



Pengaruh Efektivitas Manajemen Sekuriti Dalam Keamanan Perusahaan

Cahyo Rahmat Irawan^{1*}, Achmad Fauzi², Ferry Sanjaya³, Andi Ramadhan⁴, Liza Adelia⁵, Enjelya Peronika Lumban Toruan⁶

¹Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, cahyorachmatirawan@gmail.com

²Dosen Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia

³Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia

⁴Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia

⁵Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia

⁶Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia

Corresponding Author: cahyorachmatirawan@gmail.com¹

Abstract: *The effectiveness of security management plays a crucial role in maintaining corporate security in today's digital era. This research aims to identify the impact of effective security management implementation on the level of organizational security. The research method used is quantitative and qualitative analysis of various case studies and related literature. The results show that the effectiveness of security management significantly contributes to the increased security of the company in the face of cyber and non-cyber threats. Factors such as clear policies, investment in security technology, employee training, and proactive risk management play an important role in improving security management effectiveness. In conclusion, organizations that are able to implement security management effectively will be better prepared to face modern security challenges and maintain optimal operational continuity. This study provides valuable insights for stakeholders in developing effective security strategies to protect corporate assets and information.*

Keywords: *Effectiveness, Security Management, and Corporate Security*

Abstrak: Efektivitas manajemen sekuriti memiliki peran yang krusial dalam menjaga keamanan perusahaan di era digital saat ini. Penelitian ini bertujuan untuk mengidentifikasi dampak dari implementasi manajemen sekuriti yang efektif terhadap tingkat keamanan organisasi. Metode penelitian yang digunakan adalah analisis kuantitatif dan kualitatif terhadap berbagai studi kasus dan literatur terkait. Hasil penelitian menunjukkan bahwa efektivitas manajemen sekuriti secara signifikan berkontribusi terhadap meningkatnya keamanan perusahaan dalam menghadapi ancaman cyber dan non-cyber. Faktor-faktor seperti kebijakan yang jelas, investasi dalam teknologi keamanan, pelatihan karyawan, serta manajemen risiko

yang proaktif memainkan peran penting dalam meningkatkan efektivitas manajemen sekuriti. Kesimpulannya, organisasi yang mampu mengimplementasikan manajemen sekuriti secara efektif akan lebih siap menghadapi tantangan keamanan modern dan menjaga keberlangsungan operasional perusahaan secara optimal. Studi ini memberikan pandangan yang berharga bagi pemangku kepentingan dalam mengembangkan strategi keamanan yang efektif untuk melindungi aset dan informasi perusahaan.

Kata Kunci: Efektivitas, Manajemen sekuriti, dan Keamanan Perusahaan

PENDAHULUAN

Dalam era digital yang terus berkembang, di mana teknologi informasi menjadi tulang punggung operasi bisnis, tantangan keamanan informasi semakin kompleks dan menuntut. Tidak hanya perusahaan-perusahaan besar, tetapi juga bisnis skala kecil dan menengah, rentan terhadap berbagai ancaman cyber yang berkembang dengan cepat. Ancaman tersebut mencakup serangan malware, ransomware, serangan phishing, pencurian data, dan bahkan serangan yang diarahkan secara spesifik terhadap infrastruktur perusahaan. Dalam konteks ini, manajemen sekuriti memainkan peran yang sangat penting sebagai garis pertahanan utama dalam melindungi aset, informasi sensitif, serta reputasi perusahaan. Manajemen sekuriti melibatkan serangkaian strategi, kebijakan, prosedur, dan teknologi yang dirancang untuk mengidentifikasi, mencegah, dan merespons ancaman keamanan yang mungkin timbul. Efektivitas dari manajemen sekuriti sangat mempengaruhi kemampuan sebuah perusahaan untuk menjaga integritas dan kerahasiaan informasi, meminimalkan risiko kerugian finansial, menjaga kepercayaan pelanggan, dan mematuhi peraturan dan standar keamanan yang berlaku.

Pentingnya manajemen sekuriti dalam konteks keamanan perusahaan menjadi semakin menonjol karena meningkatnya jumlah serangan cyber yang terjadi dan dampak yang dapat merusak bisnis. Data sensitif, seperti informasi keuangan, data pribadi pelanggan, dan rahasia dagang, menjadi sasaran utama bagi para penyerang. Kerugian yang ditimbulkan dari kebocoran atau kehilangan data dapat sangat merugikan, baik secara finansial maupun reputasi. Selain itu, keberhasilan manajemen sekuriti juga memiliki dampak langsung pada efisiensi operasional dan produktivitas perusahaan. Dengan sistem yang aman dan terjamin, karyawan dapat bekerja dengan lebih percaya diri dan efektif, tanpa harus khawatir akan risiko keamanan yang mengancam. Hal ini membantu meningkatkan kinerja keseluruhan perusahaan dan memperkuat daya saing di pasar yang kompetitif.

Berdasarkan latar belakang masalah di atas, maka rumusan masalah pada penelitian ini yaitu:

1. Bagaimana efektivitas manajemen sekuriti dapat mempengaruhi tingkat keamanan perusahaan dari serangan cyber dan pelanggaran keamanan lainnya?
2. Apa saja tantangan utama yang dihadapi oleh perusahaan dalam menerapkan manajemen sekuriti yang efektif untuk melindungi aset dan informasi sensitif mereka?
3. Apa strategi terbaik yang dapat diadopsi oleh perusahaan dalam mengatasi tantangan dalam menerapkan manajemen sekuriti yang efektif?

KAJIAN PUSTAKA

Efektivitas

Efektivitas manajemen sekuriti merujuk pada seberapa baik sebuah sistem atau proses manajemen sekuriti dapat mencapai tujuannya dalam melindungi aset, informasi, dan infrastruktur perusahaan dari ancaman keamanan. Ketika menggunakan teknologi telekomunikasi dan informasi untuk komunikasi elektronik untuk mengirim dan mengelola dokumen dan surat, sangat penting untuk memaksimalkan efisiensi dan efektivitas. (Tiara et

al., 2023). Dalam konteks manajemen perusahaan, Efektivitas dapat diartikan sebagai kemampuan organisasi untuk mencapai tujuan dan sasaran yang telah ditetapkan secara efektif dan efisien (Triaji, 2022). Pada dasarnya, efektivitas mengukur sejauh mana manajemen sekuriti berhasil dalam melaksanakan fungsinya untuk mencegah, mendeteksi, merespons, dan memulihkan diri dari ancaman keamanan yang mungkin timbul.

Untuk menjelaskan efektivitas manajemen sekuriti, beberapa aspek yang penting dapat diperhatikan:

1. Pencegahan: Seberapa baik sistem manajemen sekuriti mencegah terjadinya serangan dan pelanggaran keamanan. Ini mencakup implementasi kebijakan keamanan, konfigurasi teknologi keamanan, dan prosedur-prosedur yang dirancang untuk mencegah akses yang tidak sah ke sistem dan data perusahaan.
2. Deteksi: Kemampuan untuk mendeteksi ancaman keamanan dengan cepat dan efektif. Hal ini melibatkan penggunaan teknologi deteksi dini, seperti sistem deteksi intrusi (IDS) atau sistem deteksi ancaman (Threat Detection Systems), serta monitoring aktif terhadap aktivitas yang mencurigakan atau tidak biasa.
3. Respon: Bagaimana perusahaan merespons terhadap ancaman keamanan yang terdeteksi. Respon ini meliputi tindakan cepat untuk menanggapi serangan, mengisolasi atau membatasi kerusakan, dan mengambil langkah-langkah untuk memulihkan operasi normal sesegera mungkin.

Selain itu, efektivitas manajemen sekuriti juga dapat dinilai dari perspektif biaya dan efisiensi. Sebuah sistem manajemen sekuriti yang efektif harus mampu mencapai tujuan keamanan dengan biaya yang wajar dan tanpa mengganggu operasi bisnis secara berlebihan. Efektivitas manajemen perusahaan dapat diukur melalui berbagai cara, termasuk analisis kinerja, pengukuran tingkat keamanan, pengukuran efisiensi, dan pengukuran kualitas layanan (Fathurrochman et al., 2022). Dengan demikian, efektivitas manajemen sekuriti merupakan tolok ukur utama dalam mengevaluasi kualitas dan kinerja sistem keamanan suatu perusahaan. Semakin tinggi tingkat efektivitasnya, semakin baik perusahaan dalam melindungi aset dan informasi mereka dari berbagai ancaman keamanan.

Manajemen Sekuriti

Manajemen sekuriti adalah pendekatan sistematis untuk mengelola risiko keamanan informasi dan infrastruktur teknologi informasi suatu organisasi. Tujuan utama dari manajemen sekuriti adalah untuk melindungi aset dan informasi yang vital dari berbagai ancaman keamanan, seperti serangan cyber, pencurian data, atau pelanggaran keamanan lainnya. Pendekatan manajemen sekuriti melibatkan identifikasi, penilaian, perlindungan, pemantauan, dan pengendalian terhadap risiko keamanan yang mungkin dihadapi oleh organisasi. Menurut (Pradhana & Wibowo, 2020) Manajemen keamanan (security manajemen) merupakan tindakan yang harus dilakukan untuk menjamin upaya keamanan dan mencegah kerugian, sehingga tidak terjadi kegagalan yang dapat mengakibatkan kerugian. Manajemen merupakan suatu kebutuhan yang sangat penting untuk memperlancar tercapainya tujuan manusia tersebut dalam suatu organisasi.(Seni & Fauzi, 2022). Manajemen sekuriti juga melibatkan implementasi langkah-langkah perlindungan untuk mengurangi kemungkinan terjadinya serangan atau pelanggaran keamanan. Ini bisa meliputi penerapan kebijakan keamanan, penggunaan teknologi keamanan seperti firewall dan antivirus, serta penggunaan kontrol akses yang ketat untuk mengontrol akses terhadap aset dan informasi sensitif.

Keamanan Perusahaan

Keamanan perusahaan adalah praktik yang berkaitan dengan melindungi aset, data, dan sumber daya perusahaan dari ancaman internal dan eksternal yang berpotensi merugikan. Ini

mencakup berbagai aspek, termasuk keamanan fisik, keamanan informasi, keamanan jaringan, keamanan siber, dan keamanan karyawan. Keamanan perusahaan dapat diukur melalui berbagai cara, termasuk analisis kinerja, pengukuran tingkat keamanan, pengukuran efisiensi, dan pengukuran kualitas layanan (Damarjati & Sutianingsih, 2023). Dalam konteks keamanan data perusahaan, manajemen sekuriti dapat membantu dalam mengidentifikasi, menganalisis risiko, serta mengidentifikasi langkah-langkah potensial sebagai upaya mitigasi terhadap risiko sistem informasi perusahaan (Naibaho & Tjahjadi, 2022)

Keamanan perusahaan mencakup langkah-langkah proaktif seperti penerapan kebijakan keamanan, pelatihan karyawan tentang praktik keamanan, penggunaan teknologi keamanan seperti firewall dan antivirus, serta tindakan responsif seperti pengawasan dan deteksi kegiatan mencurigakan. Tujuan utamanya adalah untuk mencegah kerugian atau pencurian data, melindungi reputasi perusahaan, mematuhi peraturan dan kebijakan, serta menjaga kelangsungan bisnis yang lancar, keamanan perusahaan juga dapat terpengaruh oleh berbagai faktor, seperti strategi bisnis, orientasi pembelajaran, kemampuan manajemen, dan manajemen konflik (Shoalihin et al., 2023)

Penelitian Terdahulu

Tabel 1. Penelitian Terdahulu Yang Relevan

No	Author (Tahun)	Judul Penelitian	Hasil Riset Terdahulu	Perbedaan/ Novelty
1	(Susanto, Julia, et al., 2023)	Analisis Sistem Manajemen Sekuriti PT Unilever	PT Unilever Indonesia, Tbk mengelola risiko dan peluang dengan cara yang dipertimbangkan secara cermat, terstruktur, terkendali dan efektif. Perusahaan telah membentuk jaminan internal dan pengawasan kepatuhan untuk meninjau pengaturan risiko strategis	Perbedaan atau Novelty ada pada variabel keamanan perusahaan
2	(Erniyanti et al., 2024)	Penerapan Manajemen Sekuriti Dengan Standar, Komponen, dan K3 DI PT. Pertamina Hulu Rokan	Dalam hal ini dapat disimpulkan bahwa standar dan komponen K3 diperlukan untuk memandu perilaku karyawan agar dapat melaksanakan aturan yang telah dibuat. Dalam hal ini K3 merupakan upaya untuk mengurangi resiko kecelakaan kerja bagi pekerja.	Perbedaan atau Novelty ada pada variabel Efektivitas
3	(Soesanto, Lande, et al., 2023)	Analisis Sistem Manajemen Keamanan Di Perusahaan Tokopedia Dalam Meningkatkan Proteksi Data Dan Privasi Pengguna	sistem manajemen keamanan di perusahaan Tokopedia telah dikembangkan dengan baik dan memenuhi standar keamanan informasi yang tinggi. Tokopedia telah berhasil melaksanakan strategi dan tindakan keamanan informasi yang efektif untuk melindungi data dan privasi pengguna.	Perbedaan atau Novelty ada pada variabel Efektivitas
4	(Sofiyan et al., 2024)	Perkembangan Management Sekuriti Di PT Bank Central Asia (BCA)	Keamanan informasi adalah perlindungan perangkat komputer dan non-komputer, peralatan, data dan informasi dari penyalahgunaan oleh orang yang tidak berwenang.	Perbedaan atau novelty pada variabel keamana perusahaan

5	(Soesanto, Masyurroh, et al., 2023)	Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia	Sistem keamanan di PT SK Keris Indonesia masih belum terkoordinasi dengan baik karena kurangnya pemahaman tugas dan tanggung jawab antara polisi, aparat keamanan, dan masyarakat sekitar.	Perbedaan atau Novelty ada pada variabel Efektivitas
6	(Bakhtiar & Hidayat, 2020)	Evaluasi Sistem Manajemen Keamanan Informasi Berdasaran penilaian Indeks Kami v.4.2 Pada Dinas XYZ Provinsi Jawa Tengah	Kegagalan memenuhi persyaratan sertifikasi ISO/IEC 27001 jelas berdampak pada risiko keamanan data yang Anda kelola dan harus segera diatasi. Berdasarkan kesenjangan ancaman yang ada, laporan ini memberikan rekomendasi remediasi dan langkah-langkah spesifik untuk meningkatkan keamanan data.	Perbedaan atau Novelty ada pada variabel Efektivitas
7	(Soesanto, Ramadhon, et al., 2023)	Manajemen Sekuriti di PT Sumber Alfaria Trijaya Tbk. dalam Meningkatkan Keamanan Sistem Data,mm	PT Sumber Alfaria Trijaya Tbk memiliki banyak informasi pelanggan yang harus dijaga kerahasiaannya dan perlindungan data yang kuat juga dibutuhkan untuk menghindari pencurian data oleh pihak-pihak yang tidak bertanggung jawab.	Perbedaan atau Novelty ada apa keamanan Perusahaan
8	(Budi & Tarigan, 2018)	Konsep dan Strategi Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (kami) dan Evaluasi Kesadaran Keamanan Informasi Pada Pengguna	Semua organisasi mengandalkan sumber daya teknologi informasi untuk bertahan hidup, berkembang, dan bersaing di pasar global. Selain banyak manfaatnya yang besar, teknologi informasi juga membawa risiko yang sangat signifikan.	Perbedaan atau Novelty ada pada variabel Efektivitas
9	(Soesanto, Wijayanti, et al., 2023)	Sistem Manajemen Sekuriti PT. Pertamina (Persero)	PT.Pertamina (Persero) merupakan badan usaha milik negara yang mengelola sumber daya minyak dan gas. Sebagai mesin perekonomian negara, PT.Pertamina (Persero) merupakan badan usaha milik negara yang bergerak di bidang energi, antara lain minyak, gas, energi baru, dan energi terbarukan	Perbedaan atau Novelty ada pada variabel Efektivitas
10	(Wijaya et al., 2023)	Implementasi Manajemen Sekuriti PT. KAI: K3, Manajemen Risiko, dan Standar Keamanan pada Perlintasan Kereta Api	Meskipun pintu perlintasan kereta api sangat penting bagi keselamatan pejalan kaki, namun masih banyak perlintasan kereta api yang tidak memiliki gerbang, seperti yang digunakan oleh peneliti JL. Migrasi dilaksanakan. Ampera, Burak Kapal, Bekasi Timur.	Perbedaan atau Novelty ada pada variabel keamanan perusahaan

11	(Susanto, Moses, et al., 2023)	Analisis dan Pengembangan Sistem Manajemen Sekuriti pada PT. Denso Manufacturing Indonesia	PT Denso Indonesia senantiasa berupaya menjaga kualitas produknya, menjaga hubungan harmonis dengan masyarakat luas, serta mendorong karyawannya untuk tetap kreatif dan inovatif di masa peningkatan permintaan ini berupaya menjaga kepuasan konsumen.	Perbedaan atau Novelty ada pada variabel Keamanan Perusahaan
12	(Saputra et al., 2024)	Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo	Penerapan manajemen keamanan yang efektif di Kementerian Komunikasi dan Informatika perlu menjadi bagian integral dari strategi berkelanjutan dalam menghadapi ancaman siber.	Perbedaan atau Novelty ada pada variabel Keamanan Perusahaan
13	(Soesanto, Dwi Cahyani, et al., 2023)	Manajemen Sekuriti: Pengamanan Objek Vital Pada PT. Nusa Halmahera Minerals	Sistem Keamanan File PT.NHM menggunakan situs resmi yang menggunakan berbagai teknologi dan prosedur keamanan untuk melindungi data perusahaan dari akses, penggunaan, dan pengungkapan yang melanggar hukum.	Perbedaan atau Novelty ada apa variabel Efektivitas
14	(Soesanto, Salsabilah, et al., 2023a)	Peran Manajemen Sekuriti Bank BRI untuk Menjaga Kepercayaan Nasabah	Pengendalian keamanan berperan penting dalam menjaga kepercayaan nasabah terhadap Bank BRI. Bank BRI telah melakukan beberapa upaya untuk menjaga kepercayaan nasabah terhadap keamanan perusahaan.	Perbedaan atau Novelty ada pada variabel Keamanan Perusahaan
15	(Soesanto, Salsabilah, et al., 2023b)	Peran Manajemen Sekuriti di Bank BRI Dalam Pengamanan File Nasabah untuk Mencegah Ancaman Cyber Security dan Menjaga Objektivitas Nasional	Manajemen keamanan Bank BRI berperan penting dalam melindungi file nasabah dan menjaga netralitas negara dengan menerapkan teknik keamanan informasi terkini, pemantauan jaringan secara berkelanjutan, dan pelatihan pegawai mengenai ancaman keamanan.	Perbedaan atau Novelty ada pada Efektivitas Manajemen Sekuriti

METODE PENELITIAN

Penelitian ini merupakan penelitian deskriptif kualitatif yang bertujuan untuk mendapatkan pemahaman yang mendalam tentang pengaruh efektivitas manajemen sekuriti terhadap keamanan perusahaan. Pendekatan kualitatif dipilih karena memungkinkan peneliti untuk mengeksplorasi nuansa dan kompleksitas fenomena yang kompleks seperti manajemen sekuriti dan keamanan perusahaan.

Penelitian ini didasarkan pada teori-teori dan konsep-konsep yang relevan dalam bidang manajemen sekuriti, keamanan perusahaan, dan teori organisasi. Tinjauan pustaka akan mengidentifikasi penelitian terdahulu yang relevan, baik dalam publikasi domestik maupun internasional.

HASIL DAN PEMBAHASAN

Peran dan tanggung jawab manajemen sekuriti dalam mengelola risiko keamanan.

Manajemen sekuriti memiliki peran krusial dalam menjaga keamanan perusahaan dengan mengelola risiko yang terkait. Mereka bertanggung jawab atas berbagai aspek yang meliputi penetapan kebijakan keamanan yang jelas, identifikasi potensi ancaman dan kerentanan, serta pengelolaan risiko dengan menerapkan kontrol keamanan yang tepat. Selain

itu, manajemen sekuriti juga harus memastikan bahwa karyawan memiliki kesadaran yang cukup tentang praktik keamanan yang baik melalui pelatihan dan edukasi yang tepat. Peran dan tanggung jawab manajemen sekuriti dalam mengelola risiko keamanan sangat penting dalam melindungi aset perusahaan dan meminimalisir kerugian yang dapat terjadi akibat keamanan yang tidak memadai (Pieritsz, 2021). Mereka juga harus memastikan bahwa teknologi keamanan yang diperlukan, seperti firewall dan sistem deteksi intrusi, diterapkan dan dipelihara untuk melindungi sistem informasi perusahaan Anda dari serangan. Sebagai bagian dari tugas pekerjaannya, administrator keamanan juga perlu terus memantau aktivitas keamanan perusahaan untuk mendeteksi atau menyerang kejadian mencurigakan. Mereka harus siap merespons dengan cepat dan efektif terhadap insiden keamanan yang terjadi, termasuk investigasi, pembendungan, dan remediasi jika diperlukan.

Peran dan tanggung jawab manajemen sekuriti dalam mengelola risiko keamanan sangat penting dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi serta sumber daya perusahaan. Manajemen sekuriti juga berperan dalam manajemen risiko perusahaan. Dengan mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan keamanan informasi dan operasional, manajemen sekuriti dapat membantu perusahaan untuk mengurangi potensi kerugian dan meningkatkan efisiensi dalam menjalankan operasional sehari-hari (Marfiana, 2020). Dengan menjalankan peran dan tanggung jawab ini dengan baik, manajemen sekuriti dapat membantu perusahaan mengelola risiko keamanan dengan efektif dan menjaga integritas serta ketersediaan aset dan informasi yang penting bagi kelangsungan bisnis.

Dampak positif dari manajemen sekuriti yang efektif terhadap keseluruhan operasional perusahaan.

Manajemen sekuriti yang efektif memiliki dampak yang positif yang signifikan terhadap keseluruhan operasional perusahaan. Pertama-tama, keamanan yang dikelola dengan baik membantu mengurangi risiko kehilangan data sensitif atau penting, yang dapat menyebabkan kerugian finansial, kerusakan reputasi, atau bahkan konsekuensi hukum. Dengan demikian, manajemen sekuriti yang efektif membantu melindungi aset perusahaan dan menjaga keberlanjutan operasi. Selain itu, dengan adanya kebijakan keamanan yang jelas dan diterapkan dengan konsisten, karyawan memiliki panduan yang jelas tentang bagaimana mereka harus berperilaku dan bertindak dalam lingkungan digital. Ini membantu membangun budaya keamanan di seluruh organisasi, di mana kesadaran akan risiko keamanan meningkat, dan karyawan lebih cenderung untuk mengikuti praktik keamanan yang baik. Manajemen sekuriti yang efektif dapat meningkatkan efisiensi operasional dengan mengurangi gangguan yang disebabkan oleh insiden keamanan atau serangan siber. Dengan sistem yang terlindungi dengan baik, perusahaan dapat menghindari downtime yang tidak direncanakan dan menghindari biaya pemulihan yang tinggi.

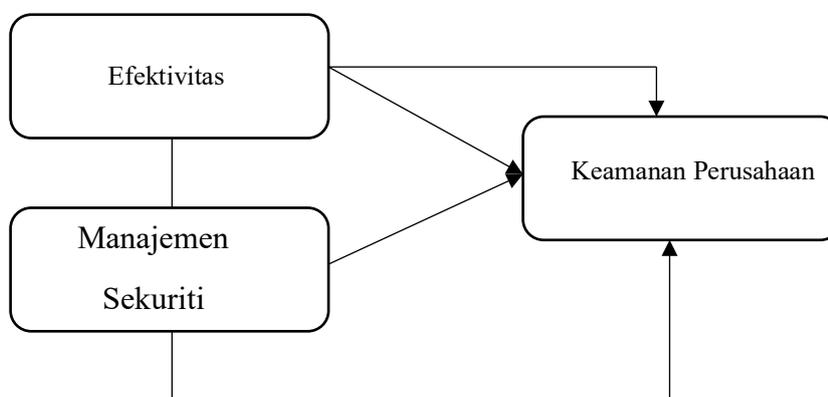
Manajemen sekuriti yang efektif membantu memperkuat kepercayaan pelanggan dan mitra bisnis. Dalam era di mana keamanan informasi menjadi semakin penting bagi pemangku kepentingan eksternal, seperti pelanggan dan mitra bisnis, sertifikasi keamanan atau kepatuhan terhadap standar keamanan tertentu dapat menjadi keunggulan kompetitif yang signifikan. Manajemen sekuriti yang baik juga membantu organisasi mematuhi peraturan dan kebijakan yang relevan. Dengan mematuhi standar keamanan yang berlaku dan menerapkan kontrol keamanan yang sesuai, perusahaan dapat mengurangi risiko sanksi hukum atau denda yang mungkin timbul akibat pelanggaran keamanan atau privasi data. Secara keseluruhan, manajemen sekuriti yang efektif tidak hanya melindungi perusahaan dari ancaman keamanan yang beragam, tetapi juga mendukung keseluruhan operasional perusahaan dengan meningkatkan efisiensi, membangun kepercayaan pelanggan, dan memastikan kepatuhan terhadap peraturan dan standar keamanan yang berlaku.

Peran manajemen sekuriti dalam melindungi aset, data, dan reputasi perusahaan.

Peran manajemen sekuriti sangat penting dalam menjaga keamanan dan kelangsungan operasional perusahaan. Salah satu peran utama mereka adalah melindungi aset, data, dan reputasi perusahaan dari berbagai ancaman yang dapat mengancam kelangsungan bisnis dan kepercayaan pemangku kepentingan. Manajemen sekuriti bertanggung jawab atas perlindungan aset perusahaan. Aset ini dapat berupa barang fisik seperti peralatan, bangunan, dan inventaris, serta aset non-fisik seperti data, informasi rahasia perusahaan, dan properti kekayaan intelektual. Melindungi aset-aset ini penting karena mereka merupakan fondasi dari operasi perusahaan. Ancaman seperti pencurian, kerusakan, atau kehilangan aset dapat memiliki dampak serius terhadap keberlangsungan bisnis. Manajemen sekuriti memainkan peran kunci dalam melindungi data perusahaan. Data adalah salah satu aset paling berharga di perusahaan modern, dan kerahasiaan, integritas, serta ketersediaannya harus dilindungi dengan ketat. Hal ini mencakup pengembangan kebijakan, prosedur, dan kontrol keamanan yang sesuai untuk melindungi data dari ancaman seperti akses tidak sah, gangguan, dan pencurian. Hal ini juga mencakup perlindungan terhadap serangan siber yang dapat membahayakan keamanan data perusahaan.

Selain menjaga aset dan data, manajemen sekuriti juga memiliki tanggung jawab untuk menjaga reputasi perusahaan. Keamanan data dan perlindungan aset tidak hanya penting untuk melindungi keberlangsungan bisnis, tetapi juga untuk memelihara reputasi perusahaan. Kehilangan data atau pelanggaran keamanan dapat menyebabkan kerusakan reputasi yang serius bagi perusahaan. Ini dapat mengurangi kepercayaan pelanggan, menurunkan nilai merek, dan mengganggu hubungan dengan mitra bisnis atau pemangku kepentingan lainnya. Oleh karena itu, manajemen sekuriti harus mengambil langkah-langkah proaktif untuk mencegah insiden keamanan yang dapat merugikan reputasi perusahaan. Manajemen sekuriti juga bertanggung jawab untuk memastikan bahwa perusahaan mematuhi semua peraturan dan standar keamanan yang berlaku. Mematuhi persyaratan keamanan ini tidak hanya mengurangi risiko hukum dan keuangan bagi perusahaan, tetapi juga membantu membangun kepercayaan pemangku kepentingan dengan menunjukkan komitmen perusahaan terhadap keamanan dan privasi data. Secara keseluruhan, manajemen sekuriti memiliki peran yang sangat penting dalam menjaga keamanan, keberlangsungan operasional, dan reputasi perusahaan. Dengan pendekatan yang holistik dan proaktif terhadap keamanan, mereka membantu memastikan bahwa perusahaan dapat beroperasi secara efisien dan aman dalam lingkungan bisnis yang semakin kompleks dan rentan terhadap ancaman keamanan.

Kerangka Konseptual



Sumber: Gambar riset

Gambar 1. Kerangka Konseptual

KESIMPULAN DAN SARAN

Manajemen sekuriti memiliki peran yang krusial dalam menjaga keamanan, keberlangsungan operasional, dan reputasi perusahaan. Dengan fokus pada perlindungan aset, data, dan reputasi, mereka memastikan bahwa perusahaan dapat beroperasi dengan aman di tengah lingkungan bisnis yang penuh dengan ancaman keamanan yang beragam. Dengan mengembangkan kebijakan, prosedur, dan kontrol keamanan yang tepat, serta mematuhi peraturan dan standar keamanan yang relevan, manajemen sekuriti membantu meminimalkan risiko keamanan yang dapat membahayakan perusahaan. Selain itu, dengan meningkatkan kesadaran karyawan tentang praktik keamanan yang baik melalui pelatihan dan edukasi yang tepat, mereka juga membangun budaya keamanan yang kuat di seluruh organisasi.

REFERENCES

- Bakhtiar, A., & Hidayat, F. S. (2020). *EVALUASI SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN PENILAIAN INDEKS KAMI v.4.2 PADA DINAS XYZ PROVINSI JAWA TENGAH*.
- Budi, D. S., & Tarigan, A. (2018). KONSEP DAN STRATEGI EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) DAN EVALUASI KESADARAN KEAMANAN INFORMASI PADA PENGGUNA. *Tahun*, 2(1).
- Damarjati, M. N., & Sutianingsih. (2023). *Peran Strategi Bisnis Memediasi Orientasi Pembelajaran, Kemampuan Manajemen Dan Dampak Work From Home Pada Kinerja Perusahaan*. 8(1), 85–95. <http://e-journal.stie-aub.ac.id/index.php/probank>
- Erniyanti, A., Soesanto, E., Annisa Putri, K., & Rahma, F. D. (2024). *PENERAPAN MANAJEMEN SEKURITI DENGAN STANDAR, KOMPONEN, DAN K3 DI PT. PERTAMINA HULU ROKAN*. 2(1).
- Fathurrochman, I., Adilah, P., Anjriyani, A., & Prasetya, A. Y. (2022). *PENGELOLAAN MANAJEMEN SEKOLAH YANG EFEKTIF*. 02(02), 1363–1374. <https://stp-mataram.e-journal.id/Amal>
- Marfiana, P. (2020). *GAMBARAN SISTEM MANAJEMEN KESELAMATAN DAN KESEHATAN KERJA DI RUMAH SAKIT*. 11(2), 182–199.
- Naibaho, B. S. G., & Tjahjadi, D. (2022). *Kajian Manajemen Risiko Sistem Informasi Menggunakan Metode Octave Allegro*.
- Pieritsz, L. R. (2021). *PERAN TATA KELOLA PERUSAHAAN DAN TANGGUNG JAWAB SOSIAL PERUSAHAAN TERHADAP MANAJEMEN LABA*.
- Pradhana, F. A., & Wibowo, P. (2020). *Analisis Pola Komunikasi Petugas pada Manajemen Sekuriti di Lembaga Pemasarakatan*.
- Saputra, F., Soesanto, E., Indah Cahyaningtyas, K., Lukmanul Hakim, Z., & Bhayangkara Jakarta Raya, U. (2024). IJM: Indonesian Journal of Multidisciplinary Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo. *IJM: Indonesian Journal of Multidisciplinary*, 2. <https://journal.csspublishing/index.php/ijm>
- Seni, & Fauzi, A. (2022). *STRATEGI PEMASARAN YANG DITERAPKAN DI HOTEL SANTIKA KEPULAUAN BANGKA BELITUNG DALAM MENINGKATKAN KUALITAS PELAYANAN DAN KEPUASAN KONSUMEN*.
- Shoalihin, Sunaryo, H., & Harijanto, D. (2023). *Dampak Manajemen Konflik Dan Kompetensi Terhadap Kinerja Pegawai Melalui Motivasi*.
- Soesanto, E., Dwi Cahyani, A., Rahma, N. H., & Ramdan, M. (2023). Manajemen Sekuriti: Pengamanan Objek Vital Pada PT. Nusa Halmahera Minerals. *Jurnal Ilmiah Multidisiplin*, 1(5), 2986–6340. <https://doi.org/10.5281/zenodo.8038861>

- Soesanto, E., Lande, A., Heru,), Sanjaya, T., Muhammad,), Hermawan, R., Bisnis, F. E., Bhayangkara, U., & Raya, J. (2023). Analisis Sistem Manajemen Keamanan Di Perusahaan Tokopedia Dalam Meningkatkan Proteksi Data Dan Privasi Pengguna. *Jurnal Kewirausahaan Dan Manajemen Bisnis*, 1(1).
- Soesanto, E., Masyuroh, A. J., Putri, G. A. M., & Maharani, S. P. (2023). Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia. *Jurnal Manajemen Riset Inovasi*, 1(3), 46–57. <https://doi.org/10.55606/mri.v1i3.1259>
- Soesanto, E., Ramadhon, A., Mardika, B. D., & Setiawan, Moch. fahmi. (2023). Mananjemen Sekuriti di PT Sumber Alfaria Trijaya Tbk. dalam Meningkatkan Keamanan Sistem Data. *Jurnal Kajian Dan Penelitian Umum*, 1(3), 110–116. <https://doi.org/10.47861/jkpu-nalanda.v1i3.227>
- Soesanto, E., Salsabilah, F., Abadi, I. C., & Rizky, M. (2023a). Peran Manajemen Sekuriti Bank BRI untuk Menjaga Kepercayaan Nasabah. In *IJM: Indonesian Journal of Multidisciplinary* (Vol. 1). <https://journal.csspublishing/index.php/ijm>
- Soesanto, E., Salsabilah, F., Abadi, I. C., & Rizky, M. (2023b). Peran Manajemen Sekuriti di Bank BRI Dalam Pengamanan File Nasabah untuk Mencegah Ancaman Cyber Security dan Menjaga Objektivitas Nasional. In *IJM: Indonesian Journal of Multidisciplinary* (Vol. 1). <https://journal.csspublishing/index.php/ijm>
- Soesanto, E., Wijayanti, A., Musyafa, M. E., & Cahyani, N. (2023). *Sistem Manajemen Sekuriti PT. Pertamina (Persero)*. <https://jurnal.arkainstitute.co.id/index.php/nautical/index>
- Sofiyan, A., Askiyah, K., Amelia, U., & Sinlae, F. (2024). Perkembangan Management Sekuriti Di PT Bank Central Asia (BCA). *Nusantara Journal of Multidisciplinary Science*, 2(1). <https://jurnal.intekom.id/index.php/njms>
- Susanto, E., Julia, M., Nisrina, G., Febriani, D. F., Bhayangkara, U., & Raya, J. (2023). Analisis Sistem Manajemen Security PT Unilever. In *IJM: Indonesian Journal of Multidisciplinary* (Vol. 1). <https://journal.csspublishing/index.php/ijm>
- Susanto, E., Moses, H., Ramadan, R., & Deanova, S. (2023). Analisis dan Pengembangan Sistem Manajemen Sekuriti pada PT. Denso Manufacturing Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, Juli, 13, 225–236. <https://doi.org/10.5281/zenodo.8149407>
- Tiara, A., Fauzi, A., Dayanti, H., Sari, N., Khotimmah, N., Roliyanah, T., & Penulis, K. (2023). *Efektivitas Penggunaan Teknologi Informasi dan Komunikasi Terhadap Tata Persuratan Elektronik (Literature Review Manajemen Sekuriti)*. 4(5). <https://doi.org/10.31933/jemsi.v4i5>
- Triaji, E. (2022). *EFEKTIVITASMANAJEMEN PEMERINTAHAN DESA: STUDI KASUS WILAYAH IV PRIANGAN PROVINSI JAWA BARAT*.
- Wijaya, C. P., Soesanto, E., Aulia, F., Aisy, H. R., & Auliya, I. (2023). Implementasi Manajemen Sekuriti PT. KAI: K3, Manajemen Risiko, dan Standar Keamanan pada Perlintasan Kereta Api. In *IJM: Indonesian Journal of Multidisciplinary* (Vol. 1). <https://journal.csspublishing/index.php/ijm>