Vol. 3, No. 2, 2025, pp. 08-17

Jurnal Ilmu Ekonomi dan Bisnis

Journal homepage: https://ejournal.pkmpi.org/index.php/ijess/index

PERANAN CYBERSECURITY DALAM MENINGKATKAN KETAHANAN BISNIS DIGITAL TERHADAP CYBERCRIME

Hani Puspita Maharani[1], Herlina Bernadecka Sidauruk[2] dan Naisyah Qila Syafitri[3]

[1]hanipuspita576@gmail.com
[2]hsidauruk8@gmail.com
[2]nesyaqila2005@gmail.com

Article Info

Article history:
Received Jun 12th, 2025
Revised Jun 19th, 2025
Accepted Aug 26th, 2025

Kata Kunci:
Cybersecurity
Bisnis digital
Cybercrime
Ketahanan digital

ABSTRAK

Transformasi digital telah membawa perubahan signifikan dalam operasional bisnis, namun di sisi lain juga meningkatkan eksposur terhadap ancaman *cybercrime* yang semakin canggih. Penelitian ini bertujuan untuk menganalisis peran *cybersecurity* dalam meningkatkan ketahanan bisnis digital terhadap serangan siber. Dengan menggunakan metode analisis deskriptif, penelitian ini mengidentifikasi berbagai jenis ancaman *cybercrime* yang umum menyerang bisnis digital, seperti *phishing*, *malware*, *ransomware,* dan serangan DDoS, serta mengkaji strategi pencegahan dan mitigasi yang dapat diterapkan. Hasil kajian menunjukkan bahwa implementasi *cybersecurity* yang menyeluruh-meliputi perlindungan jaringan, aplikasi, cloud, dan informasi, didukung oleh kebijakan manajemen risiko dan peningkatan kesadaran sumber daya manusia-berperan penting dalam melindungi aset digital, menjaga kepercayaan pelanggan, dan memastikan kontinuitas bisnis. Studi ini juga menyoroti pentingnya kolaborasi antara pelaku bisnis, konsumen, dan regulator dalam membangun ekosistem digital yang aman dan tangguh. Diharapkan, temuan ini dapat menjadi acuan bagi pelaku bisnis digital dalam merancang strategi keamanan siber yang adaptif dan berkelanjutan di era digital.

ABSTARCT

Digital transformation has brought significant changes to business operations, but at the same time, it has also increased exposure to increasingly sophisticated cybercrime threats. This study aims to analyze the role of cybersecurity in enhancing the resilience of digital businesses against cyberattacks. Using a literature review method, this research identifies various types of cybercrime threats commonly targeting digital businesses, such as phishing, malware, ransomware, and DDoS attacks, and examines prevention and mitigation strategies that can be implemented. The findings indicate that comprehensive cybersecurity implementation- including network, application, cloud, and information protection, supported by risk management policies and increased human resource awareness-plays a crucial role in safeguarding digital assets, maintaining customer trust, and ensuring business continuity. This study also highlights the importance of collaboration among business actors, consumers, and regulators in building a secure and resilient digital

ecosystem. It is expected that these findings can serve as a reference for digital business practitioners in designing adaptive and sustainable cybersecurity strategies in the digital era.

Corresponding Author:
Herlina Bernadecka Sidauruk
Universitas Negeri Medan
hsidauruk8@gmail.com

Latar Belakang

Perkembangan pesat transformasi digital pasca-pandemi Covid-19 telah mengubah lanskap bisnis global. Berbagai perusahaan, mulai dari *startup* hingga korporasi multinasional semakin bergantung terhadap teknologi digital untuk keberlangsungan operasional perusahaan. Di era *society 5.0 & industry 4.0*, transformasi digital yang meliputi adopsi komputasi awan (*Cloud Computing*), *big data analytics*, *Internet of Things* (IoT), dan *Artificial Intelligent* (AI) membuka peluang bagi perusahaan untuk meningkatkan efisiensi operasional, mempercepat inovasi produk, serta menjangkau pasar global dengan biaya lebih rendah. Melalui otomatisasi proses dan integrasi sistem, perusahaan mampu memangkas waktu produksi, mengoptimalkan rantai pasok, dan menyajikan layanan kepada pelanggan di berbagai zona waktu.

Dampak positif lain dari pemanfaatan teknologi adalah peningkatan kualitas pengambilan keputusan berbasis data (*data-driven decision making*). Dengan analisis data *real-time*, manajemen dapat melakukan prediksi tren pasar, mengidentifikasi preferensi konsumen, dan merancang strategi pemasaran yang lebih tepat sasaran. Selain itu, manfaat penggunaan teknologi pada perusahaan tidak hanya terbatas pada aspek internal, tetapi juga menyentuh aspek eksternal. Perusahaan dapat meningkatkan transparansi, memperkuat kolaborasi dengan mitra bisnis, serta membangun citra positif di mata pelanggan dan pemangku kepentingan. Dengan demikian, teknologi menjadi pendorong utama pertumbuhan dan keberlanjutan bisnis di era digital.

Namun, di balik berbagai manfaat yang dirasakan perusahaan dari penggunaan teknologi, terdapat konsekuensi serius berupa peningkatan risiko kejahatan siber (*Cybercrime*). Serangan siber seperti *phishing, ransomware, distributed denial-of- service* (DDoS), dan *supply chain attacks* kini menjadi ancaman yang semakin canggih. Data pelanggan, intelektual properti, dan infrastruktur kritis perusahaan bisa disusupi atau dienkripsi oleh pelaku jahat, menimbulkan kerugian finansial, kerusakan reputasi, bahkan gangguan kontinuitas bisnis.

Kondisi ini menegaskan bahwa inovasi teknologi tanpa pengelolaan risiko keamanan siber yang memadai justru dapat menjadi boomerang. Oleh karena itu, perusahaan perlu mengimplementasikan *cybersecurity* sebagai fondasi strategi bisnis digital mereka. *Cybersecurity* tidak hanya berkaitan dengan pemasangan alat keamanan (seperti *firewall,* sistem deteksi intrusi, dan enkripsi), melainkan juga melibatkan kebijakan manajemen risiko, kesadaran keamanan di kalangan karyawan, serta rencana respons insiden yang dilakukan. Dengan pendekatan ini, perusahaan dapat memperkuat ketahanan digital (*digital resilience*), yaitu kemampuan untuk mencegah, mendeteksi, merespons, dan pulih dari serangan siber (*cybercrime*) dengan cepat dan efektif.

Tinjauan Pustaka

Defenisi dan Konsep Dasar Cybersecurity dan Cybercrime

Cybersecurity adalah teknologi, proses dan praktik yang dirancang untuk melindungi jaringan, komputer, program dan data dari serangan, kerusakan atau akses yang tidak sah. *Cybersecurity* juga disebut sebagai upaya untuk melindungi informasi dari adanya *cyber attack* (Wibowo *et al.,*2023). Menurut NIST (*National Institute of Standard and Technology*), *cybersecurity* mencakup serangkaian teknologi, proses, dan kebijakan yang dirancang untuk mencegah, mendeteksi, dan merespons ancaman siber (NIST,2021). *Cybersecurity* bertujuan menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi digital agar sistem tetap aman dari berbagai ancaman siber. Selain itu, *cybersecurity* juga merupakan upaya perlindungan terhadap sistem komputer dari berbagai serangan atau akses ilegal yang dapat mengganggu keamanan data dan informasi pada jaringan.

Cybercrime merupakan perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana atau alat, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. *Cybercrime* dapat dikategorikan menjadi dua jenis utama, yaitu *cyber-dependent crime* yang hanya bisa terjadi di dunia maya (misalnya hacking) dan *cyber-enabled crime* yang merupakan kejahatan tradisional yang diperluas melalui teknologi digita (misalnya penipuan online). Konsep *cybercrime* berkembang seiring dengan digitalisasi bisnis, dimana pelaku kejahatan memanfaatkan kerentanan sistem untuk melakukan eksploitasi

Jenis-Jenis Ancaman *Cybercrime* yang Umum Menyerang Bisnis Digital

Bisnis digital menghadapi berbagai ancaman cybercrime yang dapat mengganggu operasional dan merugikan secara finansial. Beberapa jenis ancaman yang umum adalah :

1. Phishing : Teknik penipuan dengan mengelabui korban agar memberikan data pribadi atau kredensial melalui email atau situs palsu.
2. Malware : Perangkat lunak berbahaya seperti virus, worm, trojan, ransomware, spyware, yang dirancang untuk merusak, mencuri data, atau mengendalikan sistem korban.
3. *Distributed Denial of Service* (DDoS) : Serangan yang membanjiri server dengan trafik palsu sehingga layanan menjadi tidak tersedia bagi pengguna.
4. Pencurian Data : Pengambilan data penting perusahaan atau pegawai yang dapat digunakan untuk kepentingan ilegal atau persaingan tidak sehat.
5. Ransomware : Malware yang mengenkripsi data korban dan menuntut tebusan untuk mengembalikan akses.
6. *Insider Threats* : Ancaman dari dalam organisasi, baik disengaja, misalnya ada karyawan yang berniat buruk, atau tidak disengaja, biasanya disebabkan oleh kelalaian karyawan.

Jenis-Jenis *Cybersecurity* Dalam Bisnis Digital

Dalam konteks bisnis digital, *cybersecurity* tidak hanya sebatas perlindungan terhadap serangan, tetapi mencakup berbagai jenis keamanan yang fokus pada aspek berbeda dan sistem teknologi informasi. Berikut adalah jenis-jenis cybersecurity yang penting untuk melindungi bisnis digital :

1. Keamanan Jaringan (*Network Security*)

Keamanan jaringan bertujuan melindungi infrastruktur jaringan internal dari ancaman eksternal maupun internal, seperti penyusupan, malware, dan serangan *denial of service*. Teknologi yang umum digunakan meliputi firewall, antivirus, sistem deteksi dan pencegahan intrusi (IDS/IPS), serta enkripsi data yang dikirim melalui jaringan. Keamanan jaringan memastikan lalu lintas data tetap aman dan tidak disusupi oleh pihak yang berniat jahat.

2. Keamanan Aplikasi (*Application Security*)

Jenis ini fokus pada perlindungan aplikasi dari eksploitasi celah keamanan yang dapat dimanfaatkan oleh peretas. Upaya keamanan aplikasi meliputi pengkodean yang aman (*secure coding*), validasi input, penerapan enkripsi, serta pembaruan (patching) secara berkala untuk menutup kerentanan.

3. Keamanan Cloud (*Cloud Security*)

Jurnal Ilmu Ekonomi dan Bisnis
Vol. 3, No. 2, 2025, pp. 08-17

Dengan semakin banyaknya bisnis yang menggunakan layanan cloud, keamanan cloud menjadi krusial untuk melindungi data yang tersimpan dan diproses di lingkungan cloud. Cloud security mencakup kontrol akses berbasis peran, enkripsi data di cloud, pemantauan aktivitas, serta kebijakan keamanan yang ketat untuk mencegah akses tidak sah dan serangan siber terhadap layanan cloud.

4. Keamanan Informasi (*Information Security*)

Keamanan informasi berfokus kepada perlindungan data dan informasi penting agar tetap terjaga kerahasiaan, integritas, dan ketersediaannya. Metode yang digunakan termasuk enkripsi data, manajemen hak akses, kebijakan privasi, serta audit keamanan. Hal ini penting untuk mencegah kebocoran dan pencurian data yang dapat merugikan bisnis dan pelanggan.

5. Keamanan Identitas *(Identity Security*)

Keamanan identitas bertujuan memastikan hanya pengguna yang terverifikasi dan berwenang yang dapat mengakses sistem dan data bisnis. Teknologi yang digunakan meliputi otentikasi multi-faktor (MFA), *single sign-on* (SSO), manajemen identitas digital, dan kontrol akses berbasis peran.

6. Keamanan Operasional (*Operational Security*)

Operational security mencakup kebijakan, produser, dan pelatihan karyawan untuk menjaga keamanan informasi dan sistem. Fokusnya adalah pada pengelolaan risiko keamanan melalui kontrol akses, manajemen insiden, serta kesadaran keamanan siber di seluruh organisasi. Pendekatan ini memastikan bahwa aspek manusia dan proses juga terlindungi, bukan hanya teknologi.

7. Keamanan *Internet of Things* (*IoT Security*)

Dengan semakin banyaknya perangkat IoT yang terhubung dalam bisnis digital, keamanan IoT menjadi penting untuk melindungi perangkat tersebut dari eksploitasi kerentanan yang dapat membahayakan jaringan dan data. IoT security melibatkan enkripsi komunikasi perangkat, autentikasi perangkat, serta pemantauan aktivitas untuk mencegah serangan siber melalui perangkat IoT.

Teori dan Model Ketahanan Bisnis Digital (*Digital Resilience)*

Ketahanan bisnis digital (*digital resilience*) merupakan kemampuan organisasi untuk mengantisipasi, merespons, dan pulih dari berbagai gangguan digital, termasuk serangan siber, kegagalan teknologi, atau krisis lainnya, sembari mempertahankan operasi inti dan reputasi (World Economic Forum, 2021). Konsep ini berkembang seiring meningkatnya ketergantungan bisnis pada teknologi digital dan kompleksitas ancaman siber. Menurut Smith & Brooks (2023), ketahanan digital tidak hanya mencakup aspek teknis seperti keamanan sistem, tetapi juga elemen strategis seperti manajemen risiko, budaya organisasi, dan kelincahan operasional. Ketahanan organisasi (*organizational resilience*) dibangun melalui pendekatan holistik yang menggabungkan kepemimpinan, adaptasi, dan pembelajaran berkelanjutan.

Ketahanan bisnis digital adalah kemampuan perusahaan untuk bertahan dan pulih dari gangguan seperti serangan siber. Teori penting yang mendukung ini adalah *Resource-Based View* (RBV) yang menekankan pentingnya sumber daya internal seperti teknologi dan SDM, serta *Dynamic Capabilities* yang fokus pada kemampuan adaptasi dan inovasi. Model ketahanan melibatkan manajemen risiko digital, ketahanan operasional, inovasi adaptif, dan pemulihan. Siklusnya meliputi pencegahan, deteksi, respons, dan pemulihan. Keberhasilan bergantung pada kepemimpinan, regulasi, dan investasi teknologi. Intinya, ketahanan bisnis digital adalah tentang menggabungkan teknologi, sumber daya manusia, dan proses untuk menghadapi tantangan dan terus berkembang.

Metode Penelitian

Penelitian ini menggunakan metode analitik bersifat analisis deskriptif, yaitu data diurai secara teratur dari hasil yang diperoleh, lalu agar dapat dipahami dengan baik oleh pembaca maka diberikan pemahaman dan penjelasan. Penelitian ini menggunakan desain penelitian tinjauan pustaka atau *literature review* yang mencakup tahap pencarian, pengidentifikasian, pembacaan, pemahaman, pencatatan dan analisis terhadap informasi yang relevan dari literatur yang sudah teridentifikasi. *Literature review* merupakan suatu penelusuran dan penelitian kepustakaan dengan cara membaca dan menelaah berbagai jurnal, buku, dan berbagai naskah terbitan lainnya yang berkaitan dengan topik penelitian untuk menghasilkan sebuah tulisan yang berkenaan dengan suatu topik atau isu tertentu. Kata kunci yang digunakan adalah "*cybersecurity"*, "bisnis digital", "*cybercrime".* Artikel dan buku yang digunakan berkaitan langsung dengan judul penelitian yang dibawakan oleh penulis. Penelusuran artikel penelitian didapatkan dari yang dipublikasikan di internet melalui *Research Rabbit* dan *Google Scholar*.

Hasil dan Pembahasan

Peran Cybersecurity dalam Ketahanan Bisnis

A. Pencegahan (Prevention)

Cybersecurity memainkan peran sentral dalam melindungi bisnis digital dari ancaman *cybercrime* dengan menerapkan praktik dan teknologi yang berlapis untuk mengamankan perangkat, jaringan, aplikasi dan data kritis. Teknologi dasar seperti *firewall* dan sistem deteksi serta pencegahan intrusi (IDS/IPS) berfungsi sebagai garis pertahanan pertama, memblokir akses tidak sah dan memantau aktivitas mencurigakan secara *real time,* sementara enkripsi memastikan bahwa data yang tersimpan atau ditransmisikan tetap tidak dapat dibaca oleh pihak yang tidak berwenang. Selain itu, penerapan *threat intelligence* yaitu pengumpulan dan analisis informasi tentang taktik, teknik, dan prosedur penyerang memungkinkan organisasi merespons serangan yang sedang berlangsung atau potensi vektor baru secara proaktif sebelum kerugian terjadi. Namun, keamanan tidak hanya bergantung pada teknologi, faktor manusia sering kali menjadi titik lemah utama. Program pelatihan keamanan siber dan kampanye kesadaran (*security awareness*) mengajarkan karyawan mengenali taktik *social engineering*, seperti *phising* dan *pretexting*, sehingga mereka dapat menghindari jebakan penyerang dan melaporkan insiden yang mencurigakan sejak dini. Kebijakan manajemen risiko yang baik juga menjabarkan prosedur dan tanggung jawab jelas mulai dari pengolahan kata sandi hingga penggunaan perangkat pribadi untuk memperkecil peluang kesalahan manusia yang dapat dimanfaatkan penjahat siber.

Ketika insiden terjadi, kesiapan melalui rencana tanggap insiden (*Incident Respons Plan*) dan strategi pemulihan bencana (*Disaster Recovery Plan*) menjadi kunci menjaga kesinambungan bisnis. Rencana tersebut mencakup langkah-langkah struktural untuk deteksi cepat, isolasi zona terdampak, investigasi forensik, dan pemulihan layanan sehingga *downtime* dapat diminimalkan dan kerugian finansial ditekan. Latihan simulasi insiden secara berkala memastikan bahwa tim respons dapat bekerja efektif di bawah tekanan, mempercepat waktu pemulihan, dan memverifikasi keandalan prosedur.

B. Deteksi (Detection)

Deteksi merupakan tahapan yang paling penting dalam *cybersecurity,* berfungsi sebagai peringatan dini terhadap ancaman dan aktivitas tidak sah dalam sebuah sistem. Meskipun dalam sebuah organisasi mempunyai sistem pertahanan yang kuat selalu ada kemungkinan serangan dapat menembus pertahanan tersebut. Oleh karena itu, diperlukan mekanisme deteksi yang efektif, yang mampu mengidentifikasi insiden keamanan secara *real- time*. Mekanisme ini harus

Jurnal Ilmu Ekonomi dan Bisnis
Vol. 3, No. 2, 2025, pp. 08-17

memberikan peringatan segera kepada tim keamanan, sehingga mereka dapat merespons dengan cepat sebelum dampak dari ancaman tersebut menjadi lebih besar.

1. *Security Information and Event Management* (SIEM)

Security Information and Event Management (SIEM) adalah solusi keamanan terintegrasi yang menggabungkan manajemen informasi keamanan (SIM) dan manajemen kejadian keamanan (SEM) dalam satu sistem untuk membantu organisasi mendeteksi, menganalisis, dan merespons ancaman keamanan secara real-time sebelum mengganggu operasi bisnis. Komponen Utama SIEM :

a. Pengumpulan Data : Mengumpulkan log dan data keamanan dari berbagai sumber di seluruh infrastruktur TI.
b. Normalisasi dan Pemrosesan : Mengubah data mentah menjadi format standar yang konsisten untuk analisis.
c. Analisis dan Deteksi : Menggunakan teknik analitik untuk mengidentifikasi ancaman dan aktivitas abnormal.
d. Manajemen Kejadian : Memungkinkan tim keamanan merespons insiden dengan cepat, termasuk pemberian peringatan dan tindakan otomatis.
e. Pelaporan dan Pemantauan : Menyediakan laporan komprehensif dan pemantauan real-time untuk mendukung kepatuhan dan pengambilan keputusan.

Fungsi dan Manfaat SIEM:

a. Manajemen Log Terpusat : Menyederhanakan pengumpulan dan analisis data keamanan dari berbagai sumber dalam satu platform.
b. Korelasi Kejadian : Mengidentifikasi hubungan antar peristiwa untuk mendeteksi ancaman yang kompleks.
c. Pemantauan dan Respons Insiden : Memberikan visibilitas real-time dan peringatan dini sehingga tim keamanan dapat merespons dengan cepat.
d. Kepatuhan Regulasi : Membantu organisasi memenuhi persyaratan audit dan regulasi keamanan dengan otomatisasi pelaporan.
e. *Advanced Analytics* : Memanfaatkan kecerdasan buatan dan machine learning untuk meningkatkan akurasi deteksi ancaman dan mengurangi *false positive.*

2. *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS)

IDS dan IPS adalah dua jenis sistem yang dirancang untuk mendeteksi (dan dalam hal IPS, juga mencegah) aktivitas berbahaya dalam jaringan atau sistem computer.

a. IDS (*Intrusion Detecftion System*)

Intrusion Detection System (IDS) adalah sistem keamanan siber yang dirancang untuk mendeteksi aktivitas tidak sah, mencurigakan, atau berbahaya dalam jaringan atau sistem komputer. IDS tidak secara aktif menghentikan serangan, tetapi memberikan peringatan (*alert*) kepada administrator atau sistem keamanan agar mereka dapat segera menindaklanjuti. IDS berfungsi sebagai sistem pengawasan yang terus memantau lalu lintas data dan aktivitas sistem untuk mencari pola yang mengindikasikan adanya serangan seperti penyusupan (*intrusion*), eksploitasi kerentanan, akses tidak sah, aktivitas malware.

b. Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) adalah sistem keamanan jaringan yang berfungsi untuk mendeteksi, mengidentifikasi, dan secara otomatis mencegah ancaman siber sebelum dapat merusak sistem atau data yang dilindungi. IPS bekerja secara proaktif dengan memantau lalu lintas jaringan secara real-time, menganalisis paket data yang masuk dan keluar, serta mengambil tindakan pencegahan seperti memblokir lalu lintas berbahaya, menghentikan koneksi mencurigakan, atau mereset koneksi yang terinfeksi.

C. Response

Incident Response Plan adalah rangkaian kegiatan terstruktur yang dirancang untuk mendeteksi, menganalisis, dan memitigasi dampak kejahatan siber terhadap bisnis digital. Proses ini terdiri dari empat fase utama :

a. Persiapan (penyusunan kebijakan, pembentukan tim, dan pelatihan simulasi)
b. Deteksi dan Analisis (pemantauan real-time menggunakan SIEM, IDS/IPS, dan monitoring endpoint untuk mengidentifikasi anomali)
c. Kontainmen, Eradikasi, dan Pemulihan (isolasi sistem terdampak, pembersihan malware, dan restore data dari backup)
d. Kegiatan Pasca-Insiden (forensik, analisis akar masalah, dan perbaikan prosedur).

Setiap fase saling berkorelasi output dari tahapan sebelumnya menjadi input bagi tahap berikutnya sehingga organisasi dapat menyesuaikan respon dengan cepat dan mengurangi waktu henti operasional. Dengan menanamkan proses respon insiden yang matang dan teknologi canggih ke dalam kerangka kerja keamanan siber, bisnis digital dapat tidak hanya menanggulangi serangan saat terjadi, tetapi juga meningkatkan ketahanan jangka panjang terhadap ancaman masa depan.

D. Pemulihan (*Recovery*)

Setelah serangan siber atau insiden keamanan berhasil dideteksi dan direspons, tahapan selanjutnya yang tak kalah penting adalah pemulihan (*recovery*). Tahap ini bertujuan untuk mengembalikan sistem, data, dan operasional bisnis ke kondisi normal secepat dan seaman mungkin, sekaligus meminimalkan dampak jangka panjang. Pemulihan bukan hanya soal memperbaiki sistem yang rusak, tetapi juga melibatkan proses strategis yang melindungi integritas data dan menjamin kelangsungan operasional organisasi. Tiga komponen utama yang menyokong proses pemulihan adalah backup data, *disaster recovery plan* (DRP), dan *business continuity management* (BCM).

1. *Backup Data*

Backup data adalah proses mencadangkan salinan data penting ke lokasi atau media terpisah, sebagai bentuk perlindungan terhadap kehilangan data akibat serangan, kerusakan perangkat keras, bencana alam, atau kesalahan manusia.

Jenis-Jenis Backup

a. *Full Backup* : Salinan lengkap dari seluruh data sistem. Waktu dan kapasitas penyimpanan besar, tetapi sangat andal
b. Incremental Backup : Hanya mencadangkan data yang berubah sejak backup terakhir. Efisien secara ruang dan waktu, namun prose pemulihan bisa lebih kompleks.
c. *Diffrential Backup* : Mencadangkan semua perubahan sejak backup penuh terakhir. Menyediakan keseimbangan antara efisiensi dan kecepatan pemulihan.

2. *Disaster Recovery Plan* (DRP)

Disaster Recovery Plan (DRP) adalah dokumen terstruktur yang merinci langkah- langkah yang harus diambil organisasi untuk memulihkan dan melanjutkan operasional TI serta data penting setelah terjadi bencana, baik yang disebabkan oleh gangguan alam, kegagalan sistem, serangan siber, maupun kesalahan manusia. Tujuan utama DRP adalah meminimalkan waktu henti (*downtime*), melindungi data, dan memastikan kelangsungan bisnis dengan cara yang terencana dan terkoordinasi.

3. *Business Continuity Management* (BCM)

Business Continuity Management (BCM) adalah proses manajemen yang mengembangkan dan menerapkan strategi untuk meminimalkan gangguan operasional akibat berbagai risiko dan memastikan kelangsungan bisnis tetap berjalan meskipun terjadi bencana atau insiden yang mengganggu. BCM mencakup perencanaan, pengorganisasian, pelaksanaan, pengujian, dan pemeliharaan kebijakan dan prosedur yang memungkinkan organisasi untuk merespons dan pulih dari gangguan secara efektif.

Tantangan Implementasi Cyber Security dalam Bisnis Digital

Jurnal Ilmu Ekonomi dan Bisnis
Vol. 3, No. 2, 2025, pp. 08-17

Penting diketahui bahwa upaya memperkuat ketahanan bisnis digital terhadap kejahatan siber memerlukan komitmen holistik, mulai dari kebijakan, teknologi, hingga sumber daya manusia. Di lapangan, perusahaan seringkali menghadapi berbagai hambatan yang menghambat efektivitas proteksi, seperti keterbatasan anggaran, kekurangan tenaga ahli, serta ancaman yang semakin kompleks dan cepat berubah. Masing-masing tantangan ini tidak hanya menyulitkan implementasi solusi teknis, tetapi juga berpotensi melemahkan kesiapsiagaan dan respons insiden secara keseluruhan. Oleh karena itu, memahami konteks dan dampak dari setiap kendala merupakan langkah awal yang esensial sebelum merancang strategi keamanan siber yang adaptif dan berkelanjutan.

1. Budget Terbatas untuk Infrastruktur *Cybersecurity*

Banyak organisasi, khususnya UMKM dan perusahaan skala menengah, menghadapi tantangan yang signifikan terkait alokasi anggaran untuk infrastruktur keamanan siber. Pengadaan perangkat keras dan lunak keamanan, seperti *firewall* generasi terbaru, sistem deteksi dan pencegahan intrusi (IDS/IPS), *Security Information and Event Management* (SIEM), serta enkripsi tingkat lanjut memerlukan investasi awal yang besar, belum termasuk biaya lisensi berkala dan pembaruan perangkat. Ketika anggaran TI sudah tersita untuk kebutuhan operasional sehari-hari, prioritas alokasi dana ke *cybersecurity* kerap tertunda atau dikurangi, sehingga organisasi menjadi rentan terhadap vektor serangan yang terus berkembang.

Selain investasi pada teknologi, biaya pemeliharaan dan integrasi sistem keamanan juga menyerap sumber daya finansial. Misalnya, penerapan SIEM membutuhkan tidak hanya perangkat dan lisensi, tetapi juga infrastruktur server, kapasitas penyimpanan untuk log yang besar, dan bandwith untuk transfer data *real-time*. Jika organisasi tidak mampu menanggung beban infrastruktur ini, mereka mungkin hanya mengandalkan solusi parsial atau open-source yang kurang terkelola, sehingga efektivitas monitoring dan respon insiden menurun. Kondisi ini menciptakan kesenjangan antara kebutuhan proteksi ideal dan kemampuan riil organisasi, memperlebar attack surface akibat infrastruktur yang tidak memadai.

2. Kurangnya SDM Ahli di Bidang Keamanan Siber

Permintaan terhadap profesional keamanan siber terus meningkat seiring dengan bertambahnya insiden dan kompleksitas serangan, tetapi pasokan tenaga ahli belum mampu mengikuti. Banyak perusahaan kesulitan menemukan atau mempertahankan talenta seperti s*ecurity analysts, ethical hackers, dan incident responders*, yang memiliki kombinasi keterampilan teknis, sertifikasi (CISSP, CEH, atau CISM), dan pengalaman operasional. Akibatnya, tim TI sering kali harus menangani tugas keamanan siber di samping tanggung jawab lain, sehingga prioritas pencegahan dan monitoring menjadi terbagi dan kinerja turun.

Keterbatasan SDM ini juga berdampak pada efektivitas pelatihan dan transfer pengetahuan internal. Tanpa mentor atau *lead security* yang kompeten, program *upskilling* maupun *onboarding* praktisi baru cenderung minim struktur dan materi yang komprehensif. Ketika organisasi mengadopsi teknologi baru, misalnya platform cloud atau container orchestration, ketidaksiapan tim dalam memahami dan mengamankan lingkungan tersebut meningkatkan risiko kesalahan konfigurasi (*misconfiguration*), yang menjadi jalan masuk populer bagi peretas. Untuk menutupi kekurangan ini, banyak perusahaan harus mengandalkan layanan pihak ketiga (MDR, managed SOC), tetapi biaya berkelanjutan dari *outsourcing* juga dapat menekan anggaran.

3. Kompleksitas Ancaman yang Terus Berkembang

Salah satu tantangan paling mendasar dalam keamanan siber adalah evolusi ancaman yang cepat dan beragam, mulai dari serangan ransomware yang terautomasi, *advanced persistent threaths* (APT) yang menargetkan rantai pasok, hingga eksperimen awal serangan berbasis *quantum computing*. Teknologi kuantum menjanjikan kemampuan memecah enkripsi klasik (RSA, ECC) secara jauh lebih cepat melalui algoritma, sehingga sistem yang saat ini dianggap aman bisa menjadi rentan dalam satu dekade mendatang. Meskipun ancaman kuantum bersifat teoritis dan masih dalam tahap penelitian, perusahaan perlu mulai mempersiapkan migrasi ke kriptografi pasca-kuantum untuk menjaga keutuhan data jangka panjang.

Ciri-Ciri Keamanan Bisnis Digital Terserang Cybercrime

Berikut ini ciri-ciri keamanan bisnis digital yang terserang *cybercrime* :

a. Kinerja Sistem Menurun Tiba-tiba
   Sistem yang tiba-tiba lambat, sering hang, atau crash bisa jadi akibat aktivitas mencurigakan seperti malware yang berjalan di latar belakang, botnet, atau penyusup yang sedang menyalin data. Ini biasanya terjadi ketika sumber daya sistem seperti RAM dan CPU digunakan tanpa alasan yang jelas. Contoh: Website e-commerce jadi sangat lambat padahal tidak banyak pengunjung.
b. Adanya Aktivitas yang Tidak Wajar
   Aktivitas seperti login di waktu tidak biasa, dari lokasi asing (misalnya negara lain), atau percobaan login berulang bisa menandakan percobaan peretasan atau akun sudah diretas. Perubahan pengaturan sistem atau file oleh pengguna yang tidak dikenal juga termasuk gejala umum. Contoh : Akun admin login dari IP Rusia padahal seluruh tim berada di Indonesia
c. Kehilangan atau Kebocoran Data
   Data penting tiba-tiba hilang, rusak, atau diakses oleh pihak luar bisa jadi akibat pencurian data (data breach). Ransomware juga sering menyebabkan file terenkripsi dan tidak bisa diakses tanpa membayar tebusan. Contoh: File laporan keuangan tidak bisa dibuka dan muncul pesan meminta pembayaran tebusan.
d. Lalu Lintas Jaringan Tidak Biasa
   Jika ada lonjakan *traffic* jaringan tanpa peningkatan aktivitas bisnis, bisa jadi server anda diserang (misalnya DDoS attack) atau sedang mengirim data keluar secara diam-diam. *Tools* pemantau jaringan biasanya bisa mendeteksi pola aneh ini. Server kecil tiba-tiba mengirim data besar ke IP luar negeri di jam malam.
e. Perubahan Tampilan Website atau Aplikasi
   Website bisa di-*deface* (dihancurkan tampilannya) oleh hacker untuk menunjukkan keberhasilan serangan mereka atau menyebarkan propaganda. Atau pengguna dialihkan ke situs lain berbahaya. Contoh : *Homepage* website berubah menjadi halaman bertuliskan “Hacked by XYZ”.
f. Email *Phising* atau Malware Meningkat
   Banyak karyawan menerima email yang berisi link mencurigakan, file terinfeksi, atau permintaan informasi sensitif. Ini bisa jadi bagian dari upaya penyusupan awal melalui rekayasa sosial. Contoh : Email dari “CEO” meminta login ke sistem keuangan melalui link palsu.
g. Antivirus atau Keamanan Nonaktif
   Malware tingkat lanjut sering menonaktifkan antivirus, firewall, atau sistem keamanan lainnya agar lebih mudah menyebar. Jika proteksi hilang tanpa disengaja oleh user, itu tanda bahaya serius. Contoh : Antivirus mati dan tidak bisa dinyalakan kembali.

Kesimpulan

Berdasarkan hasil analisis, dapat disimpulkan bahwa peran *cybersecurity* sangat krusial dalam meningkatkan ketahanan bisnis digital terhadap ancaman *cybercrime* yang semakin kompleks dan dinamis. Implementasi *cybersecurity* yang komprehensif, meliputi perlindungan jaringan, aplikasi, cloud, informasi, identitas, serta operasional, mampu meminimalisir risiko serangan siber seperti *phishing*, *malware*, *ransomware*, dan DDoS yang dapat mengakibatkan kerugian finansial, kerusakan reputasi, serta gangguan operasional bisnis. Selain aspek teknologi, penguatan kebijakan manajemen risiko, pelatihan keamanan siber bagi karyawan, serta kesiapan rencana tanggap insiden menjadi faktor kunci dalam membangun digital resilience, yaitu kemampuan organisasi untuk mencegah, mendeteksi, merespons, dan pulih dari serangan siber secara efektif.

Penelitian ini juga menegaskan pentingnya pendekatan holistik dalam pengelolaan risiko *cybercrime*, di mana sinergi antara teknologi, sumber daya manusia, dan proses bisnis harus berjalan seimbang. Dengan memahami dan mengelola risiko *cybercrime* secara terstruktur, bisnis digital dapat melindungi aset penting seperti data pelanggan dan informasi keuangan, menjaga kepercayaan pelanggan, serta memastikan kelangsungan operasional di tengah lanskap

ancaman siber yang terus berkembang. Namun, keterbatasan penelitian ini terletak pada ruang lingkup yang masih sebatas elaborasi literatur, sehingga diperlukan riset lanjutan untuk mengembangkan solusi praktis dan strategi adaptif dalam menghadapi tantangan *cybercrime* di masa depan.

Daftar Pustaka

Aska, M. F., Putra, D. P., & Sinambela, C. J. M. (2024). Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital. *Journal of Informatic and Information Security*, *5*(2), 187-200.

Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile: Studi literatur mengenai cybercrime dan mitigasinya. *Akuntansi Dan Teknologi Informasi*, *17*(2), 221-237.

Balafif, S. (2023). Penyesuaian Model Ketahanan Siber Umkm Di Indonesia Dengan Nist Cybersecurity Framework. Jurnal Informatika: Jurnal Pengembangan IT (JPIT). Vol. 8

Irfan, M., Elvia, M., & Dania, S. (2023). Ancaman Cybercrime dan Peran Cybersecurity pada E-commerce: Systematic Literature Review. *Jursima*, *11*(1), 110-121.

Napu, I. A., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis Peran Keamanan Siber dan Keterampilan Digital dalam Pertumbuhan Usaha Kecil Menengah di Era Ekonomi Digital di Indonesia. *Sanskara Ekonomi Dan Kewirausahaan*, *2*(03), 156-167.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSW 29). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Ramadian, A., Fitriyani, A., & Novita, N. N. S. (2024). Mengukur dan Mengelola Risiko Cybercrime dalam E-Commerce: Peran Strategis Cybersecurity untuk Keamanan Informasi dan Perlindungan Data. *JURNAL ILMIAH EDUNOMIKA*, *8*(2).

Samudra, Y., Hidayat, A., & Wahyu, M. F. (2023). Pengenalan Cyber Security Sebagai Fundamental Keamanan Data Pada Era Digital. *AMMA: Jurnal Pengabdian Masyarakat*, *1*(12), 1594-1601.

Suartana, I. M., Putra, R. E., Bisma, R., & Prapanca, A. (2022). Pengenalan pentingnya cyber security awareness pada umkm. *Jurnal Abadimas Adi Buana*, *5*(02), 197-204.

Susanto, E., Antira, L., Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber Di Era Digital. *Journal of Business And Entrepreneurship*, *11*(1), 23-33.

Wibowo, K., Hidayat, U., & Yasin, V. (2023). Kajian Cyber Security Dalam Rangka Koperasi Menghadapi Revolusi Industri 4.0. *Journal of Information System, Applied, Management, Accounting and Research*, *7*(3), 634-645.

World Economic Forum. (2021). *Digital resilience: Building the economies of tomorrow on a foundation of cybersecurity*. https://www.weforum.org/stories/2022/05/digital- resilience-building-the-economies-of-tomorrow-on-a-foundation-of-cybersecurity