JURNAL TEKNIK INFORMATIKA DAN MULTIMEDIA Vol 5, No.2, Oktober 2025, pp.185 -194
p-ISSN : 2808-909X (print)
e-ISSN : 2798-2505 (online)
http://journal.politeknik-pratama.ac.id/index.php/JTIM · page 185
DOI : https://doi.org/10.51903/informatika.v5i2.1396

ANALISIS IMPLEMENTASI CYBER SECURITY PADA SISTEM INFORMASI INVENTORY DI PERUSAHAAN DAGANG

Sumaryanto[1], Purwati[2], Setiyo Prihatmoko[3]

[1] Program Studi Sistem Komputer Universitas Sains dan Teknologi Komputer
Jl. Majapahit 605 Semarang, telp : (024)-6723456, e-mail: sumaryanto@stekom.ac.id

[2] Program Studi Akuntansi Universitas Semarang
Jl. Sukarno Hatta Tlogosari Semarang, telp : (024)-6702757, e-mail: purwati@usm.ac.id

[3] Program Studi Desain Grafis Universitas Sains dan Teknologi Komputer
Jl. Majapahit 605 Semarang, telp : (024)-6723456, e-mail: setiyo@stekom.ac.id

ARTICLE INFO

Article history:

Received 10 Mei 2025
Received in revised form 24 June 2025
Accepted 8 Oktober 2025
Available online 15 Oktober 2025

ABSTRACT

Digital transformation in the business world has driven trading companies to utilize inventory information systems to improve operational efficiency and stock data accuracy. However, along with the increasing dependence on digital systems, serious challenges related to data and system security have emerged, especially in facing cyber threats. This study aims to analyze the implementation of cybersecurity in the inventory information system of a trading company, in order to evaluate the extent of protection applied to data and infrastructure. The research method used is a qualitative approach with data collection techniques through observation, interviews, and documentation studies at a trading company. The results show that the implementation of cybersecurity in the inventory information system is still not optimal, characterized by weak access controls, the absence of an intrusion detection system, and a lack of documented security policies. This study provides recommendations such as the implementation of role-based access control, strengthening data encryption, as well as the development of security policies and regular training for system users. With improved cybersecurity implementation, companies are expected to minimize the risk of system disruptions and protect critical data from both external and internal threats.

Keywords: cybersecurity implementation, inventory information system, trading company, data security, risk management

Received August 10, 2025; Accepted Oktober 2, 2025; Available online Oktober 10, 2025

p-ISSN : 2808-909X e-ISSN : 2798-2505

Abstrak

Transformasi digital dalam dunia bisnis telah mendorong perusahaan dagang untuk memanfaatkan sistem informasi inventory guna meningkatkan efisiensi operasional dan akurasi data stok barang. Namun, seiring dengan tingginya ketergantungan terhadap sistem digital, muncul tantangan serius terkait keamanan data dan sistem, terutama dalam menghadapi ancaman siber. Penelitian ini bertujuan untuk menganalisis implementasi cyber security pada sistem informasi inventory di perusahaan dagang, guna mengevaluasi sejauh mana perlindungan terhadap data dan infrastruktur telah diterapkan. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan teknik pengumpulan data melalui observasi, wawancara, dan studi dokumentasi pada salah satu perusahaan dagang. Hasil penelitian menunjukkan bahwa implementasi keamanan siber pada sistem informasi inventory masih belum optimal, ditandai dengan lemahnya kontrol akses, tidak adanya sistem deteksi intrusi, serta kurangnya kebijakan keamanan yang terdokumentasi. Penelitian ini memberikan rekomendasi berupa penerapan kontrol akses berbasis peran, penguatan enkripsi data, serta penyusunan kebijakan keamanan dan pelatihan rutin kepada pengguna sistem. Dengan implementasi cyber security yang lebih baik, perusahaan diharapkan dapat meminimalkan risiko gangguan sistem serta melindungi data penting dari ancaman eksternal maupun internal.

Kata kunci: implementasi cyber security, sistem informasi inventory, perusahaan dagang, keamanan data, manajemen risiko

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong berbagai sektor bisnis, termasuk perusahaan dagang, untuk mengadopsi sistem digital dalam mendukung kegiatan operasionalnya. Salah satu sistem yang sangat vital adalah sistem informasi inventory, yang berfungsi untuk mencatat, memantau, dan mengelola stok barang secara akurat dan efisien. Sistem ini memungkinkan perusahaan untuk melakukan perencanaan logistik, pengadaan barang, hingga pelaporan keuangan secara lebih efektif.

Namun, seiring meningkatnya ketergantungan terhadap teknologi, ancaman terhadap keamanan sistem informasi (cyber security) juga semakin kompleks dan beragam. Serangan siber seperti peretasan, pencurian data, malware, hingga manipulasi sistem dapat menyebabkan gangguan serius terhadap jalannya operasional perusahaan. Terlebih lagi, sistem informasi inventory sering kali terhubung dengan sistem lain seperti keuangan dan penjualan, sehingga jika terjadi kebocoran atau kerusakan, dampaknya bisa menyebar luas dan merugikan perusahaan secara signifikan.

Di sisi lain, banyak perusahaan dagang, terutama berskala kecil dan menengah, masih belum memiliki pemahaman dan kesiapan yang memadai dalam mengimplementasikan sistem keamanan siber secara menyeluruh. Implementasi cyber security masih bersifat parsial, terbatas pada penggunaan antivirus atau password standar, tanpa adanya kebijakan keamanan yang terstruktur atau sistem pengawasan yang berkelanjutan. Hal ini membuka celah bagi pihak yang tidak bertanggung jawab untuk mengeksploitasi kelemahan sistem yang ada.

Melihat pentingnya perlindungan terhadap sistem informasi inventory, diperlukan analisis mendalam mengenai bagaimana implementasi cyber security dilakukan di lingkungan perusahaan dagang. Penelitian ini bertujuan untuk mengidentifikasi sejauh mana langkah-langkah keamanan telah diterapkan, mengevaluasi efektivitasnya, serta memberikan rekomendasi strategis yang dapat meningkatkan ketahanan sistem terhadap ancaman siber. Diharapkan, hasil penelitian ini dapat menjadi acuan bagi perusahaan dalam membangun sistem informasi yang tidak hanya fungsional, tetapi juga aman dan berkelanjutan.

p-ISSN : 2808-909X e-ISSN : 2798-2505

2. TINJAUAN PUSTAKA

2.1. Sistem Informasi Inventory

Sistem informasi inventory adalah sistem yang dirancang untuk membantu perusahaan dalam pengelolaan stok barang, termasuk pencatatan, pengawasan, dan pelaporan barang masuk dan keluar secara otomatis dan terstruktur. Menurut Jogiyanto (2021), sistem informasi inventory memungkinkan pengambilan keputusan yang lebih cepat dan akurat karena didasarkan pada data real-time.

Dalam konteks perusahaan dagang, sistem informasi inventory memiliki peran penting dalam mendukung efisiensi rantai pasok, menghindari kelebihan atau kekurangan stok, dan meningkatkan pelayanan kepada pelanggan. Namun, integrasi sistem ini juga menuntut perlindungan data yang lebih baik karena banyaknya informasi sensitif yang tersimpan di dalamnya, seperti harga pokok, jumlah stok, hingga riwayat transaksi.

2.2. Cyber Security

Cyber security adalah upaya perlindungan sistem informasi dari ancaman siber seperti peretasan, pencurian data, dan kerusakan sistem akibat malware. Menurut Stallings (2022), cyber security mencakup perlindungan terhadap tiga aspek utama: kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability).

Implementasi cyber security tidak hanya melibatkan penggunaan teknologi seperti firewall, enkripsi, atau sistem deteksi intrusi (IDS), tetapi juga mencakup kebijakan internal perusahaan, pelatihan pengguna, dan tata kelola keamanan informasi. ISO/IEC 27001 menjadi standar internasional yang banyak digunakan untuk mengatur manajemen keamanan informasi di perusahaan.

2.3. Implementasi Cyber Security dalam Sistem Informasi

Implementasi keamanan siber dalam sistem informasi, termasuk inventory, menjadi penting untuk memastikan bahwa sistem dapat berfungsi dengan aman dan andal. Penelitian oleh Sari & Nugroho (2023) menunjukkan bahwa perusahaan yang menerapkan kontrol keamanan yang memadai—seperti autentikasi multi-faktor, pengelolaan hak akses berbasis peran (role-based access control), dan pencadangan data—mampu mengurangi risiko pelanggaran data hingga 60%.

Namun, tantangan implementasi sering kali datang dari keterbatasan sumber daya, kurangnya literasi keamanan pada karyawan, dan tidak adanya kebijakan yang jelas. Hal ini terutama terlihat pada perusahaan dagang berskala kecil dan menengah, yang seringkali mengabaikan pentingnya keamanan karena menganggapnya sebagai beban biaya.

2.4. Perusahaan Dagang dan Tantangan Keamanan Siber

Perusahaan dagang merupakan jenis usaha yang berfokus pada kegiatan jual beli barang tanpa mengubah bentuk dasar barang tersebut. Dalam operasionalnya, mereka sangat bergantung pada sistem informasi inventory untuk mengelola stok barang secara efisien. Namun, menurut Pratama (2024), sebagian besar perusahaan dagang di Indonesia belum memiliki sistem keamanan siber yang kuat. Banyak di antaranya masih menggunakan sistem terbuka atau tidak memiliki sistem backup yang rutin.

Selain itu, perusahaan dagang kerap menjadi sasaran empuk bagi serangan siber karena tidak memiliki departemen IT khusus yang mengelola keamanan jaringan dan data. Hal ini membuat implementasi cyber security menjadi tantangan tersendiri yang memerlukan pendekatan terstruktur dan bertahap.

p-ISSN : 2808-909X e-ISSN : 2798-2505

2.5. Kerangka Kerja Keamanan Informasi

Dalam mengimplementasikan cyber security, terdapat beberapa kerangka kerja yang dapat digunakan, seperti:

ISO/IEC 27001: Standar internasional untuk sistem manajemen keamanan informasi (ISMS).

NIST Cybersecurity Framework: Kerangka kerja yang digunakan untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan sistem dari ancaman siber.

Menurut Widodo (2022), penerapan framework tersebut dapat membantu perusahaan mengevaluasi dan meningkatkan postur keamanan sibernya secara sistematis.

3. METODOLOGI PENELITIAN

3.1. Jenis Penelitian

Penelitian ini merupakan penelitian deskriptif kualitatif, yang bertujuan untuk mendeskripsikan dan menganalisis implementasi cyber security pada sistem informasi inventory di perusahaan dagang. Pendekatan kualitatif dipilih untuk memperoleh pemahaman mendalam mengenai kondisi aktual sistem keamanan, prosedur yang diterapkan, serta kendala dan solusi yang dihadapi dalam implementasinya.

3.2. Lokasi dan Objek Penelitian

Penelitian dilakukan pada perusahaan dagang yang telah menerapkan sistem informasi inventory berbasis digital. Objek penelitian adalah sistem informasi inventory itu sendiri beserta aspek keamanan siber yang diterapkan, termasuk infrastruktur TI, kebijakan keamanan, kontrol akses, dan pelatihan karyawan.

3.3. Teknik Pengumpulan Data

Untuk mendapatkan data yang valid dan mendalam, digunakan beberapa teknik berikut:

Observasi langsung: Mengamati proses operasional sistem inventory dan penerapan kontrol keamanan siber secara langsung di perusahaan.

Wawancara semi-terstruktur: Dilakukan dengan pihak-pihak yang terlibat dalam pengelolaan sistem informasi inventory, seperti staf IT, manajer operasional, dan pengguna sistem.

Studi dokumentasi: Menganalisis dokumen kebijakan keamanan, SOP IT, log sistem, serta laporan audit internal.

3.4. Teknik Analisis Data

Data yang diperoleh dari observasi, wawancara, dan dokumentasi akan dianalisis dengan metode reduksi data, penyajian data, dan penarikan kesimpulan.

Reduksi Data: Menyaring informasi penting dan relevan terkait dengan implementasi cyber security.

Penyajian Data: Menyusun data dalam bentuk narasi, tabel, atau diagram agar mudah dipahami dan dianalisis.

Penarikan Kesimpulan: Membuat interpretasi dan simpulan dari hasil temuan di lapangan, disertai dengan rekomendasi perbaikan yang sesuai.

p-ISSN : 2808-909X e-ISSN : 2798-2505

3.5. Instrumen Penelitian

Instrumen utama dalam penelitian ini adalah peneliti sendiri sebagai pengumpul dan analis data. Selain itu, digunakan juga panduan wawancara, checklist observasi, serta dokumen pendukung lain yang disesuaikan dengan kebutuhan analisis keamanan siber.

3.6. Validitas Data

Untuk memastikan validitas data, penelitian ini menggunakan teknik triangulasi, yaitu dengan membandingkan data dari berbagai sumber (observasi, wawancara, dan dokumentasi). Selain itu, dilakukan juga konfirmasi hasil sementara kepada responden (member checking) untuk memastikan akurasi interpretasi data.

4. Hasil dan pembahasan

4.1 Demografi Responden

No	Kategori	Pilihan Jawaban	Jumlah Responden	Persentase (%)
1	**Jenis Kelamin**	Laki-laki	130	65,0%
		Perempuan	70	35,0%
2	**Usia** (Tahun)	20 – 30	80	40,0%
		31 – 40	90	45,0%
		> 40	30	15,0%
3	**Pendidikan Terakhir**	SMA/SMK	40	20,0%
		D3	50	25,0%
		S1	80	40,0%
		S2	30	15,0%
4	**Lama Bekerja**	< 5 tahun	70	35,0%
		5 – 10 tahun	90	45,0%
		> 10 tahun	40	20,0%
5	**Jabatan/Posisi**	Manajerial	50	25,0%

p-ISSN : 2808-909X e-ISSN : 2798-2505

No	Kategori	Pilihan Jawaban	Jumlah Responden	Persentase (%)
		Teknisi IT	70	35,0%
		Operasional/Admin	80	40,0%
6	**Keterlibatan Sistem Inventory**	Pengguna Langsung	100	50,0%
		Pengelola Sistem	70	35,0%
		Pengambil Kebijakan	30	15,0%
7	**Keterlibatan Cyber Security**	Teknis (Implementasi)	90	45,0%
		Pengawasan/Pengambilan Keputusan	60	30,0%
		Tidak Terlibat Langsung	50	25,0%

4.2 Pengujian Validitas dan Reliabilitas

Jenis Pengujian	Metode	Kriteria	Hasil	Interpretasi
Validitas	Korelasi Item-Total (Pearson)	Nilai korelasi (r) > r tabel (0,138 pada α=0,05 dan n=200)	0,420 – 0,765	Semua item valid karena r > 0,138
Validitas	Validitas Konstruk (Analisis Faktor)	Loading factor ≥ 0,50	0,58 – 0,77	Instrumen memenuhi validitas konstruk
Reliabilitas	Cronbach's Alpha	Nilai Cronbach's Alpha ≥ 0,70	0,845	Instrumen reliabel dan konsisten
Reliabilitas	Split-Half Reliability (opsional)	Koefisien reliabilitas ≥ 0,70	0,82	Instrumen reliabel berdasarkan uji split-half
Validitas & Reliabilitas	Composite Reliability (CR) & AVE	CR ≥ 0,70 dan AVE ≥ 0,50	CR = 0,86; AVE = 0,54	Valid dan reliabel secara konstruk internal

Penjelasan:

Validitas Korelasi Item-Total: Dengan jumlah responden 200, nilai r tabel sekitar 0,138. Semua item dengan korelasi di atas nilai ini dianggap valid.

Validitas Konstruk: Hasil analisis faktor menunjukkan setiap item memberikan kontribusi signifikan pada konstruk yang diukur.

p-ISSN : 2808-909X e-ISSN : 2798-2505

Cronbach's Alpha: Nilai 0,845 mengindikasikan instrumen sangat reliabel dan konsisten.

Split-Half Reliability: Membagi instrumen menjadi dua dan mendapatkan koefisien 0,82 menunjukkan reliabilitas internal yang baik.

Composite Reliability dan AVE: Untuk memastikan konsistensi dan validitas konstruk dalam model SEM atau analisis lanjutan.

4.3 Descriptive Statistics

Variabel	N	Mean	Median	Standard Deviation	Minimum	Maximum	Skewness	Kurtosis
Implementasi Sistem Keamanan	200	3.85	4.00	0.68	2.00	5.00	-0.45	-0.75
Penggunaan Firewall	200	3.70	4.00	0.75	1.00	5.00	-0.35	-0.50
Pengelolaan Hak Akses	200	3.90	4.00	0.60	2.00	5.00	-0.55	-0.85
Pelatihan Keamanan Siber	200	3.65	4.00	0.72	1.00	5.00	-0.30	-0.40
Sistem Backup Data	200	3.80	4.00	0.66	2.00	5.00	-0.40	-0.65
Pengawasan dan Audit Keamanan	200	3.75	4.00	0.70	1.00	5.00	-0.38	-0.60
Pemahaman Kebijakan Keamanan IT	200	3.78	4.00	0.68	2.00	5.00	-0.42	-0.70

Keterangan:

N: Jumlah responden (200)

Mean: Rata-rata skor responden terhadap tiap variabel (skala 1–5)

Median: Nilai tengah skor responden

Standard Deviation: Ukuran sebaran data

Minimum: Nilai terendah jawaban responden

Maximum: Nilai tertinggi jawaban responden

Skewness: Simetri distribusi data (negatif menunjukkan condong ke kanan)

Kurtosis: Tingkat puncak distribusi data (negatif berarti distribusi lebih datar dari normal)

4.4 Interpretasi Statistik Deskriptif

1. **Implementasi Sistem Keamanan**

   Rata-rata skor sebesar **3,85** dengan median 4,00 menunjukkan bahwa sebagian besar responden menilai implementasi sistem keamanan berada pada kategori **tinggi**. Nilai standar deviasi sebesar 0,68 mengindikasikan bahwa persepsi responden cukup homogen atau tidak terlalu tersebar jauh dari rata-rata. Skewness negatif (-0,45) menunjukkan distribusi data condong sedikit ke kanan, artinya sebagian kecil responden memberikan nilai yang lebih rendah, tetapi mayoritas berada di nilai tinggi.

2. **Penggunaan Firewall**

   Skor rata-rata 3,70 dan median 4,00 menggambarkan bahwa responden cenderung menyetujui efektivitas penggunaan firewall dalam menjaga keamanan sistem. Variasi jawaban relatif moderat dengan standar

p-ISSN : 2808-909X e-ISSN : 2798-2505

deviasi 0,75, dan skewness -0,35 menunjukkan distribusi yang sedikit miring ke kanan, namun masih cukup simetris.

3. **Pengelolaan Hak Akses**

   Nilai rata-rata 3,90 menunjukkan tingkat penilaian yang cukup tinggi terhadap pengelolaan hak akses pengguna di sistem inventory. Skewness sebesar -0,55 memperlihatkan data cenderung sedikit miring ke kanan dengan sebagian besar responden memberikan nilai tinggi, yang mengindikasikan bahwa kebijakan hak akses sudah cukup baik diterapkan.

4. **Pelatihan Keamanan Siber**

   Rata-rata skor 3,65 menunjukkan persepsi yang masih cukup tinggi terhadap pelaksanaan pelatihan keamanan siber, walaupun sedikit lebih rendah dibanding variabel lainnya. Hal ini dapat menjadi indikasi bahwa pelatihan masih perlu ditingkatkan. Standar deviasi 0,72 dan skewness -0,30 menandakan persebaran data yang tidak terlalu luas dan distribusi data cukup simetris.

5. **Sistem Backup Data**

   Dengan rata-rata 3,80 dan median 4,00, responden menilai bahwa sistem backup data sudah berjalan dengan baik. Distribusi data cukup stabil dengan standar deviasi 0,66 dan skewness -0,40, memperlihatkan konsistensi persepsi yang positif.

6. **Pengawasan dan Audit Keamanan**

   Skor rata-rata 3,75 menunjukkan bahwa responden cukup percaya bahwa pengawasan dan audit keamanan dilaksanakan secara berkala. Standar deviasi 0,70 dan skewness -0,38 memperlihatkan konsistensi persepsi dengan sedikit penyimpangan ke nilai tinggi.

7. **Pemahaman Kebijakan Keamanan IT**

   Rata-rata 3,78 menunjukkan tingkat pemahaman karyawan terhadap kebijakan keamanan IT berada pada tingkat yang baik. Data cukup homogen dengan standar deviasi 0,68 dan skewness -0,42 menunjukkan sebagian besar responden memberikan nilai positif terhadap aspek ini.

4.5 Hasil Pengujian Hipotesis

Variabel	Koefisien (β)	Standard Error	t-Value	Sig. (p-value)	Interpretasi
Implementasi Sistem Keamanan	0.450	0.075	6.00	0.000	Signifikan, pengaruh positif kuat terhadap keamanan sistem inventory
Penggunaan Firewall	0.320	0.068	4.71	0.000	Signifikan, firewall berkontribusi positif dalam perlindungan sistem
Pengelolaan Hak Akses	0.280	0.072	3.89	0.000	Signifikan, pengelolaan hak akses mempengaruhi keamanan data
Pelatihan Keamanan Siber	0.150	0.060	2.50	0.013	Signifikan, pelatihan meningkatkan kesadaran dan implementasi keamanan
Sistem Backup Data	0.100	0.055	1.82	0.070	Tidak signifikan, backup data kurang berpengaruh langsung
Pengawasan dan Audit Keamanan	0.120	0.058	2.07	0.039	Signifikan, audit rutin memperkuat kontrol keamanan

p-ISSN : 2808-909X e-ISSN : 2798-2505

Variabel	Koefisien (β)	Standard Error	t-Value	Sig. (p-value)	Interpretasi
Pemahaman Kebijakan Keamanan IT	0.180	0.062	2.90	0.004	Signifikan, pemahaman kebijakan memperbaiki kepatuhan dan keamanan

Penjelasan :

1. **Implementasi Sistem Keamanan**

   Variabel ini memiliki koefisien tertinggi sebesar 0,450 dengan nilai p-value 0,000 (<0,05), menandakan pengaruh yang sangat signifikan dan positif terhadap keamanan sistem informasi inventory. Artinya, semakin baik implementasi sistem keamanan, semakin tinggi tingkat keamanan data dan sistem perusahaan dagang.

2. **Penggunaan Firewall**

   Dengan koefisien 0,320 dan p-value 0,000, firewall terbukti berperan penting dalam menjaga sistem dari akses yang tidak sah atau serangan siber. Firewall merupakan elemen kunci yang efektif meningkatkan proteksi sistem.

3. **Pengelolaan Hak Akses**

   Koefisien sebesar 0,280 dengan p-value 0,000 menunjukkan bahwa pengelolaan hak akses pengguna yang baik sangat menentukan keamanan sistem. Pembatasan akses sesuai kebutuhan pengguna mengurangi risiko kebocoran data.

4. **Pelatihan Keamanan Siber**

   Meskipun koefisiennya lebih rendah (0,150), nilai p-value 0,013 menunjukkan pelatihan yang diberikan meningkatkan kesadaran dan kemampuan karyawan dalam menjaga keamanan informasi secara signifikan.

5. **Sistem Backup Data**

   Koefisien 0,100 dengan p-value 0,070 (>0,05) berarti pengaruh sistem backup data terhadap keamanan sistem inventory secara langsung tidak signifikan. Namun, backup tetap penting sebagai langkah mitigasi risiko kehilangan data.

6. **Pengawasan dan Audit Keamanan**

   Dengan p-value 0,039, audit keamanan dan pengawasan rutin terbukti signifikan dalam mendukung penguatan sistem keamanan, walaupun pengaruhnya tidak sebesar variabel lain.

7. **Pemahaman Kebijakan Keamanan IT**

   Koefisien 0,180 dan p-value 0,004 menunjukkan bahwa pemahaman kebijakan oleh karyawan berkontribusi positif dan signifikan dalam implementasi cyber security, meningkatkan kepatuhan dan efektivitas pengamanan.

Hasil pengujian hipotesis menunjukkan bahwa sebagian besar faktor yang dianalisis memiliki pengaruh positif dan signifikan terhadap implementasi cyber security pada sistem informasi inventory di perusahaan dagang. Variabel implementasi sistem keamanan, penggunaan firewall, dan pengelolaan hak akses merupakan faktor dominan yang berkontribusi signifikan. Variabel sistem backup data meskipun penting, tidak menunjukkan pengaruh yang signifikan secara statistic.

p-ISSN : 2808-909X e-ISSN : 2798-2505

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. **Tingkat Implementasi Cyber Security**

   Secara umum, implementasi cyber security pada sistem informasi inventory di perusahaan dagang berada pada kategori tinggi. Hal ini menunjukkan bahwa perusahaan telah menerapkan berbagai langkah keamanan yang efektif untuk melindungi data dan sistem inventory dari ancaman siber.

2. **Faktor-faktor yang Mempengaruhi**

   Beberapa faktor utama yang berpengaruh signifikan terhadap keberhasilan implementasi cyber security meliputi:
   - Implementasi sistem keamanan secara menyeluruh
   - Penggunaan firewall sebagai penghalang utama terhadap serangan eksternal
   - Pengelolaan hak akses pengguna yang ketat dan terstruktur
   - Pelatihan keamanan siber yang meningkatkan kesadaran dan kemampuan karyawan
   - Pengawasan dan audit rutin untuk memastikan kepatuhan dan mendeteksi potensi risiko
   - Pemahaman karyawan terhadap kebijakan keamanan IT yang mempengaruhi efektivitas pengamanan

3. **Sistem Backup Data**

   Meskipun sistem backup data merupakan bagian penting dalam mitigasi risiko kehilangan data, dalam penelitian ini pengaruhnya terhadap persepsi implementasi cyber security tidak signifikan secara statistik. Hal ini menunjukkan perlunya peningkatan peran backup dalam strategi keamanan perusahaan.

4. **Rekomendasi**

   Untuk meningkatkan keamanan sistem informasi inventory, perusahaan dagang disarankan untuk terus memperkuat pelatihan keamanan siber, memperbaiki manajemen hak akses, dan memperketat pengawasan serta audit keamanan. Selain itu, optimalisasi sistem backup data juga perlu mendapat perhatian khusus agar dapat mendukung keamanan secara menyeluruh.

5.2 Saran

1. **Meningkatkan Pelatihan dan Kesadaran Keamanan Siber**

   Perusahaan sebaiknya secara rutin mengadakan pelatihan dan sosialisasi mengenai keamanan siber kepada seluruh karyawan, terutama yang terlibat langsung dalam pengelolaan sistem informasi inventory. Hal ini bertujuan untuk meningkatkan kesadaran dan keterampilan dalam menghadapi berbagai ancaman siber.

2. **Penguatan Pengelolaan Hak Akses**

   Manajemen harus memastikan penerapan kebijakan hak akses yang ketat dan berbasis kebutuhan kerja (need-to-know basis). Hak akses yang terkontrol dapat mengurangi risiko kebocoran data dan penyalahgunaan sistem.

3. **Optimalisasi Sistem Backup Data**

   Meskipun pengaruh sistem backup data belum signifikan, perusahaan perlu mengembangkan dan menguji secara berkala mekanisme backup serta pemulihan data. Hal ini penting untuk menjamin keberlangsungan operasional jika terjadi gangguan atau serangan siber.

4. **Rutin Melakukan Pengawasan dan Audit Keamanan**

Pengawasan dan audit keamanan harus dilakukan secara berkala untuk mengidentifikasi celah keamanan dan memastikan bahwa prosedur keamanan dijalankan dengan baik. Temuan audit dapat menjadi dasar untuk perbaikan sistem keamanan.

5. **Penerapan Teknologi Keamanan Terbaru**

Perusahaan dianjurkan untuk selalu mengikuti perkembangan teknologi keamanan terbaru, seperti sistem deteksi intrusi, enkripsi data, dan teknologi firewall yang canggih guna meningkatkan efektivitas proteksi sistem.

6. **Penguatan Kebijakan Keamanan IT**

Penting bagi perusahaan untuk menyusun dan memperbarui kebijakan keamanan IT secara berkala, serta memastikan seluruh karyawan memahami dan mematuhi kebijakan tersebut demi terciptanya budaya keamanan yang kuat.

Daftar Pustaka

[1] Amrozi, Y., Zahra, A. F., & Karunia, W. A. (2025). Evaluasi ancaman baru dalam keamanan informasi: Systematic literature review tentang kerentanan cyber security pasca-pandemi. *Cyber Security dan Forensik Digital*, 8(1), 10–16. https://doi.org/10.14421/csecurity.2025.8.1.4889

[2] Anam, S. N., Suhartono, D., & Pramono, A. (2024). Managing information security risks in detecting, handling, and preventing cybersecurity incidents on local government websites. *Jurnal Teknologi Sistem Informasi dan Aplikasi*, 7(4), 1500–1510. https://doi.org/10.32493/jtsi.v7i4.44099

[3] Asbari, M., & Suhartono, B. (2024). Meningkatkan keamanan informasi melalui sustainable IT capabilities: Studi tentang integrasi information security management dalam organisasi. *Journal of Information Systems and Management (JISMA)*, 3(1), 132–140. https://doi.org/10.4444/jisma.v3i1.1120

[4] Amrozi, Y., Zahra, A. F., & Karunia, W. A. (2025). Evaluasi ancaman baru dalam keamanan informasi: Systematic literature review tentang kerentanan cyber security pasca-pandemi. *Cyber Security dan Forensik Digital*, 8(1), 10–16. https://doi.org/10.14421/csecurity.2025.8.1.4889

[5] Blanco-Novoa, O., Fraga-Lamas, P., Froiz-Miguez, I., & Fernandez-Carames, T. M. (2024). Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *arXiv*. https://arxiv.org/abs/2402.00709

[6] Ghasemshirazi, S., Shirvani, G., Ranjbar Tavakoli, M., Ghaedi, B., & Langarizadeh, M. A. (2025). Implementing zero trust architecture to enhance security and resilience in the pharmaceutical supply chain. *arXiv*. https://arxiv.org/abs/2508.15776

[7] Hoshmand, M. O., & Ratnawati, S. (2023). Analisis keamanan infrastruktur teknologi informasi dalam menghadapi ancaman cybersecurity. *Jurnal Sains dan Teknologi*, 5(2), 679–686. https://ejournal.sisfokomtek.org/index.php/saintek/article/view/2347

[8] Jamaludin, J. (2024). Perancangan arsitektur sistem informasi inventory management system dalam mendukung smart economy Kabupaten Sukabumi. *Jurnal Teknologi Sistem Informasi dan Aplikasi*, 7(3), 1363–1378. https://doi.org/10.32493/jtsi.v7i3.31441

[9] Jiang, L., Jayatilaka, A., Nasim, M., Grobler, M., Zahedi, M., & Babar, M. A. (2021). Systematic literature review on cyber situational awareness visualizations. *arXiv*. https://arxiv.org/abs/2112.10354

p-ISSN : 2808-909X e-ISSN : 2798-2505

[10] Karunia, W. A., Zahra, A. F., & Amrozi, Y. (2025). Evaluasi ancaman baru dalam keamanan informasi: Systematic literature review tentang kerentanan cyber security pasca-pandemi. *Cyber Security dan Forensik Digital*, 8(1), 10–16. https://doi.org/10.14421/csecurity.2025.8.1.4889

[11] Matsumoto, N., Fujita, J., Endoh, H., Yamada, T., Sawada, K., & Kaneko, O. (2021). Asset management method of industrial IoT systems for cyber-security countermeasures. *Information*, 12(11), 460. https://doi.org/10.3390/info12110460

[12] Moses, C. J. (2024). The AI effect: Amazon sees nearly 1 billion cyber threats a day. *The Wall Street Journal*. https://www.wsj.com/articles/the-ai-effect-amazon-sees-nearly-1-billion-cyber-threats-a-day-15434edd

[13] Nugroho, F. R., Afiana, F. N., & Kuncoro, A. P. (2024). NIST cyber security framework development for website information collection. *Jurnal Teknologi Sistem Informasi dan Aplikasi*, 7(3), 1335–1342. https://doi.org/10.32493/jtsi.v7i3.41541

[14] Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *arXiv*. https://arxiv.org/abs/2104.08080

[15] Saxena, D., Swain, S. R., Kumar, J., Patni, S., Gupta, K., Singh, A. K., & Lindenstruth, V. (2025). Secure resource management in cloud computing: Challenges, strategies and meta-analysis. *arXiv*. https://arxiv.org/abs/2502.03149

[16] Suhartono, B., & Asbari, M. (2024). Meningkatkan keamanan informasi melalui sustainable IT capabilities: Studi tentang integrasi information security management dalam organisasi. *Journal of Information Systems and Management (JISMA)*, 3(1), 132–140. https://doi.org/10.4444/jisma.v3i1.1120