Journal of Engineering Environment Energy and Science
Vol. 3, No. 2, Juni 2024, pp. 59 - 66
e-ISSN : 2828-6170

Dampak Teknologi Lanjutan terhadap Keamanan Data Manajemen Sekuriti: Tantangan dan Peluang di Era Digital

Yehezkiel Kharisma Yonatan[1], Tubagus Hedi Saepudin*[2], Ananda Putra Siaga[3], M. Arifin[4], Hidayat[5], Rafli Nur Firmansyah[6], Farrel Muhammad Daffa[7], Riyan Alamsyah[8]
[1,2,3,4,5,6,7,8]Teknik Industri, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia.
e-mail: [1] 202210215190@mhs.ubharajaya.ac.id,[2]***tubagus.hedi@dsn.ubharajaya.ac.id**,
[3]2202210215029@mhs.ubharajaya.ac.id, [4] 202210215183@mhs.ubharajaya.ac.id,
[5]202210215004@mhs.ubharajaya.ac.id, [6]202210215038@mhs.ubharajaya.ac.id,
[7]202210215032@mhs.ubharajaya.ac.id, [8]202210215208@mhs.ubharajaya.ac.id

Abstract

The digital era has brought about a transformation in data security management, with advanced technology at its core. These developments present new challenges and opportunities for data security practitioners in protecting sensitive information from increasingly sophisticated cyber-attacks. Understanding the impact of advanced technologies on data security in the context of security management is critical, as it affects the strategies, policies and infrastructure that organisations use to protect their data. The effectiveness of security management plays a crucial role in keeping organisations safe in today's digital age. This research aims to identify the impact of effective security management implementation on organisational security levels. The research method used is descriptive qualitative on 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. Increased connectivity, adoption of new technologies, and potential misuse of advanced technologies by attackers present new challenges for data security management. Effective security management must be comprehensive, utilise advanced technologies, and increase user awareness. Good data security is essential to protect corporate assets, maintain continuity of operations, and comply with regulations.

Keywords : *Security Management, Advanced Technology, Internet of Things (IoT), Cyber Threats, Data Security Awareness*

Abstrak

Era digital membawa transformasi dalam manajemen keamanan data, dengan teknologi canggih menjadi intinya. Perkembangan ini menghadirkan tantangan dan peluang baru bagi praktisi keamanan data dalam melindungi informasi sensitif dari serangan cyber yang semakin canggih. Memahami dampak teknologi lanjutan terhadap keamanan data dalam konteks manajemen sekuriti sangatlah penting, karena hal ini mempengaruhi strategi, kebijakan, dan infrastruktur yang digunakan organisasi untuk melindungi data mereka. 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 deskriptif 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. Peningkatan konektivitas, adopsi teknologi baru, dan potensi penyalahgunaan teknologi lanjutan oleh penyerang menghadirkan tantangan baru bagi manajemen keamanan data. Manajemen keamanan yang efektif harus komprehensif, memanfaatkan teknologi lanjutan, dan meningkatkan kesadaran pengguna. Keamanan data yang baik sangat penting untuk melindungi aset perusahaan, menjaga keberlanjutan operasi, dan mematuhi peraturan.

Kata Kunci: Manajemen Sekuriti, Teknologi Lanjutan, Internet of Things (IoT), Ancaman Cyber, Kesadaran Keamanan Data.

Submitted: **24/06/2024**; Revised: **26/06/2024**; Accepted: **28/06/2024**; Published: **30/06/2024**

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. Perkembangan teknologi sudah sangat pesat, terutama pada internet yang dapat digunakan untuk komunikasi. Tidak hanya dapat digunakan pada perangkat besar seperti komputer atau laptop yang terhubung ke jaringan, tetapi bagian dari komunikasi tersebut kini dapat diakses oleh perangkat yang lebih ringkas, khususnya ponsel(Novianto et al., 2023).

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.

Keamanan Sistem Informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memilikiarti fisik(Nurul et al., 2022). Perkembangan teknologi sudah sangat pesat, terutama pada internet yang dapat digunakan untuk komunikasi. Tidak hanya dapat digunakan pada perangkat besar seperti komputer atau laptop yang terhubung ke jaringan, tetapi bagian dari komunikasi tersebut kini dapat diakses oleh perangkat yang lebih ringkas, khususnya ponsel(Novianto et al., 2023).

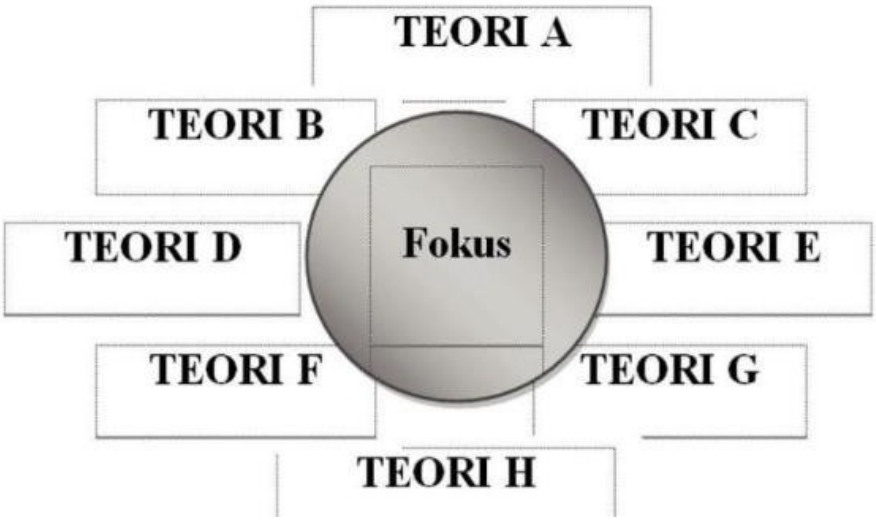
Salah satu aspek penting dari teknologi lanjutan adalah peningkatan konektivitas. Perkembangan infrastruktur jaringan, termasuk internet yang semakin cepat dan luas, telah memungkinkan organisasi untuk mengakses dan menyimpan data secara lebih efisien. Meskipun teknologi-teknologi ini membawa manfaat besar dalam hal efisiensi dan inovasi, mereka juga menimbulkan risiko keamanan tambahan. Misalnya, IoT menyebabkan peningkatan jumlah titik akses yang rentan terhadap serangan, sementara kecerdasan buatan dapat digunakan untuk mendeteksi dan merespons ancaman dengan lebih cepat, namun juga meningkatkan potensi serangan yang dipelajari.(Firmansyah et al., n.d.)Oleh karena itu, penting untuk terus memantau kinerja teknologi, mendengarkan umpan balik dari pengguna, dan melakukan perbaikan atau peningkatan yang diperlukan untuk menjaga relevansi dan efektivitasnya.
Cara kerja teknologi melibatkan serangkaian langkah yang kompleks, mulai dari identifikasi masalah hingga pengembangan, implementasi, dan pemeliharaan teknologi yang telah dibangun. Proses ini memerlukan kolaborasi antara berbagai disiplin ilmu dan melibatkan pemahaman yang mendalam tentang prinsip-prinsip ilmiah, teknis, dan praktis. Dengan pemahaman yang baik tentang cara kerja teknologi, kita dapat mengembangkan solusi yang inovatif dan efektif untuk tantangan yang dihadapi oleh masyarakat *modern*.

METODE PENELITIAN

Penelitian deskriptif kualitatif adalah istilah yang digunakan untuk menggambarkan penelitian ini. Penelitian ini didasarkan pada penelitian sebelumnya yang telah diterbitkan dalam publikasi domestik dan internasional. Selanjutnya, memanfaatkan alat Mendeley untuk berkonsultasi dengan Daftar Pustaka. Penelitian deskriptif ini merupakan pendekatan yang digunakan untuk memahami kejadian dengan mengumpulkan data informasi, berasal dari aplikasi mendeley, google scholar, google cendekia maupun *book online* lainnya.

Tujuan dari hasil penelitian kualitatif, yang dimana manajemen sekuriti ini mengimplementasikan suatu teknologi lanjutan untuk melindungi keamanan suatu data dari ancaman dan risiko yang mengancam. Penelitian ini diharapkan dapat memberikan wawasan dan solusi baru yang dapat digunakan untuk mengembangkan kebijakan keamanan data yang lebih efektif dalam menghadapi

tantangan yang terus berkembang di era digital ini. Metode yang digunakan dalam penelitian ini adalah kualitatif, bahan yang dikumpulkan berupa katakata, gambar, bukan angka, artinya hasil penelitian dibuat apa adanya atau sesuai dengan keadaan yang sebenarnya. Metode penelitian meliputi analisis permasalahan, arsitektur atau rancangan metode yang digunakan untuk menyelesaikan masalah**.** Analisis permasalahan mendeskripsikan permasalahan yang ada dan diselesaikan dalam penelitian ini. Rancangan menggambarkan cara penyelesaian masalah dan sebaiknya disajikan dalam bentuk Tabel dengan penjelasan yang lengkap.



Gambar 1 Kumpulan Bebeberapa Teori sebagai Bingkai Penerapan Kasus Penelitian

Adapun teknik pengumpulan jenis dan sumber data yang mana merupakan Langkah paling strategis dalam penelitian, karena tujuan utama dari sebuah penelitian adalah mendapatkan data. Oleh karena itu pengumpulan data yangakan dipergunakan dalam penelitian ini terbagi menjadi dua, yaitu :

1. Jenis Data Sekunder
   Data sekunder adalah data yang didapatkan dari peraturan-peraturan yang dipergunakan dalam objek penelitian yang di gunakan pada objek penelitian.
2. Jenis Data Primer
   Data primer adalah data yang diperoleh secara langsung dengan cara observasi ke lapangan secara langsung dan wawancara terhadap permasalahan yang berkaitan dalam penelitian ini. Observasi yaitu pengambilan data yang bertumpu pada pengamatan langsung terhadap objek penelitian. Sasaran yang diobservasi adalah situasi sosial dan manusia. Sedangkan wawancara dilakukan dengan proses tanya jawab yang bertujuan untuk mengetahui informasi secara mendalam dari seorang informan.

Tahapan penelitian pada penelitian ini, yaitu:

1. Menentukan Topik Penelitian
   Pada tahapan ini penulis melakukan diskusi terkait latar belakang permasalahan yang akan di di teliti.
2. Pelaksanaan Penelitian (Pengumpulan Data)
   Tahapan ini penulis mulai membagi tugas antar anggota kelompok agar pelaksanaan penelitian dapat berjalan dengan optimal.
3. Analisa Data
   Setelah data yang terkumpul dianggap sesuai dengan latar belakang penelitian yang telah ditentukan, peneliti mulai melakukan analisa data dengan menentukan pendekatan penelitian melalui studi literatur, membaca jurnal-jurnal yang telah terkumpul untuk dapat di analisa.
4. Hasil dan Pembahasan
   Adapun hasil diperoleh ketika tahapan-tahapan penelitian sebelumnya telah dilakukan dan mendapatkan hasil dari proses penelitian dan mendapatkan luaran penelitian yang sesuai dengan

Submitted: **24/06/2024**; Revised: **26/06/2024**; Accepted: **28/06/2024**; Published: **30/06/2024**

penelitian terdahulu dan merangkum dengan kajian ;aporan sendiri.

5. Kesimpulan
   Setelah didapatkan hasil penelitian yang sesuai peneliti mulai menjelaskan mengenai kesimpulan yang merupakan hasil akhir berdasarkan uraian yang sudah dijelaskan sebelumnya dari sebuah tulisan.

HASIL DAN PEMBAHASAN

Manusia lebih mampu melakukan tugasnya seiring dengan kemajuan teknologi. Misalnya, menangani dokumen yang sebelumnya disimpan secara eksklusif di lemari arsip kini dapat dilakukan berkat terciptanya sistem manajemen dokumen berbasis digital. Oleh karena itu, memiliki sistem informasi yang dapat meningkatkan efektivitas dan kualitas lembaga menjadi sangat penting. Sekitar waktu ini, banyak organisasi mulai menggunakan sistem informasi untuk mengumpulkan data untuk penggunaan di berbagai tingkatan. Pekerja memanfaatkan data terkomputerisasi untuk fungsi internal atau manajemen, untuk mempercepat layanan pelanggan, atau keduanya. Teknologi berkembang pesat, membuat tugas administrasi kantor seperti pengarsipan, dokumen, dan korespondensi — yang sering diselesaikan di lingkungan kantor menjadi lebih efektif dan efisien. Keamanan informasi sudah menjadi kebutuhan dan syarat utama untuk menjaga keberlangsungan bisnis bagi organisasi. Organisasi menghasilkan berbagai data dan informasi. Data dan informasi yang dihasilkan sangatlah berharga karena besarnya jumlah sumber daya yang dikeluarkan untuk pembuatannya. Keamanan informasi sudah menjadi kebutuhan dan syarat utama dalam menjaga keberlangsungan bisnis suatu organisasi. Suatu organisasi akan menghasilkan sejumlah data dan informasi. Data dan Informasi yang dihasilkan memiliki nilai yang sangat berharga karena banyaknya sumber daya yang telah dikeluarkan untuk menghasilkan data dan informasi tersebut. Beberapa dari data dan informasi biasanya merupakan produk yang memiliki nilai jual dan pada akhirnya dapat memengaruhi citra atau reputasi suatu organisasi(Saputra & Sucahyo, 2018).

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. bidasan malware seumpama *virus, worm spyware, dan spam* merusak beberapa aset sebelumnya menyebabkan kehilangan data.

Dalam pembahasan kali ini membahas tentang jurnal penelitian terdahulu yang telah penulis rangkum sebagai berikut:

(Rahmat Irawan et al., n.d.)Berdasar kajian pada *table* 1 manajemen keamanan memainkan peran penting dalam menjaga keamanan, kelangsungan bisnis, dan reputasi sebuah organisasi. Manajemen keamanan berfokus pada perlindungan aset, data, dan reputasi perusahaan, serta memungkinkan perusahaan untuk beroperasi dengan aman bahkan di tengah lingkungan bisnis yang penuh dengan berbagai ancaman keamanan. Berada di tengah-tengah lingkungan bisnis yang penuh dengan berbagai ancaman keamanan. Dengan mengembangkan kebijakan, prosedur, dan kontrol keamanan yang tepat serta mematuhi peraturan dan standar keamanan yang relevan, manajemen keamanan membantu meminimalkan risiko keamanan yang dapat merugikan organisasi.

(Firmansyah et al., n.d.)Teknologi memiliki dampak yang signifikan terhadap keamanan data dalam manajemen keamanan seperti yang ada pada *table* 1. Dengan perkembangan teknologi, risiko keamanan data meningkat karena serangan siber yang semakin canggih. Namun, teknologi juga memberikan solusi berupa sistem keamanan yang lebih canggih, seperti enkripsi data, sistem deteksi penyusupan, dan otentikasi ganda untuk melindungi informasi sensitif. Singkatnya, teknologi tidak hanya meningkatkan risiko keamanan data, tetapi juga memberikan solusi untuk melindungi data secara lebih efektif.

(Tiara et al., 2023)Komunikasi elektronik sangat bergantung pada teknologi informasi dan komunikasi, seperti yang terlihat dari penjelasan di atas. Teknologi informasi dan komunikasi memungkinkan kantor untuk menghemat, menyederhanakan, dan merampingkan komunikasi dan file

digital. atau file digital yang dibuat dengan menggunakan teknologi informasi dan komunikasi. Penggunaan teknologi informasi dan komunikasi dapat meningkatkan efisiensi sistem administrasi dan kecepatan pencarian file. Teknologi informasi dan komunikasi dapat membantu Anda menyelesaikan pekerjaan dengan lebih cepat seperti yang ada pada kajian *table* 1. Korespondensi elektronik atau digital menggantikan atau mengurangi penggunaan kertas dalam korespondensi.

(Soesanto et al., 2023)Aqua memiliki tradisi keselamatan yang dimulai sejak tahun 1973. Aqua telah menjadi merek nomor satu melalui peningkatan kualitas, inovasi, distribusi yang luas dan peningkatan iklan. Dalam hal pemasaran, PT Aqua terlibat dalam pemasaran langsung, periklanan, promosi penjualan, pemasaran online dan sponsor seperti kajian perbedaan pada *table* 1. Untuk penilaian keamanan, PT Aqua perlu meningkatkan kualitas produknya. Ada dua cara bagi PT Aqua untuk menilai risiko: "mengoptimalkan risiko" dan "mengelola keamanan".

(Bahtiar et al., n.d.)Berdasarkan pemetaan BAD6 Managed IT Change proses DSS02 *Managed Service Requests and Incidents* pada COBIT 2019, status penerapan tata kelola TI mengenai pengelolaan layanan TI masih belum optimal kajian tersebut terdapat pada *table* 1. Terdapat beberapa aktivitas yang belum dilakukan dan berdasarkan pemetaan proses domain AFO13 *Managed Security*, semua aktivitas yang termasuk dalam proses *Security Management* sudah dilakukan atau diimplementasikan.

Teknologi yang berkembang merupakan inti dari transformasi dalam manajemen keamanan data. Perkembangan ini memberikan tantangan dan peluang baru bagi para profesional manajemen keamanan untuk melindungi informasi sensitif dari serangan siber yang semakin canggih. Sebagai bagian dari manajemen keamanan, penting untuk memahami bagaimana teknologi yang sedang berkembang berdampak pada keamanan data, karena berdampak pada strategi, kebijakan, dan infrastruktur yang digunakan organisasi untuk melindungi data mereka.

Aspek utama dari teknologi yang sedang berkembang adalah peningkatan konektivitas. Kemajuan dalam infrastruktur jaringan, seperti kecepatan internet yang lebih cepat dan lebih luas, memungkinkan organisasi untuk mengakses dan menyimpan data dengan lebih efisien. Namun, hal ini juga membuka pintu bagi serangan siber yang lebih luas dan kompleks. Ancaman seperti serangan penolakan layanan terdistribusi (DDoS) dan *ransomware* menjadi semakin parah seiring dengan semakin canggihnya teknologi.

Selain itu, pengenalan teknologi seperti komputasi awan, kecerdasan buatan, dan *Internet of Things (IoT)* juga mengubah paradigma keamanan data. Meskipun teknologi ini membawa manfaat yang signifikan dalam hal efisiensi dan inovasi, mereka juga membawa risiko keamanan tambahan. Misalnya, IoT menyebabkan peningkatan jumlah titik akses yang rentan terhadap serangan, sementara kecerdasan buatan memungkinkan kita untuk mendeteksi dan merespons ancaman dengan lebih cepat, tetapi juga meningkatkan kemungkinan untuk mempelajari serangan

Dalam konteks manajemen perusahaan, Efektivitas dapat diartikan sebagai kemampuan organisasi untuk mencapai tujuan dan sasaran yang telah ditetapkan secara efektif dan efisien. 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.

Tantangan dan peluang teknologi lanjutan dapat kita peroleh dengan cara melakukan manajemensekuriti dan keamanan data. 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.

Submitted: **24/06/2024**; Revised: **26/06/2024**; Accepted: **28/06/2024**; Published: **30/06/2024**

Tabel 1 Penelitian Terdahulu yang Relevan

NO	Author	Judul Penelitian	Kesamaan	Perbedaan
1	(Rahmat Irawan et al., n.d.)	Pengaruh Efektivitas Manajemen Sekuriti Dalam Keamanan Perusahaan	Manajemen keamanan memainkan peran penting dalam menjaga keamanan, kelangsungan bisnis, dan reputasi sebuah organisasi	Riset ini tidak ada pengaruh *system* tentang perlindungan *asset* suatu perusahaan
2	(Firmansyah et al., n.d.)	Manajemen Sekuriti Dalam Era-Digital untuk Mengoptimalisasi Perlindungan Data dengan Teknologi Lanjutan	Teknologi memiliki dampak yang signifikan terhadap keamanan data dalam manajemen keamanan	Perbedaan atau Novelty ada pada tidak adanya data spesifik tentang solusi melindungi data
3	(Tiara et al., 2023)	Efektivitas Penggunaan Teknologi Informasi dan Komunikasi Terhadap Tata Persuratan Elektronik (Literature Review Manajemen Sekuriti)	membahas tentang Teknologi informasi dan komunikasi dapat membantu Anda menyelesaikan pekerjaan dengan lebih cepat	Perbedaan dengan riset ini tidak ada efektifitas teknologi terhadap persuratan elektronik
4	(Soesanto et al., 2023)	Assessment Manajemen Sekuriti PT AQUA	membahas tentang pentingnya keamanan sekuriti	Tidak adanya persamaan variabel teknologi dalam branding sebuah produk

5	(Bahtiar et al., n.d.)	Analisis Dan Perancangan Tata Kelola Teknologi Informasi Bumn Pada Proses Pengelolaan Layanan Dan Pengelolaan Sekuriti Teknologi Informasi Menggunakan Cobit 2019 (Studi Kasus : Pt Nindya Karya (Persero)) Analysis And Design Of Operational Control Information Technology Governance In Service Management And Information Technology Security Management Using Cobit 2019 Framework (Case Study : Pt Nindya Karya (Persero))	Implementasi Teknologi Infromasi dan Komunikasi mempermudah segala urusan	Tidak adanyapersamaan variabel teknologi dalam pengelolaan TI

KESIMPULAN DAN SARAN

Berdasarkan pembahasan di atas dapat disimpulkan bahwa dampak teknologi lanjutan pada manajemen keamanan data. Teknologi lanjutan meningkatkan kemampuan organisasi untuk mendeteksi, mencegah, dan merespons terhadap ancaman keamanan data. Peningkatan konektivitas, adopsi teknologi baru, dan potensi penyalahgunaan teknologi lanjutan oleh penyerang menghadirkan tantangan baru bagi manajemen keamanan data. Manajemen keamanan yang efektif harus komprehensif, memanfaatkan teknologi lanjutan, dan meningkatkan kesadaran pengguna. Keamanan data yang baik sangat penting untuk melindungi aset perusahaan, menjaga keberlanjutan operasi, dan mematuhi peraturan.

Saran yang penulis berikan merujuk kepada selalu meningkatkan konektivitas dan kesadaran terhadap tantangan dan peluang dari teknologi lanjutan yang dapat kita peroleh dengan cara melakukan manajemen sekuriti dan keamanan data.

DAFTAR PUSTAKA

Bahtiar, Y., Amalia, A., Fajrillah, N., Mm, B., Santosa, I., & Si, S. (n.d.). *Analisis Dan Perancangan Tata Kelola Teknologi Informasi Bumn Pada Proses Pengelolaan Layanan Dan Pengelolaan Sekuriti Teknologi Informasi Menggunakan Cobit 2019 (Studi Kasus : Pt Nindya Karya (Persero)) Analysis And Design Of Operational Control Information Technology Governance In Service Management And Information Technology Security Management Using Cobit 2019 Framework (Case Study : Pt Nindya Karya (Persero))*.

Firmansyah, P. D., Fauzi, A., Barja, R., Mulyana, A. P., Putri, T. N., Surachman, A., & Ramadhan, G. (n.d.). *Manajemen Sekuriti Dalam Era-Digital untuk Mengoptimalisasi Perlindungan Data dengan Teknologi Lanjutan*. https://doi.org/10.38035/jkmt.v2i2

Novianto, E., Heri Ujianto, E. I., & Rianto, R. (2023). Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Kepegawaian dengan Defense In Depth. *Jurnal Komputer Dan Informatika*, *11*(1), 1–6. https://doi.org/10.35508/jicon.v11i1.9139

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). *Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)*. *3*(5). https://doi.org/10.31933/jemsi.v3i5

Rahmat Irawan, C., Fauzi, A., Ramadhan, A., Adelia, L., Peronika, E., & Toruan, L. (n.d.). *Pengaruh Efektivitas Manajemen Sekuriti Dalam Keamanan Perusahaan*. https://doi.org/10.38035/jim.v3i1

Saputra, A., & Sucahyo, Y. G. (2018). *Rancangan Tata Kelola Organisasi Sistem Manajemen Keamanan Informasi Dinas Komunikasi dan Informatika Kabupaten Bekasi Organization Governance Design of Information Security Management System Bekasi Communications and Information Technology Agency* (Vol. 20, Issue 1).

Submitted: **24/06/2024**; Revised: **26/06/2024**; Accepted: **28/06/2024**; Published: **30/06/2024**

Soesanto, E., Fakultas, D., Bisnis, E., Bhayangkara, U., Raya, J., Hariyati, V., Fakultas, M., Munisari, M., & Naveli, N. (2023). *Assessment Manajemen Sekuriti PT AQUA*. *1*(2), 72–78. https://doi.org/10.54066/jurma.v1i2.321

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