulkan, menelaah, dan menganalisis berbagai sumber literatur yang relevan, seperti buku, jurnal ilmiah, artikel, dan laporan penelitian yang membahas terkait keamanan komunikasi, kerja hybrid dan remote, serta manajemen sekuriti informasi. Selain itu, penulis juga memanfaatkan data sekunder yang diperoleh dari lembaga riset untuk memperkuat analisis. Dengan menggunakan metode ini, diharapkan penulisan dapat menghasilkan kajian yang komprehensif, sistematis, dan objektif sesuai dengan tujuan penelitian.

HASIL DAN PEMBAHASAN

Risiko Komunikasi di perangkat pribadi (BYOD)

Penerapan skema kerja hybrid dan remote working secara inheren telah mendorong penggunaan perangkat pribadi karyawan, atau dikenal sebagai kebijakan Bring Your Own Device (BYOD), yang meskipun memberikan fleksibilitas tinggi dan meningkatkan produktivitas individu, namun menciptakan risiko keamanan komunikasi yang signifikan dan kompleks bagi organisasi, menantang prinsip-prinsip manajemen sekuriti tradisional yang bergantung pada perimeter jaringan yang terdefinisi. Dalam konteks kerja jarak jauh, di mana karyawan menggunakan berbagai aplikasi kolaboratif seperti Google Docs, Sheets, Slides, Notion, atau Telegram untuk komunikasi sehari-hari dan berbagi dokumen, seperti yang dicontohkan dalam penelitian tentang model komunikasi remote working, perangkat pribadi menjadi end-point utama yang membawa data perusahaan melampaui batas keamanan fisik kantor, padahal perangkat tersebut mungkin tidak memenuhi standar keamanan korporat, rentan terhadap malware dari penggunaan personal, atau tidak memiliki patch sistem operasi yang terbaru, sehingga secara langsung bertentangan dengan tujuan utama manajemen keamanan untuk melindungi aset informasi dari akses dan perubahan yang tidak sah. Ketergantungan pada perangkat non-standar ini secara drastis memperluas permukaan serangan, membuat organisasi rentan terhadap insiden kebocoran data yang dapat berasal dari kesalahan atau kelalaian pengguna pribadi, di mana nilai-nilai etika seperti tanggung jawab dan kesadaran keamanan siber menjadi garis pertahanan terakhir. (Chairiyah Batubara et al., 2017)

Risiko komunikasi dalam skema BYOD secara mendalam berkaitan dengan aspek etika profesi dan akuntabilitas individu, sebuah isu yang sangat relevan dengan temuan dalam kasus kebocoran data Bank Syariah Indonesia (BSI), yang menggarisbawahi bahwa kegagalan etis dapat menjadi pemicu utama kerentanan keamanan, bahkan ketika kontrol teknis telah diterapkan. Dalam lingkungan BYOD, jika seorang karyawan gagal menjunjung tinggi nilai tanggung jawab dan integritas misalnya, dengan menyimpan dokumen sensitif di penyimpanan lokal perangkat pribadi yang tidak terenkripsi, atau menggunakan aplikasi komunikasi yang tidak disetujui untuk membahas hal-hal rahasia maka human error ini dapat memicu kebocoran informasi yang setara dengan serangan siber eksternal, sehingga menuntut adanya integrasi prinsip etika dalam tata kelola TI untuk memperkuat pertahanan internal. Kelemahan ini diperparah oleh fakta bahwa dalam komunikasi remote working, sering terjadi slow response atau miss komunikasi melalui teks, yang mana jika dibarengi dengan praktik BYOD yang ceroboh, dapat menimbulkan ketidakjelasan informasi yang selanjutnya dieksploitasi oleh pihak yang tidak bertanggung jawab, baik secara sengaja maupun tidak disengaja, menjadikan manajemen risiko berbasis etika dan kebijakan perangkat pribadi yang ketat menjadi sangat krusial.

Pentingnya manajemen keamanan yang efektif di era digitalisasi, seperti yang dijelaskan dalam literatur, menekankan perlunya strategi komprehensif untuk mengelola risiko BYOD, yang tidak hanya bersifat teknis, tetapi juga edukatif dan regulatif. Secara teknis, organisasi harus menerapkan solusi Mobile Device Management (MDM) atau Mobile Application Management (MAM) untuk memisahkan data pribadi dan korporat, memastikan enkripsi data, dan

memberlakukan sandi yang kuat pada perangkat pribadi yang digunakan untuk mengakses sumber daya perusahaan. Namun, solusi ini harus didukung oleh kebijakan keamanan yang jelas dan transparan, yang secara eksplisit mengatur penggunaan aplikasi komunikasi yang disetujui, prosedur penanganan data sensitif di perangkat pribadi, dan mekanisme pelaporan insiden, untuk memastikan akuntabilitas setiap individu dalam mematuhi standar keamanan, meminimalisir peluang akses yang tidak sah, serta mencegah konsekuensi finansial dan reputasi buruk akibat pelanggaran keamanan. Kegagalan untuk memperbarui strategi dan teknik keamanan seiring dengan cepatnya perubahan teknologi dan lingkungan bisnis akan membuat risiko BYOD terus meningkat, sehingga investasi dalam teknologi keamanan dan pendidikan kesadaran menjadi sangat mendesak. (D. Anugrah C Mediyastuti Sofyan, 2025)

Lebih jauh, risiko BYOD juga diperparah oleh adanya kesenjangan keterampilan digital di kalangan tenaga kerja, sebagaimana ditunjukkan dalam studi tentang peningkatan keterampilan digital, di mana meskipun program pelatihan dapat meningkatkan kemampuan menggunakan tools produktivitas digital, pemahaman mendalam tentang etika penggunaan teknologi dan keamanan data seringkali masih menjadi tantangan. Dalam konteks BYOD, pemahaman yang lemah tentang literasi digital dapat menyebabkan karyawan secara tidak sengaja mengunduh malware yang menyadap sesi komunikasi digital mereka, atau salah mengkonfigurasi pengaturan privasi yang kemudian membuka akses ke data perusahaan. Oleh karena itu, strategi manajemen sekuriti yang efektif harus mencakup pelatihan kesadaran keamanan yang berkelanjutan dan spesifik untuk lingkungan BYOD, mengajarkan karyawan cara mengidentifikasi phishing, pentingnya menggunakan koneksi Virtual Private Network (VPN) saat bekerja dari jaringan publik, serta mendidik mereka tentang konsekuensi pelanggaran etika profesional terhadap keamanan informasi, agar setiap pengguna perangkat pribadi menjadi garis pertahanan pertama, bukan justru menjadi titik terlemah dalam sistem keamanan organisasi yang terdistribusi. Intinya, mengatasi risiko BYOD dalam komunikasi hybrid adalah tantangan manajemen perubahan yang menuntut pemimpin untuk mengadopsi gaya kepemimpinan yang adaptif dan suportif, sebagaimana yang disarankan oleh literatur kepemimpinan hybrid, yang menekankan pada pembangunan kepercayaan dan penetapan ekspektasi yang jelas, alih-alih mengandalkan pengawasan mikro yang mustahil. Pemimpin harus mampu menyeimbangkan fleksibilitas yang ditawarkan oleh BYOD dengan kebutuhan akan governance keamanan, memastikan bahwa kebijakan keamanan tidak dirasakan sebagai hukuman, tetapi sebagai bagian integral dari tanggung jawab profesional, sambil menyediakan teknologi penunjang seperti solusi MDM yang user-friendly dan pelatihan yang kontekstual. Jika leadership gagal memberikan panduan yang transparan dan adil mengenai BYOD, seperti yang disoroti sebagai masalah equity dalam lingkungan hybrid, hal itu dapat menimbulkan konflik interpersonal dan ketidakpatuhan, yang pada akhirnya akan merusak budaya keamanan kolektif dan meningkatkan kemungkinan terjadinya insiden keamanan data dari perangkat pribadi.

VPN, Secure Access Service Edge (SASE)

Di tengah tantangan mendasar yang ditimbulkan oleh model kerja hybrid dan remote serta adopsi perangkat pribadi (BYOD), di mana tim bekerja secara geografis tersebar dan mengandalkan komunikasi digital, solusi konektivitas dan keamanan jaringan menjadi imperatif untuk melindungi aset informasi yang mengalir di luar perimeter kantor tradisional, dan dalam konteks ini, Virtual Private Network (VPN) dan Secure Access Service Edge (SASE) muncul sebagai dua pilar utama dalam strategi manajemen sekuriti. Ketergantungan pada komunikasi digital melalui media seperti Telegram dan Google Meet, serta kolaborasi pada cloud-based tools seperti Google Workspace dan Notion, yang dilakukan dari berbagai lokasi dengan tingkat keamanan jaringan yang bervariasi, menuntut suatu mekanisme untuk mengenkripsi dan mengamankan transmisi data agar informasi sensitif terlindungi dari penyadapan atau akses tidak sah oleh pihak luar, yang merupakan tujuan inti dari manajemen keamanan yang efektif di era digital. VPN telah lama menjadi standar emas dalam mengatasi tantangan ini, menciptakan terowongan terenkripsi dari perangkat pengguna ke jaringan korporat, yang secara efektif

memperpanjang batas keamanan kantor ke lokasi remote karyawan, memastikan bahwa komunikasi remote working tetap bersifat pribadi dan terproteksi dari ancaman siber yang meningkat.

Meskipun VPN menawarkan solusi yang handal untuk enkripsi data dan identifikasi jaringan, arsitektur tradisionalnya yang mengarahkan semua lalu lintas data kembali ke pusat data kantor (head-hauling) menjadi tidak efisien dan rentan terhadap latensi ketika sebagian besar aplikasi beralih ke cloud, sebuah realitas yang dipercepat oleh transformasi digital dan adopsi hybrid work. Oleh karena itu, muncul evolusi ke arah Secure Access Service Edge (SASE), sebuah kerangka arsitektur yang dikembangkan untuk menjawab kebutuhan model kerja hybrid yang semakin permanen, di mana SASE mengintegrasikan fungsi jaringan wide area networking (WAN) dengan layanan keamanan berbasis cloud (seperti Secure Web Gateway, Cloud Access Security Broker, dan Firewall-as-a-Service) menjadi satu layanan terpadu yang disediakan dari cloud. Arsitektur SASE ini secara fundamental mendukung filosofi kepemimpinan hybrid dan remote dengan menempatkan kontrol keamanan sedekat mungkin dengan pengguna dan data, terlepas dari lokasi fisik mereka, sehingga mampu memberikan kinerja koneksi yang lebih baik untuk aplikasi cloud sambil tetap menegakkan kebijakan keamanan yang konsisten, berbanding terbalik dengan VPN tradisional yang sering membatasi waktu panggilan atau koneksi. (Damanik, 2016; Fachrudin et al., 2024)

Lebih jauh, penerapan SASE sangat relevan dengan konteks manajemen sekuriti yang menuntut akuntabilitas dan governance etis yang kuat, terutama untuk mencegah potensi risiko kebocoran data yang diakibatkan oleh faktor internal, seperti yang disoroti dalam kasus BSI, di mana etika profesi yang lemah turut berkontribusi terhadap insiden keamanan. SASE memfasilitasi model Zero Trust Network Access (ZTNA), yang secara prinsipil tidak mempercayai pengguna atau perangkat mana pun secara default, dan selalu memverifikasi identitas serta konteksnya sebelum memberikan akses ke sumber daya, bahkan jika pengguna sudah terhubung melalui VPN. Mekanisme ini memastikan bahwa akses ke dokumen dan data sensitif yang penting untuk kolaborasi dalam Google Workspace diberikan secara granular berdasarkan peran dan konteks real-time, sehingga secara teknis dapat memperkuat penerapan nilai-nilai etika seperti akuntabilitas dan tanggung jawab individual. Dengan SASE, manajemen dapat secara efektif menegakkan kebijakan keamanan dan mengurangi risiko unauthorized access yang berpotensi terjadi dari perangkat pribadi (BYOD) atau jaringan remote yang tidak aman, memberikan lapisan kontrol yang melampaui kemampuan VPN konvensional.

Dalam perspektif manajemen sekuriti, SASE dan VPN, meskipun berbeda secara arsitektur, sama-sama berperan sebagai enabler kritis bagi peningkatan keterampilan digital dan produktivitas di era global. Sementara VPN memastikan jalur komunikasi yang terenkripsi untuk sesi Google Meet atau pertukaran dokumen melalui Google Drive, SASE memastikan bahwa akses ke berbagai tools produktivitas cloud yang digunakan dalam program pelatihan keterampilan digital, seperti Canva dan Trello, dilakukan dalam kerangka keamanan yang optimal dan berkinerja tinggi. Dengan menyediakan koneksi yang aman, cepat, dan terukur, SASE membantu menghilangkan hambatan teknologi dan infrastruktur yang seringkali menjadi tantangan utama dalam lingkungan kerja hybrid, sehingga memungkinkan tim untuk fokus pada outcome pekerjaan alih-alih terganggu oleh masalah konektivitas atau miss komunikasi akibat latensi. Fleksibilitas keamanan yang ditawarkan oleh SASE menjadikannya strategi fundamental untuk mendukung SDM yang adaptif dan kompeten secara digital, sejalan dengan kebutuhan organisasi untuk mempercepat transformasi digital dan beroperasi secara efisien dalam paradigma kerja baru. (Fenti Cahyani et al., 2025)

Kesimpulannya, dalam konteks manajemen sekuriti untuk lingkungan hybrid dan remote, transisi dari VPN tradisional menuju arsitektur SASE mencerminkan respons strategis terhadap hilangnya batas keamanan yang statis dan tuntutan akan cloud-based governance. SASE adalah investasi strategis yang bukan hanya tentang konektivitas, tetapi juga tentang penguatan governance keamanan informasi secara etis dan teknis, memberikan kapabilitas untuk melakukan manajemen risiko yang tepat dan menegakkan kebijakan keamanan yang jelas dan

terintegrasi di seluruh lingkungan yang terdistribusi. Dengan mengintegrasikan keamanan jaringan dan akses, SASE memungkinkan organisasi untuk mengelola Digital Skills Gap dan risiko BYOD dengan lebih baik, menciptakan fondasi keamanan yang tangguh dan berkelanjutan, yang mendukung work-life balance dan fleksibilitas tanpa mengorbankan perlindungan terhadap aset informasi kritikal dari ancaman keamanan siber yang terus berevolusi.

Monitoring dan Logging Aktivitas Komunikasi

Dalam konteks manajemen sekuriti di lingkungan kerja hybrid dan remote yang terdistribusi, monitoring dan logging aktivitas komunikasi merupakan komponen vital yang menggantikan fungsi pengawasan fisik tradisional, dan menjadi alat utama untuk menegakkan akuntabilitas, mendeteksi anomali, serta mengumpulkan bukti insiden keamanan, sejalan dengan prinsip-prinsip manajemen keamanan yang menekankan pada pelaporan keamanan yang teratur dan identifikasi risiko. Ketika interaksi spontan dan pengamatan langsung berkurang drastis di antara tim yang bekerja jarak jauh melalui Computer Mediated Communication (CMC), mekanisme pencatatan (logging) menjadi mata dan telinga sistem keamanan, melacak setiap aktivitas di platform komunikasi digital seperti chat Telegram, sesi Google Meet, dan kolaborasi dokumen di Notion atau Google Drive. Fungsi ini menjadi sangat penting karena kepemimpinan hybrid berfokus pada hasil (outcome-based leadership), yang secara tidak langsung memerlukan data aktivitas untuk memverifikasi upaya kerja, namun secara sekuriti, logging adalah data historis tak terbantahkan yang dapat mengungkapkan pola perilaku tidak etis atau upaya akses tidak sah, sehingga menjadikannya bagian integral dari kontrol internal dan tata kelola TI. (Meilinda C Sutapa, 2019)

Secara spesifik, monitoring dan logging aktivitas komunikasi memiliki korelasi yang sangat erat dengan mitigasi risiko etika profesi dan pencegahan kebocoran data, yang menjadi pelajaran penting dari insiden BSI, yang menyoroti perlunya mekanisme audit dan pelaporan pelanggaran yang efektif. Tanpa logging yang komprehensif, akan sulit untuk mengidentifikasi dan menghentikan praktik tidak etis sejak dini, karena semua aktivitas komunikasi lisan dan tertulis yang berpotensi melanggar kode etik, seperti upaya phishing internal, transfer data sensitif yang mencurigakan melalui chat, atau bahkan sabotase, akan tersembunyi. Sistem logging yang terperinci tidak hanya mencatat waktu, pengirim, dan penerima pesan, tetapi juga melacak perubahan dokumen, upaya akses ke sistem sensitif (terutama dari perangkat BYOD), dan bahkan log kehadiran dalam rapat virtual, yang semuanya berfungsi sebagai bukti audit yang diperlukan untuk menegakkan akuntabilitas individu dan menyelidiki insiden kebocoran data. (Mutakin C Hubeis, 2011)

Implementasi teknis monitoring dan logging harus mencakup semua tools komunikasi yang digunakan dalam lingkungan remote working untuk memastikan visibilitas keamanan yang menyeluruh, terutama karena karyawan cenderung menggunakan berbagai platform untuk kolaborasi cepat. Sebagai contoh, di remote environment seperti PT. Riliv Psikologi Indonesia, di mana komunikasi didominasi oleh Telegram, Google Meet, dan Notion, logging harus mencakup pencatatan metadata pesan di Telegram, perekaman dan transkripsi weekly/monthly meeting di Google Meet (tentu dengan persetujuan dan pemberitahuan), serta pelacakan riwayat versi dan access log pada dokumen-dokumen yang dikelola di Notion atau Google Drive. Data log yang terkumpul ini kemudian dianalisis oleh sistem Security Information and Event Management (SIEM) untuk mengidentifikasi pola anomali, seperti lonjakan aktivitas pengunduhan data oleh satu pengguna atau akses ke sistem di luar jam kerja yang tidak biasa, yang secara efektif berfungsi sebagai deteksi dini terhadap ancaman internal dan eksternal.

Namun demikian, monitoring dan logging aktivitas komunikasi harus dilakukan dengan keseimbangan yang cermat antara kebutuhan keamanan organisasi dan hak privasi karyawan, serta prinsip equity dalam kepemimpinan hybrid. Manajemen sekuriti harus memastikan bahwa kebijakan logging bersifat transparan, jelas, dan adil, sebagaimana yang dituntut dalam manajemen risiko. Jika implementasi logging dirasakan sebagai pengawasan mikro yang berlebihan, hal ini dapat menimbulkan perasaan isolasi, kurangnya kepercayaan, dan hilangnya

sense of belonging di antara karyawan remote, yang justru merusak budaya organisasi dan keterlibatan tim, yang merupakan tantangan utama dalam kepemimpinan hybrid. Oleh karena itu, kebijakan harus berfokus pada logging yang terkait dengan aset dan keamanan perusahaan, bukan pada aktivitas pribadi, dan log tersebut hanya boleh diakses oleh pihak yang berwenang untuk tujuan audit keamanan dan investigasi insiden, bukan untuk pengawasan kinerja sehari hari yang dapat dicapai melalui outcome-based leadership. (Salim C Halim, 2025)

Pada akhirnya, peran monitoring dan logging dalam manajemen sekuriti adalah untuk memperkuat tata kelola keamanan informasi di era hybrid dengan menjembatani kesenjangan antara teori etika profesional dan praktik nyata organisasi. Dengan memiliki log yang robust dan dapat diaudit, organisasi dapat menunjukkan kepatuhan terhadap regulasi perlindungan data pribadi dan standar keamanan, yang pada gilirannya meningkatkan kepercayaan nasabah dan pemangku kepentingan. Logging juga menjadi dasar bagi post-mortem analysis setelah terjadinya insiden (seperti kasus kebocoran data), memungkinkan organisasi untuk belajar dari kesalahan, memperkuat sistem pertahanan, dan memberikan masukan kebijakan yang konkret bagi regulator, sehingga memastikan sistem keamanan informasi tidak hanya kuat secara teknis, tetapi juga didukung oleh budaya kepatuhan kolektif dan akuntabilitas berbasis bukti.

Integrasi AI dalam Sistem Monitoring Keamanan

Kemajuan teknologi kecerdasan buatan (AI) dan machine learning membuka peluang baru untuk meningkatkan monitoring keamanan komunikasi. AI mampu mendeteksi pola anomali perilaku komunikasi pengguna secara real-time, seperti pola pengunduhan file yang tidak biasa, percobaan akses pada jam tidak wajar, atau perubahan gaya penulisan yang mengindikasikan potensi kompromi akun (behavioral analytics). Professor et al. (2024) menjelaskan bahwa integrasi AI ke dalam kerangka SASE dapat meningkatkan kemampuan deteksi ancaman dan mengurangi beban kerja analis keamanan. Dalam konteks kerja hybrid, AI menjadi penting karena volume aktivitas digital yang sangat tinggi tidak mungkin dianalisis secara manual. Dengan kemampuannya melakukan automated threat detection, organisasi dapat mencegah insiden lebih cepat sebelum berdampak besar. Namun, penggunaan AI harus tetap sejalan dengan etika privasi, transparansi, serta batasan akses data yang jelas.

KESIMPULAN

Kesimpulan penelitian ini menegaskan bahwa keamanan komunikasi di lingkungan kerja hybrid dan remote merupakan aspek krusial yang harus dikelola secara strategis seiring meningkatnya penggunaan teknologi digital dan perangkat pribadi dalam aktivitas organisasi. Hasil pembahasan menunjukkan bahwa risiko keamanan komunikasi, seperti kebocoran data dan akses tidak sah, menuntut penerapan manajemen sekuriti yang terintegrasi melalui kebijakan BYOD yang jelas, pemanfaatan teknologi keamanan jaringan seperti VPN dan Secure Access Service Edge (SASE), serta penerapan monitoring dan logging aktivitas komunikasi secara transparan dan akuntabel.

Perbaikan yang perlu dilakukan adalah penguatan tata kelola keamanan informasi yang tidak hanya berfokus pada aspek teknis, tetapi juga pada peningkatan kesadaran etika profesi dan tanggung jawab individu dalam menjaga keamanan data. Dengan pendekatan tersebut, organisasi diharapkan mampu membangun sistem keamanan komunikasi yang lebih adaptif, berkelanjutan, dan selaras dengan kebutuhan kerja hybrid dan remote tanpa mengurangi fleksibilitas kerja.

REFERENSI

Afif, M. R. (n.d.-a). Analisis Pengelolaan Hybrid Working Team pada Lembaga Ketahanan Nasional Republik Indonesia. In *Edu Society: Jurnal Pendidikan, Ilmu Sosial, dan Pengabdian Kepada Masyarakat* (Vol. 5).

Afif, M. R. (n.d.-b). Analisis Pengelolaan Hybrid Working Team pada Lembaga Ketahanan Nasional Republik Indonesia. In *Edu Society: Jurnal Pendidikan, Ilmu Sosial, dan Pengabdian Kepada Masyarakat* (Vol. 5).

Afifi Al-Atsari, H., C Suharjo, I. (2023). Integrasi Server On-Premise dengan Server Cloud Menggunakan Cloud VPN dan Mikrotik Ipsec Untuk Peningkatan Keamanan Koneksi. *Jurnal Syntax Admiration*, *4*(11), 1977–1996. https://doi.org/10.46799/jsa.v4i11.757

Agroindustri, P. T., Teknologi, J., Pertanian, I., Teknologi, F., Ipb, P., Teknologi, M., Pertanian, T., Machfud, I., C Sukardi, J. (2010). Identifikasi dan Evaluasi Risiko Manajemen Rantai Pasok Komoditas Jagung dengan Pendekatan Logika Fuzzy Suharjito Bambang Haryanto. In *Jurnal Manajemen dan Organisasi* (Issue 2).

Alfath, I., Fathony, N., Mareta, A., Adiana, B. E., Wardhani, O., Halim, A., Studi, P., C Informasi, T. (2025). *ELKOM (Jurnal Elektronika dan Komputer) Optimisasi Whisper Speech-to-Text Bahasa Indonesia dengan Hybrid Cloud dan Multi-Engine*. *18*(1). https://journal.stekom.ac.id/index.php/elkom

And, I., C Expert, D. (2023). *Pengembangan Real-Time Monitoring dan Data Logging Berbasis Web Pada Proses Robot Painting untuk Meningkatkan Efisiensi Produksi INFORMASI ARTIKEL A B S T R A K* (Vol. 5, Issue 2). https://e-journal.unper.ac.id/index.php/informatics

Anugrah, D., C Mediyastuti Sofyan, M. (2025). *Keamanan Siber di Kementerian Komunikasi dan Digital: Studi Tentang Pengembangan Kebijakan Keamanan Data dan Perlindungan Privasi Pengguna di Era Digital*. *05*(01), 47–55. https://doi.org/10.52496/identitas.v5i1.698

Anugrah, S., Raihana Qalby, N., Himawan, M. Z., C Nurmiati, E. (2025). *Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis The Influence of Professional Ethics on Information Security in the Context of the BSI Data Breach: A Systematic Literature Study*. *11*(2), 106–112.

Aranda, K., C Suryanti, F. I. (2025). Studi Literatur: Peran Elemen Komunikasi Internal dan Teknologi Digital dalam Meningkatkan Kepuasan Kerja Karyawan. *Jurnal Ilmu Sosial Humaniora Indonesia*, *4*(2), 306–317. https://doi.org/10.52436/1.jishi.206

Bayu Taruno, R., Wahyu Winarno, W., Adhipta, D., C Teknik Elektro dan Teknologi Informasi, J. (n.d.). *Se m ina r Na sio na l Te kno lo g i Info rm a si da n Multim e dia 2014 STMIK AMIKO M Yo g y a ka rta , 8 Fe b rua ri 2014 STRATEGI "BRING YOUR OWN DEVICES" PADA PERUSAHAAN SEBAGAI TANTANGAN PENYELARASAN BISNIS DAN TI UNTUK MEMENUHI SASARAN FINANSIAL*.

Bintang Praja, A.-T., Tahir, M., Cahyani, W. I., Zahro'eva, N., Anam, S., C Prameswari, A. (2025). *Jurnal Restikom : Riset Teknik Informatika dan Komputer Implementasi Monitoring dan Logging Jaringan WiFi Ruang Kelas Berbasis Digital di Universitas Trunojoyo Madura Menggunakan Wireshark dan Power BI*. *7*(1), 97–105. https://restikom.nusaputra.ac.id

Candro, D., Sinaga, P., Sitorus, M., Ary, E., Marpaung, P., Lubisndra, R. H., Amalliaendra, D. N., Informatika, T., Nusantara, P., C Bisnis,). (2025). PENGUATAN LITERASI DIGITAL MELALUI PENGENALAN KECERDASAN BUATAN DI KALANGAN PELAJAR. In *Communnity Development Journal* (Vol. 6, Issue 3).

Chairiyah Batubara, S., Syamsul Maarif, M., C Eko Irianto, H. (2017). *MODEL MANAJEMEN RANTAI PASOK INDUSTRI PERIKANAN TANGKAP BERKELANJUTAN DI PROPINSI MALUKU* (Vol. 8, Issue 2). *d7dcf44b873083a30c18b0edddS8bc81ceafcd2cS01e3f1cf5efcadbfa2b2S2e*. (n.d.).

Damanik, B. (2016). MENINGKATKAN KEAMANAN DATA DENGAN MENGUNCI FOLDER PADA WINDOWS 7 TANPA SOFTWARE. *Jurnal Mahajana Inforamasi*, *1*(1).

Fachrudin, R., Respaty, E., Adilah, I. S., C Sinlae, F. (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. *Nusantara Journal of Multidisciplinary Science*, *2*(1). https://jurnal.intekom.id/index.php/njms

Faisal, A., C Cupiadi, H. (2024). *Sinergi International Journal of Logistics Cybersecurity in Digital Supply Chains: A Narrative Review of Threats and Strategic Frameworks for Sustainable Logistics*. *3*(2). https://journal.sinergi.or.id/

Fenti Cahyani, Desyawati Utami, Izzatu Millah, C Mugi Wahidin. (2025). Studi Komparasi Kualitas Hidup dan Kinerja pada Karyawan dengan Model Kerja Hybrid dan Full-Remote di Yayasan XYZ Jakarta Selatan. *Sehat Rakyat: Jurnal Kesehatan Masyarakat*, *4*(1), 46–55. https://doi.org/10.54259/sehatrakyat.v4i1.4113

Gisma Putra, F., C Soewito, B. (n.d.). *Measurement of Security System Performance on Websites of Personnel Information Systems in Government Using Common Vulnerability Scoring System*. https://www.acunetix.com/,

Hatmoko, J. U. D., C Kistiani, F. (2017). Model Simulasi Risiko Rantai Pasok Material Proyek Konstruksi Gedung. *MEDIA KOMUNIKASI TEKNIK SIPIL*, *23*(1), 1. https://doi.org/10.14710/mkts.v23i1.14697

Hilda, S. D., Heryana, N., C Ridha, A. A. (2024). WEBSITE SECURITY ANALYSIS CURUG VILLAGE GOVERNMENT USING OPEN WEB APPLICATION SECURITY PROJECT (OWASP). *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3S1). https://doi.org/10.23960/jitet.v12i3s1.5236

Hudin, N. S., Habidin, N. F., C Othman, J. (2019). Risk Communication Framework towards High-Performance Food Supply Chain. *International Journal of Academic Research in Business and Social Sciences*, *S*(12), 820–834. https://doi.org/10.6007/IJARBSS/v9-i12/6795

Judul, S., Tantangan, :, Kerja, B., Teknologi, D., Di, H., Hybrid, E., Charlos Hutabalian, J., Lumban Tobing, J. M., C Simbolon, M. S. (2025). *Jurnal Ilmu Ekonomi dan Bisnis DIGITAL DI INDONESIA* (Vol. 3, Issue 2).

Kajan, E. (2004). The Maturity of Open Systems for B2B. In *ACM SIGEcom Exchanges* (Vol. 5, Issue 2).

Kieras, T., Farooq, M. J., C Zhu, Q. (2019). *RIoTS: Risk Analysis of IoT Supply Chain Threats*. http://arxiv.org/abs/1911.12862

Kipkoech Denzel. (2025). A survey of security in zero trust network architectures. *GSC Advanced Research and Reviews*, *22*(2), 182–214. https://doi.org/10.30574/gscarr.2025.22.2.0036

Kumar, P., C Aziz, S. (2023). Managing Supply Chain Risk with the Integration of Internet of things in the manufacturing Sector of Pakistan. *Dutch Journal of Finance and Management*, *5*(2), 22405. https://doi.org/10.55267/djfm/13676

Meijler, T. D., C Nietzold, F. (2011). *Light-weight Model-based Realization of a B2B Protocol and a SOA Integration Engine*.

Meilinda, S., C Sutapa, N. (2019). *Analisis Risiko Keamanan Rantai Pasok di Perusahaan Jasa Ekspedisi Sebagai Dasar Penerapan ISO 28000* (Vol. 7, Issue 2).

Mutakin, A., C Hubeis, M. (2011). Hubeis-Pengukuran Kinerja Manajemen Rantai Pasokan | 89. In *Jurnal Manajemen dan Organisasi: Vol. II* (Issue 3).

Mutiah, N., Rusi, I., Sistem Informasi, J., C MIPA UniversitasTanjungpura Jalan Hadari Nawawi, F. H. (n.d.). *Coding: Jurnal Komputer dan Aplikasi MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS (FMEA) DAN KONTROL ISO/IEC 27001:2013 (Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Sambas)*.

Nurcahyo, C. B., Putu, I., C Wiguna, A. (n.d.). *Jurnal Aplikasi Teknik Sipil Analisis Risiko Rantai Pasok Beton Ready Mix pada Proyek Pembangunan Apartemen di Surabaya*.

Nurillah, R. A., C Trihandoyo, A. (n.d.). *Analisis Faktor-Faktor Keamanan Informasi Perusahaan Dalam Penerapan Bring Your Own Device (BYOD)*. https://doi.org/10.37817/ikraith-informatika.v8i2*pena-fokus-vol-5-no-1-70-80*. (n.d.).

Pengabdian, J., C Berdampak, M. (2025). *Peningkatan Keterampilan Teknologi Digital untuk Siap Kerja di Era Global Memanfaatkan Pembelajaran Hybrid* (Vol. 1, Issue 2).

https://journals.raskhamedia.or.id/index.php/jupembaDOI:https://doi.org/99.99999/jupembA.v9i9.999

Professor, A., Year, F., C Author, C. (2024). Securing Generative AI: A Survey on the Role of Secure Access Service Edge (SASE) in Mitigating Exploitability. *International Journal of Innovative Science and Research Technology*, *S*. https://doi.org/10.5281/zenodo.14575878

PROSIDING Webinar Nasional Ilmu Komunikasi FISIP-Universitas Jenderal Soedirman. (n.d.). https://datareportal.com/digital-in-indonesia.

Putra, R. G., Fauzi, A., Prasetyo, E. T., Pratama, S. R., Ramadhan, I. D., Febriyanti, F., C Nurlela, S. (n.d.). *Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id 3. Universitas Bhayangkara Jakarta Raya, Indonesia, ery.teguh@ubharajaya.ac.id 4*. *2*(1). https://doi.org/10.38035/jim.v2i1

Ranaweera, P., Imrith, V. N., Liyanage, M., C Delia Jurcut, A. (n.d.). *Security as a Service Platform Leveraging Multi-Access Edge Computing Infrastructure Provisions*.

Risiko Rantai Pasok Tebu Illia Seldon Magfiroh dan Rudi Wibowo, M., Risiko Rantai Pasok Tebu, M., Seldon Magfiroh dan Rudi Wibowo, I., Kalimantan, J., C Tegal Boto Jember Jawa Timur, K. (n.d.). *The Supply Chain Risk Management of Sugarcane (Case Study in PTPN X)*.

Salim, A., C Halim, A. (2025). Penerapan VPN (Virtual Private Network) untuk Keamanan Komunikasi Antar Perangkat loT pada Jaringan Smart Home. *Karapan Network Journal*, *I, No.I*. https://doi.org/10.20473/KNJ.I.I.316-326

Saputra, A. D., Dione, F., C Uluputty, I. (2023). Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *5*(2), 159–187. https://doi.org/10.33701/jtkp.v5i2.3735

Septian, R., Kenotariatan, C. M., C Hukum, F. (n.d.). *PERLINDUNGAN HUKUM PERJANJIAN LISENSI RAHASIA DAGANG DI INDONESIA*.

Shantilawati, I., Zebua, S., C Tarmizi, R. (2024). Jurnal Manajemen Retail Indonesia Penggunaan Digital Marketing Dalam Meningkatkan Penjualan Bisnis Retail. *Jurnal Manajemen Retail Indonesia*, *5*(1).

Soliha, E. (2008). ANALISIS INDUSTRI RITEL DI INDONESIA. *Jurnal Bisnis Dan Ekonomi (JBE)*, *15*(2), 128–142.

Solusi Penerapan Byod Berdasarkan Kontrol Keamanannya, P., C Idris, M. (2019). PEMILIHAN SOLUSI PENERAPAN BRING YOUR OWN DEVICE (BYOD) BERDASARKAN KONTROL KEAMANANNYA. *Jurnal Ilmiah MATRIK*, *21*(3).

Subagyo, A. A., Hadi Nasyuha, A., C Pratiwi, H. D. (2025). EDUKASI LITERASI DIGITAL UNTUK MENINGKATKAN KEAMANAN DATA BAGI MASYARAKAT DESA PURWOMARTANI. *PEMANAS: Jurnal Pengabdian Masyarakat Nasional*, *5*(1), 6–14.

Sugiarto, B., Dewanto, R., Susilo, T., Arismunandar, S., C Wahyudi, E. (2025). KEPEMIMPINAN DI ERA KERJA HYBRID: TANTANGAN, PELUANG, DAN STRATEGI EFEKTIF. *Sosial Dan Bisnis*, *3*(7), 36–50.

Triwahyuni, D., C Wulandari, T. A. (2016). STRATEGI KEAMANAN CYBER AMERIKA SERIKAT. In *Jurnal Ilmu Politik dan Komunikasi: Vol. VI* (Issue 1). http://www.census.gov/population/www/popc

Yulia, R., C Sidharta, V. (n.d.). Model Komunikasi Kegiatan Remote Working. In *Jurnal Ilmu Komunikasi Andalan)* | (Vol. 6, Issue 2). https://jurnal.unma.ac.id/index.php/