MUSYTARI
ISSN: 3025-9495

Neraca Manajemen, Ekonomi
Vol 12 no. 7 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

STRATEGI INTELIJEN BISNIS UNTUK MENGHADAPI ANCAMAN CYBER: DEFINISI DAN PENERAPAN *BUSINESS INTELLIGENCE STRATEGY* FOR ADDRESSING CYBERSECURITY: DEFINITION AND ANALYSIS

Putri Ratnasari
[1]Fakultas Ekonomi dan Bisnis, Universitas Cenderawasih
[1]putriratna046@gmail.com

Abstrak

Teknologi digital telah mengubah cara pelanggan, perusahaan, dan mitra mereka berinteraksi, menyebabkan dislokasi industri yang belum pernah terjadi sebelumnya, dan mengubah ekonomi bisnis secara signifikan. Sekarang perusahaan menggunakan berbagai teknologi, seperti seluler, Internet of Things (IoT), dan Kecerdasan Buatan (AI), untuk membangun dan memperkuat hubungannya dengan pelanggan dan mitra dengan fokus pada kebutuhan, penggunaan, dan keinginan mereka. Dalam beberapa tahun terakhir, pertumbuhan eksponensial teknologi informasi, terutama dalam hal penggunaan internet, telah memicu perdebatan tentang potensi ancaman yang dapat muncul. Jumlah ancaman dan serangan siber dan kompleksitasnya meningkat bersama dengan ukuran jaringan, yang membuat alat yang tersedia bagi penyerang semakin canggih dan efektif. Internet telah menjadi fenomena penting dalam kehidupan manusia seiring dengan kemajuan teknologi informasi. Ini memungkinkan aplikasi nirkabel seperti akses internet, pembayaran digital, dan pemesanan tiket. Meskipun ada keuntungan, penggunaan internet juga memiliki efek negatif, yaitu meningkatkan kemungkinan perilaku anti-sosial dan kejahatan siber yang sebelumnya dianggap tidak mungkin. Competitive Intelligence (CI) menjadi sangat penting dalam lingkungan bisnis yang semakin kompetitif. Komponen penting dari perencanaan dan manajemen strategis perusahaan adalah kecerdasan buatan, yang memungkinkan pengumpulan data dan informasi dari sudut pandang yang luas untuk memprediksi perubahan dalam lingkungan kompetitif. Perusahaan harus membuat proteksi yang kuat untuk mencegah serangan dari luar agar tetap beroperasi dengan baik di pasar global yang penuh persaingan. Oleh karena itu, artikel ini akan membahas definisi CI, bagaimana strategi intelijen bisnis diterapkan, dan cara bisnis dapat melindungi data mereka dari ancaman siber untuk tetap hidup dan sukses di era digital yang terus berkembang.

Kata Kunci: Ancaman Siber, Kecerdasan Kompetisi, Keamanan Data, Transformasi Digital

Article History
Received: November 2024
*Review*ed: November 2024
Published: November 2024

Plagirism Checker No 234
Prefix DOI :
10.8734/Musytari.v1i2.365

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 12 no. 7 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

Abstract

Digital technology has changed how customers, businesses, and their partners interact, causing industry disruptions that could not previously occur, and significantly altering business economics. These days, businesses use a variety of technologies, such as smartphones, the Internet of Things (IoT), and artificial intelligence (AI), to build and strengthen relationships with customers and partners by focusing on their needs, wants, and desires. In recent years, the emergence of spontaneous information technology, particularly in the area of internet usage, has sparked debate about potential ancaman. The number of sibers and ancaman increases in tandem with the size of the network, making the available tools for users more effective and efficient. The internet has become a significant phenomenon in human life due to the advancement of information technology. This enables nirkabel applications such as internet access, digital payments, and tiket transactions. Although there are benefits, using the internet also has drawbacks, such as increasing the likelihood of antisocial behavior and cyberbullying that were previously thought to be unfeasible. In a more competitive business environment, competitive intelligence (CI) is crucial. A crucial element of business strategy and management is kecerdasan, which enables the collection of data and information from extensive sources to predict changes in the competitive environment. Businesses must provide strong protection to keep off outsiders so they may continue to operate successfully in the global market with weaker penetration. Because of this, this article will discuss what CI is, how business intelligence strategies are implemented, and how businesses may protect their data from sibers to ensure their success in the constantly evolving digital age.

Keywords: *Cyber Threats, Competitive Intelligence, Data Security, Digital Transformation*

PENDAHULUAN

Cara pelanggan, perusahaan, dan mitra berinteraksi telah berubah karena teknologi digital. Kekuatan digital telah mengubah industri dengan cara yang belum pernah terlihat sebelumnya, mengubah ekonomi bisnis. Organisasi memikirkan kembali kebutuhan, penggunaan, dan keinginan pelanggannya dengan menggunakan berbagai teknologi, seperti seluler, Internet of Things (IoT), dan AI (Artificial Intelligence).

Dengan pertumbuhan pesat teknologi informasi dalam beberapa tahun terakhir, penggunaan internet untuk mendapatkan informasi telah menjadi subjek kontroversi yang semakin meningkat dan menimbulkan semakin banyak perdebatan tentang potensi bahaya yang

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 12 no. 7 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

dapat muncul. Setiap hari, jumlah ancaman meningkat, dan serangan telah meningkat baik dalam jumlah maupun kompleksitasnya. Seiring dengan meningkatnya ukuran jaringan, penyerang potensial tidak hanya menjadi lebih banyak, tetapi alat yang mereka gunakan menjadi lebih canggih, efektif, dan efisien.

Cara pelanggan berinteraksi dengan perusahaan adalah salah satu perubahan paling mencolok yang disebabkan oleh transformasi digital. Pelanggan sekarang memiliki akses yang lebih besar terhadap informasi, barang, dan layanan karena adanya internet dan teknologi komunikasi yang canggih. Mereka dapat membandingkan harga, membaca ulasan pelanggan lain, dan melakukan pembelian dengan beberapa klik. Ini berarti bahwa perusahaan harus menyediakan produk berkualitas tinggi dan pengalaman pelanggan yang memuaskan. Dalam konteks ini, perusahaan yang mampu memahami kebutuhan dan preferensi pelanggan akan memiliki keunggulan kompetitif yang signifikan.

Namun, perubahan ini juga membawa tantangan baru, terutama dalam hal keamanan data. Dengan semakin banyaknya data yang dihasilkan dan disimpan secara digital, ancaman terhadap keamanan informasi menjadi semakin kompleks. Cybercrime, yang mencakup berbagai tindakan ilegal yang dilakukan melalui internet, telah menjadi salah satu isu paling mendesak bagi perusahaan di seluruh dunia. Dari pencurian data hingga ransomware, serangan ini dapat menyebabkan kerugian finansial yang signifikan dan merusak reputasi perusahaan.

Seiring dengan pesatnya kemajuan teknologi informasi, hal ini menjadikan internet sebagai fenomena dalam kehidupan manusia. Contohnya adalah munculnya teknologi aplikasi nirkabel. Misalnya, sebuah ponsel yang dapat mengakses internet, membayar rekening bank, memesan tiket pesawat, dan lain-lain.

Selain itu, integrasi antara CI dan strategi keamanan siber dapat memperkuat pertahanan perusahaan terhadap serangan. Dengan memiliki informasi yang akurat dan terkini tentang ancaman yang ada, perusahaan dapat merespons dengan lebih cepat dan efisien. Misalnya, jika perusahaan mengetahui bahwa pesaingnya baru-baru ini mengalami pelanggaran data, mereka dapat dengan segera mengambil langkah-langkah untuk memperkuat keamanan mereka sendiri. Pendekatan ini tidak hanya melindungi data perusahaan tetapi juga meningkatkan kepercayaan pelanggan dan pemangku kepentingan lainnya.

Dalam perkembangannya, penggunaan internet membawa banyak sisi negatif. Ini meningkatkan peluang untuk tindakan perilaku anti-sosial dan kriminal yang sebelumnya dianggap tidak mungkin. Pada akhirnya, banyak orang yang melakukan penyalahgunaan dalam penggunaan teknologi komputer, yang kemudian meningkat menjadi kejahatan di dunia virtual, yang biasa disebut *cyber crime*.

Ketika banyak perusahaan bersaing dalam ekonomi global maka diperlukan suatu komponen intelijen bisnis yang bertujuan untuk mendapatkan keuntungan strategis yang biasa disebut dengan competitive intelligence (CI). Kebutuhan CI dalam konteks global menjadi hal penting untuk keberhasilan sebuah perusahaan lebih lanjut.

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 12 no. 7 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

Menurut Bose (2008), CI adalah komponen vital dari proses perencanaan dan manajemen strategis perusahaan, dimana dalam hal ini mengumpulkan data dan informasi dari sudut pandang yang sangat besar dan strategis, memungkinkan perusahaan untuk memprediksi atau memperkirakan apa yang akan terjadi dalam lingkungan kompetitifnya.

Dengan banyaknya persaingan yang dilakukan antar perusahaan, diperlukan juga proteksi untuk menangkal serangan dari luar (saingan), sehingga perusahaan tetap dapat berjalan semestinya. Artikel ini bertujuan untuk memberikan wawasan komprehensif tentang perubahan yang dibawa oleh teknologi digital, tantangan yang dihadapi oleh perusahaan, serta strategi yang dapat diterapkan untuk memastikan keberlanjutan dan keamanan dalam lingkungan bisnis yang semakin kompetitif.

METODE PENELITIAN

Metode penulisan ini menggunakan pendekatan **normatif**, yang mengandalkan data sekunder dan kepustakaan pada penggunaan bahan atau materi penelitian berdasarkan **data sekunder**. Pendekatan normatif berfokus pada analisis dan interpretasi norma, prinsip, dan kebijakan yang relevan dalam konteks penelitian. Oleh karena itu, penelitian ini tidak hanya mengandalkan data empiris, tetapi juga mempertimbangkan landasan teori dan praktik yang ada.

Data sekunder yang digunakan dalam penelitian ini mencakup berbagai sumber seperti, artikel jurnal, buku dan artikel yang menjelaskan konsep-konsep dasar mengenai transformasi digital, *Competitive Intelligence* (CI), dan keamanan data.

PEMBAHASAN

1. Pengertian *Competitive Intelligence* (CI)

Menurut Bernhardt (1995) dalam De Almeida, dkk (2016), CI dapat didefinisikan sebagai proses analitik yang mengubah data pesaing, industri, dan pasar terpilah menjadi pengetahuan strategis yang dapat ditindak lanjuti tentang kemampuan, niat, kerja, dan posisi bersaing. CI biasanya dapat ditemukan sebagai elemen dari banyak strategi perusahaan dan CI tidak menyiratkan kegiatan yang ilegal (Bressler dan Inda, 2014). CI dapat membuktikan alat yang berharga dalam memantau kegiatan pesaing, meningkatkan penjualan, dan membuat kesepakatan yang lebih baik dengan pelanggan.

Menurut Kahaner (19970 dalam Maungwa dan Ina (2018), CI adalah proses total, bukan hanya fungsi dalam perusahaan yang terdari dari empat langkah, yaitu perencanaan dan arah, pengumpulan data, analisis dan penyebaran. Data atau informasi diperlukan pada lingkungan tempat organisasi atau perusahaan berasal. Kecerdasan ini digunakan dalam pengambilan keputusan strategis.

CI dikonseptualisasikan sebagai proses pemantauan lingkungan kompetitif, dengan tujuan untuk memberikan kecerdasan yang dapat ditindak lanjuti yang akan memberikan keunggulan kompetitif bagi organisasi (Bose, 2008).

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 12 no. 7 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

Menurut Bergeron dan Hiller (2002) dalam Maungwa dan Ina (2018), CI mengacu pada pengumpulan, transmisi, analisis, dan penyebaran informasi yang relevan yang tersedia untuk umum, yang diperoleh secara etis dan legar sebagai sarana untuk menghasilkan pengetahuan yang dapat ditindak lanjuti.

Competitive Intelligence (CI) sering dikelompokkan ke dalam dua kategori, yaitu strategis dan taktis. CI strategis berfokus pada isu-isu jangka panjang seperti risiko utama dan peluang yang dihadapi perusahaan. CI taktis berfokus pada masalah jangka pendek dan memberikan input pada item, seperti meningkatkan pendapatan atau melihat pangsa pasar.

2. Penerapan *Cyber Security*

Perkembangan teknologi informasi dekade terakhir telah banyak mempengaruhi aspek kehidupan bermasyarakat dan bernegara. Era revolusi 4.0 telah membuat pentingnya peran teknologi informasi dalam semua aspek kegiatan ekonomi. Sektor ekonomi tentulah menjadi salah satu wilayah yang sangat memiliki ketertangungan yang tinggi dari peran tekonologi informasi. Sebab, banyak kegiatan ekonomi yang sangat diuntungkan dengan berkembangnya teknologi informasi. Belum lagi teknologi informasi ini juga melahirkan berbagai platform yang bisa digunakan untuk melakukan proses bisnis. Dengan demikian *cyber security* merupakan aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan cyber crime. Selain itu upaya untuk melindungi informasi dari adanya *cyber attack. Cyber att*ack dalam operasi informasi adalah semua jenis tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) informasi.

Seringkali masalah keamanan masih berada pada urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Bahkan, ketika dianggap menggangu kinerja dari sistem, seringkali aspek keamanan dikurangi atau ditiadakan. Padahal di era digitalisasi saat ini celah serangan cyber tentu akan semakin terbuka lebar. Menurut Hasibuan (2016), macam-majam bentuk kejahatan komputer yaitu:*Illegal Access*/Akses tanpa ijin ke sistem komputer dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain. *Hacking* merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi.

1. *Illegal Contents*/ Memasukkan data atau informasi tentang hal-hal yang tidak benar, tidak etis, atau yang dapat dianggap melanggar hukum atau mengganggu ketertiban umum merupakan tindakan kriminal.
2. *Data Forgery*/Pemalsuan data atau pemalsuan data adalah kejahatan dengan memalsukan data pada dokumen penting yang tersimpan sebagai dokumen tanpa script di internet. Sebagian besar, kejahatan ini ditujukan pada dokumen e-commerce dengan membuat seolah-olah salah ketik terjadi, yang pada akhirnya akan menguntungkan pelaku.

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 12 no. 7 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

3. *Spionase Cyber* atau mata-mata adalah kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki sistem jaringan komputer pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang memiliki dokumen atau data penting disimpan dalam sistem kompu.
4. Data *Theft*/adalah kegiatan memperoleh data komputer secara ilegal untuk digunakan sendiri atau diberikan kepada orang lain. Salah satu jenis kejahatan ini yang sering diikuti dengan penipuan adalah penipuan identitas. Penyebaran data juga sering diikuti oleh kejahatan ini.
5. *Misuse of devices*/menggunakan peralatan komputer dengan sengaja dan tanpa hak; memproduksi, menjual, berusaha memperoleh, menggunakan, impor, diedarkan, atau cara lain dengan tujuan untuk digunakan; atau membuat seluruh atau sebagian sistem komputer dapat diakses dengan tujuan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau merusak peralatan komputer lainnya. Contoh kejahatan komputer termasuk penyalahgunaan hak cipta, perjudian melalui komputer, pemalsuan kartu kredit, dan lainnya.

KESIMPULAN

Dari uraian di atas, dapat disimpulkan bahwa manajemen informasi (CI) adalah bagian penting dari proses perencanaan dan manajemen strategis perusahaan. Mengumpulkan data dan informasi dari sudut pandang strategis memungkinkan perusahaan untuk memprediksi dan memperkirakan apa yang akan terjadi di lingkungan kompetitifnya. Selain itu, CI mengacu pada pengumpulan, transmisi, analisis, dan penyebaran informasi yang relevan dan dapat diakses untuk umum sebagai cara untuk menghasilkan pengetahuan yang dapat ditindak lanjuti.

Karena banyaknya persaingan antar perusahaan, proteksi juga diperlukan untuk melindungi perusahaan dari serangan luar. Hasil pengamatan penekanan tombol papan ketik biasanya disimpan dalam berkas catatan, atau log file, oleh perekam ketikan.

banyak metode untuk menjaga data dan informasi yang tersimpan di media penyimpanan komputer aman. Salah satunya adalah dengan terus mengawasi program yang terinstal di komputer. Tidak ada yang mencurigakan ketika melihat struktur hardware komputer. Untuk menghindari kehilangan data penting, teknik ini harus digunakan. Namun, untuk melindungi bisnis di era digital saat ini, teknik tersebut harus dipilih dengan hati-hati.

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 12 no. 7 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

DAFTAR PUSTAKA

Bose, Ranjit. 2008. *Competitive Intelligence Process And Tools For Intelligence Analysis*. Journal Industrial Management & Data Systems, 108(4): 510-528.

Bressler, Martin S., & Inda, Bressler. 2014. *Protecting Your Company's Intellectual Property Assets From Cyber-Espionage*. Journal Of Legal, Ethical And Regulatory Issues, 17(2).

De Almeida, Fernando. C., Humbert, Lesca., & Adolpho, W. P. Canton. 2016. *Intrinsic Motivation For Knowledge Sharing – Competitive Intelligence Process In A Telecom Company*. Journal Of Knowledge Management, 20(6).

Hasibuan, Muhammad. Siddik. 2016. *Keylogger Pada Aspek Keamanan Komputer.* Jurnal Teknovasi, 3(1): 8-15.

Maungwa, Tumelo., & Ina, Fourie. 2018. *Competitive Intelligence Failures: An Information Behaviour Lens To Key Intelligence And Information Needs*. Journal Of Information Management.

Riadi, Dhekra. B. S, Anissa, Frini., Wahiba, Ben., & Naoufel, Kraiem. 2015. *Competitive Intelligence: History, Importance, Objectives, Process, And Issues.* IEEE Ninth International Conference On Research Challenges In Information Science (RCIS).