Jurnal Cendekia Hukum Indonesia (JCHI)
Vol. 2 No. 2 Oktober 2026
Licenced CC BY-SA, E-ISSN: 3064-2264 , Hal 64-72
DOI: https://doi.org/10.71417/jchi.v2i2.215
https://hukum.journalpustakacendekia.com/index.php/JCHI

Tata Kelola Keamanan Siber di Perusahaan Swasta Indonesia: Studi Kasus PT Bawi Kameloh Sukses Mandiri

Sinta Yunira[1], Miftahul Ulum[2]

[12]Ilmu Politik, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Muhammadiyah Jakarta

Alamat Universitas : Jl. K.H. Ahmad Dahlan, Cireundeu, Kec. Ciputat Timur, Kota Tangerang Selatan, Banten 15419.
E-mail Seluruh Penulis: sintayunira2@gmail.com, miftahul.ulum@umj.ac.id

Abstrak
Penelitian ini membahas tata kelola keamanan siber di perusahan swasta Indonesia, dengan fokus pada PT Bawi Kameloh Sukses Mandiri. Keamanan siber menjadi krusial dalam operasional administrasi perusahaan, khususnya yang berkaitan dengan surat-menyurat, laporan stok dan keuangan, serta dokumen ekspor-impor. Penelitian ini bertujuan untuk menganalisis implementasi kebijakan keamanan siber, praktik operasional, serta pemahaman dan kesadaran manajemen puncak dalam menjaga keamanan data perusahaan. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan pendekatan studi kasus. Data dikumpulkan melalui wawancara mendalam dengan jajaran manajemen dan puncak, serta analisis dokumen internal perusahaan. Analisis menggunakan teori Cyber Security Governance, dengan memperhatikan praktik keamanan siber berdasarkan regulasi nasional dan standar internasional, seperti ISO 27001. Hasil penelitian menunjukkan bahwa PT Bawi Kameloh Sukses Mandiri telah menerapkan berbagai praktik keamanan siber, termasuk prosedur akses data, enkripsi dokumen, dan pelatihan kesadaran siber untuk manajemen. Namun, tantangan signifikan tetap ada, seperti keterbatasan infrastruktur, ketergantungan pada sistem digital pihak ketiga, dan variasi pemahaman antar unit terkait protokol keamanan. Penelitian ini menyimpulkan bahwa keberhasilan tata kelola keamanan siber sangat bergantung pada integrasi kebijakann formal, pelatihan rutin, dan pemantauan berkelanjutan, sehingga perusahaan dapat meminimalkan risiko kebocoran data dan gangguan operasional.

Kata Kunci: Administrasi Ekspor-Impor, Cyber Security Governance, Keamanan Siber, Perusahaan Swasta Indonesia, Tata Kelola

Abstract
This study discusses cybersecurity governance in Indonesian private companies, with a focus on PT Bawi Kameloh Sukses Mandiri. Cybersecurity is crucial in the company's administrative operations, especially related to correspondence, stock and financial reports, and export-import documents. This research aims to analyze the implementation of cybersecurity policies, operational practices, and the understanding and awareness of top management in maintaining the security of company data. The research method used is qualitative descriptive with a case study approach. Data was collected through in-depth interviews with management and top brass, as well as analysis of internal company documents. The analysis uses the theory of Cyber Security Governance, paying attention to cybersecurity practices based on national regulations and international standards, such as ISO 27001. The results of the study show that PT Bawi Kameloh Sukses Mandiri has implemented various cybersecurity practices, including data access procedures, document encryption, and cyber awareness training for management. However, significant challenges remain, such as limited infrastructure, reliance on third-party digital systems, and variations in understanding between units regarding security protocols. The study concludes that the success of cybersecurity governance relies heavily on the integration of formal policies, regular training, and continuous monitoring, so that companies can minimize the risk of data leaks and operational disruptions.

Keywords*: Governance, Cybersecurity, Cyber Security Governance, Export-Import Administration, Indonesian Private Companies.*

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah menciptakan transformasi digital yang mengubah hubungan internasional, ekonomi, dan keamanan global. Ruang siber kini menjadi arena baru perebutan kekuasaan karena sifatnya yang lintas batas, saling terhubung, dan melibatkan

Received: April 10, 2026; Revised: April 13, 2026; Accepted: April 15, 2026
* Sinta Yunira, sintayunira2@gmail.com

aktor negara maupun non-negara. Keamanan siber tidak lagi dipandang sekadar persoalan teknis, melainkan isu strategis yang berkaitan dengan keamanan nasional, ketahanan ekonomi, dan stabilitas politik. NATO bahkan menempatkan ruang siber sebagai domain operasional setara dengan darat, laut, udara, dan antariksa, sementara negara-negara besar seperti Amerika Serikat, Rusia, dan Cina menjadikan ruang siber sebagai medan kompetisi geopolitik melalui pengembangan kemampuan ofensif dan defensif digital, termasuk serangan siber tingkat lanjut yang menargetkan pemerintah maupun perusahaan swasta. Fenomena ini memperlihatkan bahwa keamanan siber telah menjadi bagian penting dari dinamika hubungan internasional kontemporer dan strategi pertahanan negara (Nye, 2017; Singer & Friedman, 2014; Klimburg, 2017).

Dalam konteks tersebut, sektor swasta memiliki posisi yang sangat penting sekaligus rentan dalam ekosistem keamanan siber global. Perusahaan yang terhubung dengan perdagangan internasional menyimpan aset digital bernilai tinggi seperti data pelanggan, dokumen kontrak, hingga informasi logistik, sehingga menjadi sasaran utama kejahatan siber dan spionase ekonomi. Menurut laporan World Economic Forum, serangan siber terhadap sektor bisnis global meningkat seiring percepatan digitalisasi dan integrasi rantai pasok internasional (WEF, 2023). Gangguan terhadap sistem perusahaan dapat memicu dampak luas terhadap stabilitas pasar, kepercayaan investor, dan ketahanan ekonomi negara. Oleh karena itu, tata kelola keamanan siber perusahaan harus dipahami tidak hanya sebagai kebutuhan bisnis untuk melindungi aset dan operasional, tetapi juga sebagai kontribusi terhadap keamanan nasional dan ketahanan kolektif suatu negara. Pendekatan ini sejalan dengan konsep cybersecurity governance yang menekankan kolaborasi antara negara, sektor swasta, dan masyarakat sipil dalam menjaga stabilitas ruang siber (DeNardis, 2014; Dunn Cavelty, 2018).

Di Indonesia, transformasi digital dan integrasi ekonomi global meningkatkan risiko keamanan siber terhadap perusahaan nasional, baik BUMN maupun swasta. Literatur yang ada menunjukkan bahwa kajian keamanan siber di Indonesia lebih banyak berfokus pada regulasi, kelembagaan, dan sektor publik, seperti implementasi Undang-Undang Perlindungan Data Pribadi, peran Kementerian Komunikasi dan Informatika Republik Indonesia dan Badan Siber dan Sandi Negara, serta tantangan tata kelola digital nasional. Penelitian sebelumnya juga menyoroti rendahnya literasi digital, lemahnya pengawasan keamanan data, tingginya kasus kebocoran data, dan pentingnya kerja sama regional ASEAN dalam menghadapi ancaman siber lintas negara (Limba et al., 2019; Nugraha & Syarif, 2020). Namun demikian, sebagian besar kajian masih memandang sektor swasta hanya sebagai pihak yang diatur atau korban serangan siber, bukan sebagai aktor strategis dalam arsitektur keamanan nasional dan diplomasi ekonomi digital Indonesia.

Berdasarkan kondisi tersebut, penelitian ini mengidentifikasi tiga celah utama, yaitu kurangnya perspektif hubungan internasional dalam kajian keamanan siber korporat, dominasi fokus penelitian pada sektor publik, serta minimnya penelitian pada sektor agribisnis dan perdagangan komoditas sebagai bagian dari infrastruktur kritis digital. Penelitian ini menawarkan kebaruan dengan mengintegrasikan konsep cybersecurity governance dan hubungan internasional dalam analisis tata kelola keamanan siber perusahaan swasta nasional, khususnya pada sektor agribisnis yang memiliki keterkaitan erat dengan rantai perdagangan internasional. Selain itu, penelitian ini juga menekankan implikasi kebijakan berupa penguatan kerja sama publik-swasta, diplomasi digital, dan perlindungan infrastruktur ekonomi strategis nasional. Dengan demikian, penelitian ini diharapkan mampu menjadi jembatan antara kepentingan akademik, praktik korporasi, dan kebijakan keamanan nasional di era transformasi digital.

Urgensi penelitian ini semakin meningkat seiring tingginya ketergantungan perusahaan Indonesia terhadap sistem digital dalam aktivitas ekspor-impor, logistik, dan perdagangan global. Serangan siber terhadap perusahaan tidak hanya menimbulkan kerugian ekonomi, tetapi juga berpotensi mengganggu stabilitas rantai pasok nasional dan reputasi Indonesia dalam perdagangan internasional. Di sisi lain, sektor agribisnis sebagai salah satu penopang ekonomi nasional masih relatif jarang dikaji dalam perspektif keamanan siber dan hubungan internasional. Oleh karena itu, penelitian ini penting dilakukan untuk menghasilkan pemahaman yang lebih komprehensif mengenai peran sektor swasta dalam ketahanan siber nasional sekaligus memberikan rekomendasi kebijakan yang relevan bagi penguatan tata kelola keamanan siber perusahaan di Indonesia.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan jenis studi kasus instrumental tunggal untuk memahami secara mendalam praktik tata kelola keamanan siber di PT Bawi Kameloh Sukses Mandiri sebagai perusahaan swasta nasional di sektor agribisnis dan perdagangan internasional yang telah terdigitalisasi dan terhubung dengan rantai pasok global. Penelitian berlandaskan paradigma konstruktivis-interpretif yang memandang keamanan siber sebagai fenomena sosial yang dibentuk melalui pengalaman, persepsi, dan interaksi para aktor perusahaan. Pengumpulan data dilakukan melalui triangulasi metode berupa wawancara mendalam semi-terstruktur dengan lima informan kunci, observasi partisipatif oleh peneliti sebagai Admin Officer dan Personal Assistant Direktur Utama, serta studi dokumen internal dan eksternal perusahaan. Data dianalisis menggunakan model Miles, Huberman, dan Saldaña melalui proses reduksi data, penyajian data, dan penarikan kesimpulan dengan bantuan perangkat lunak NVivo 12. Keabsahan data dijaga melalui triangulasi sumber dan metode, member checking, prolonged engagement, observasi tekun, audit trail, dan refleksivitas peneliti, sedangkan aspek etika diterapkan melalui informed consent, perlindungan kerahasiaan informan dan perusahaan, prinsip non-maleficence, serta transparansi terkait posisi ganda peneliti sebagai bagian dari perusahaan dan peneliti akademik.

HASIL DAN PEMBAHASAN

Profil Perusahaan dan Posisinya dalam Konteks Eksternal

PT Bawi Kameloh Sukses Mandiri merupakan perusahaan swasta nasional yang bergerak di bidang agribisnis, perdagangan komoditas, serta ekspor-impor dan berlokasi di Kawasan Industri Manis, Kabupaten Tangerang, Banten. Perusahaan ini menjalankan aktivitas perdagangan produk pertanian, perikanan, rempah-rempah, dan minyak goreng berbasis kelapa sawit dengan melibatkan berbagai mitra dalam dan luar negeri sehingga menjadi bagian dari rantai pasok global. Struktur organisasi perusahaan terdiri dari Direktur Utama, unit manajemen, keuangan, logistik, dan administrasi ekspor-impor yang mengelola berbagai dokumen digital strategis seperti FCO, LOI, LOA, MoU, PO, DO, dan invoice yang berisi informasi penting terkait transaksi bisnis dan mitra dagang.

Dalam operasionalnya, perusahaan sangat bergantung pada sistem administrasi digital dan komunikasi daring untuk mempercepat transaksi dan koordinasi bisnis internasional. Pertukaran dokumen dengan mitra asing dilakukan melalui email, aplikasi pesan instan, dan platform cloud untuk mendukung efisiensi dan kecepatan komunikasi. Namun, ketergantungan pada teknologi digital, penggunaan perangkat pribadi tanpa kebijakan keamanan yang jelas, serta penyimpanan data yang terdesentralisasi meningkatkan risiko keamanan siber dan memperluas permukaan serangan perusahaan. Praktik ini menunjukkan bahwa efisiensi digital perusahaan belum sepenuhnya diimbangi dengan infrastruktur tata kelola keamanan data yang memadai.

Hasil penelitian juga menunjukkan bahwa pemahaman perusahaan terhadap regulasi keamanan siber nasional, seperti UU Perlindungan Data Pribadi (UU PDP), masih bersifat umum dan belum diterapkan dalam bentuk SOP khusus. Pengetahuan mengenai lembaga seperti Badan Siber dan Sandi Negara (BSSN) juga masih terbatas sehingga regulasi lebih dipandang sebagai kewajiban administratif daripada strategi ketahanan digital. Kondisi tersebut memperlihatkan adanya kesenjangan antara kebijakan keamanan siber nasional dan praktik operasional perusahaan. Oleh karena itu, PT Bawi Kameloh Sukses Mandiri menjadi studi kasus yang relevan untuk menganalisis tata kelola keamanan siber sektor swasta Indonesia dalam perspektif keamanan non-tradisional dan tata kelola digital di era globalisasi.

Penerapan Tata Kelola Keamanan Siber: Temuan Pada Tiga Pilar

Analisis penerapan tata kelola keamanan siber di PT Bawi Kameloh Sukses Mandiri menunjukkan adanya ketimpangan dalam tiga pilar utama Cybersecurity Governance.

a) Pilar Tata Kelola (Governance):

Perusahaan belum memiliki kebijakan formal terkait keamanan siber seperti cybersecurity policy atau data protection standard. Pengelolaan keamanan data masih bergantung pada kesadaran individu dan keputusan manajemen yang bersifat sentralistik serta reaktif ketika terjadi insiden. Tidak terdapat unit atau jabatan khusus keamanan siber, sementara tanggung jawab teknis dibebankan kepada staf administratif tanpa pelatihan khusus. Selain itu, belum ada alokasi anggaran rutin untuk penguatan keamanan siber sehingga investasi keamanan dilakukan secara insidental.

b) Pilar Manajemen Risiko (Risk Management):

Proses identifikasi risiko dilakukan secara reaktif berdasarkan pengalaman individu tanpa adanya risk assessment berkala, klasifikasi data, atau pemetaan aset digital strategis. Risiko yang dipahami hanya terbatas pada ancaman umum seperti phishing dan malware, sedangkan ancaman yang lebih kompleks seperti ransomware, APTs, dan espionase ekonomi belum menjadi perhatian utama perusahaan.

c) Pilar Program Operasional (Operational Program):

Praktik keamanan siber di tingkat operasional masih didominasi oleh pola kerja informal dan lemahnya kontrol teknis dasar. Penggunaan autentikasi dua faktor, enkripsi data, serta sistem backup belum diterapkan secara optimal. Selain itu, penggunaan aplikasi pesan instan seperti WhatsApp dan Telegram untuk berbagi dokumen bisnis menjadi praktik umum karena dianggap lebih efisien. Perusahaan juga belum memiliki pelatihan keamanan siber yang terstruktur maupun prosedur tanggap insiden yang jelas, sehingga respons terhadap ancaman sangat bergantung pada keputusan individu. Pengaturan akses data antar divisi pun masih longgar tanpa pembatasan berbasis peran, yang semakin meningkatkan potensi risiko kebocoran dan penyalahgunaan data perusahaan.

Outcome dan Kerentanan yang Teramati: Sebuah Potret Ketahanan yang Rapuh

Hasil sintesis terhadap tiga pilar tata kelola keamanan siber menunjukkan bahwa PT Bawi Kameloh Sukses Mandiri memiliki tingkat ketahanan siber yang masih sangat rendah dan rapuh. Perusahaan belum memiliki kesiapan yang memadai dalam aspek pencegahan, deteksi, respons, maupun pemulihan terhadap ancaman siber. Ketiadaan kebijakan formal, minimnya kontrol teknis, tidak adanya sistem monitoring, serta lemahnya prosedur backup dan tanggap insiden menyebabkan perusahaan sangat bergantung pada kewaspadaan individu karyawan. Kondisi ini membuat perusahaan rentan terhadap berbagai ancaman, mulai dari phishing, kebocoran data, hingga potensi serangan yang lebih kompleks seperti pencurian data strategis dan gangguan operasional sistem digital.

a) Kapabilitas Ketahanan (Resilience) yang Teramati:

Kapabilitas keamanan siber perusahaan berada pada level rendah di seluruh aspek prepare, prevent, detect, respond, dan recover. Perusahaan belum memiliki perencanaan strategis, anggaran khusus, maupun pelatihan keamanan siber yang memadai. Deteksi ancaman hanya bergantung pada kesadaran individu tanpa dukungan sistem monitoring, sementara respons dan pemulihan insiden masih bersifat ad hoc tanpa prosedur yang jelas.

b) Kerentanan Data Strategis dan Rantai Pasok:

Dokumen penting perusahaan seperti FCO, LOI, kontrak, dan data mitra bisnis masih disimpan dan dikirim melalui media yang tidak aman seperti email pribadi, aplikasi chat, dan perangkat personal tanpa enkripsi. Selain itu, penggunaan kanal komunikasi publik untuk berinteraksi dengan mitra bisnis dan pihak logistik memperluas permukaan serangan dan meningkatkan risiko kebocoran data serta serangan dari pihak ketiga.

c) Kerentanan Budaya Organisasi:

Budaya kerja perusahaan lebih mengandalkan kepercayaan antarindividu dan kesadaran personal dibandingkan kontrol sistematis. Kondisi ini menciptakan risiko tinggi karena kelalaian atau tindakan individu dapat berdampak besar terhadap keamanan perusahaan. Budaya informal tersebut juga mendorong penggunaan perangkat dan komunikasi yang tidak aman sehingga memperkuat kerentanan keamanan siber secara keseluruhan.

Pembahasan

Membaca Celah Tata Kelola: Antara Teknis, Manajerial, dan Strategis

Temuan empiris di PT Bawi Kameloh Sukses Mandiri menyingkap suatu realitas yang lebih dalam dari sekadar "belum memiliki SOP keamanan siber". Realitas tersebut adalah fragmentasi dan disintegrasi total dari sistem tata kelola keamanan siber yang ideal, yang justru mengungkap kelemahan struktural dalam cara perusahaan merespons lingkungan digital yang semakin kompleks dan mengancam. Pembahasan ini akan menautkan keruntuhan hierarkis tersebut dengan kerangka teori dan literatur yang ada, menunjukkan bahwa kondisi ini bukanlah kelainan, melainkan konsekuensi logis dari dinamika ekonomi-politik perusahaan menengah di negara berkembang.

a. Governance yang Absen:

Temuan penelitian menunjukkan bahwa lemahnya tata kelola keamanan siber di PT Bawi Kameloh Sukses Mandiri bukan disebabkan oleh ketidakpedulian manajemen, melainkan adanya kesenjangan prioritas antara kebutuhan bisnis dan keamanan digital. Direksi lebih memfokuskan sumber daya pada

pertumbuhan pasar, kontrak bisnis, dan stabilitas keuangan karena memberikan keuntungan yang lebih nyata dibandingkan investasi keamanan siber yang hasilnya sulit diukur. Selain itu, perusahaan memilih tata kelola berbasis kepercayaan dan respons ad hoc karena dianggap lebih murah dibandingkan membangun sistem keamanan formal yang memerlukan biaya besar untuk kebijakan, teknologi, dan tenaga ahli.

b. Risk Management yang Tumpul:

Ketiadaan tata kelola formal menyebabkan manajemen risiko keamanan siber tidak berjalan secara sistematis. Perusahaan hanya mampu mengenali ancaman umum seperti phishing dan virus karena ancaman tersebut sudah dikenal secara luas, sementara ancaman yang lebih kompleks seperti supply chain attack, pencurian data strategis, dan manipulasi informasi pasar tidak teridentifikasi. Kondisi ini terjadi karena perusahaan tidak memiliki kapasitas threat intelligence maupun proses risk assessment yang memadai sehingga gagal memandang keamanan siber sebagai risiko bisnis strategis.

c. Operational Program yang Kacau:

Pada tingkat operasional, kebutuhan bisnis yang menuntut kecepatan dan fleksibilitas membuat karyawan lebih memilih menggunakan aplikasi seperti WhatsApp dan perangkat pribadi untuk aktivitas bisnis. Praktik shadow IT dan BYOD muncul sebagai solusi informal akibat tidak adanya kebijakan resmi yang mampu mengakomodasi kebutuhan kerja secara aman. Akibatnya, keamanan siber dipandang sebagai hambatan operasional, bukan bagian dari sistem kerja, sehingga berbagai praktik informal justru meningkatkan kerentanan perusahaan terhadap kebocoran dan penyalahgunaan data.

d. Implikasi:

Ketiga kondisi tersebut membentuk siklus ketidaktahanan siber yang terus berulang. Tidak adanya governance menyebabkan manajemen risiko tidak berjalan, sehingga ancaman strategis tidak teridentifikasi dan operasional berjalan tanpa kontrol yang memadai. Kerentanan operasional kemudian memunculkan insiden-insiden kecil yang justru memperkuat persepsi manajemen bahwa ancaman siber hanyalah gangguan teknis biasa, bukan risiko strategis. Siklus ini membuat perusahaan terjebak dalam kondisi ketahanan siber yang lemah dan menunjukkan bahwa akar permasalahan terletak pada kegagalan organisasi dalam memandang keamanan siber sebagai bagian penting dari tata kelola korporasi dan stabilitas bisnis jangka panjang.

Mengungkap Titik Buta Geopolitik dalam Persepsi Risiko Perusahaan

Temuan bahwa PT Bawi Kameloh Sukses Mandiri hanya mengenali ancaman siber konvensional (seperti phishing dan malware) sementara mengabaikan ancaman yang lebih kompleks dan strategis, bukanlah sekadar kesenjangan pengetahuan. Ini adalah symptom dari sebuah paradigma yang telah kedaluwarsa paradigma yang memisahkan secara ketat dunia bisnis dari dunia politik dan keamanan strategis. Pembahasan ini akan membongkar akar dari titik buta (blind spot) tersebut dan menganalisis implikasinya yang jauh lebih berbahaya daripada sekadar risiko keuangan langsung.

a. Dekonstruksi Paradigma “Bisnis adalah Bisnis”:

Temuan penelitian menunjukkan bahwa PT Bawi Kameloh Sukses Mandiri masih memandang aktivitas bisnis sebagai kegiatan yang murni komersial dan terpisah dari aspek politik serta keamanan strategis. Perusahaan lebih memahami ancaman terhadap aset fisik dibandingkan ancaman terhadap data digital yang bersifat lintas negara dan sulit terlihat. Akibatnya, perusahaan belum memiliki kesadaran bahwa data perdagangan, kontrak, dan logistik dapat menjadi sasaran espionase ekonomi atau kepentingan geopolitik negara lain. Kondisi ini menunjukkan kegagalan securitization di tingkat korporat karena ancaman siber belum dipahami sebagai ancaman eksistensial terhadap bisnis dan ketahanan ekonomi.

b. Analisis Komparatif Ancaman:

Perusahaan hanya mengenali ancaman siber konvensional seperti phishing, malware, dan ransomware yang memiliki dampak langsung dan mudah terlihat. Sementara itu, ancaman strategis seperti Advanced Persistent Threats (APT), espionase ekonomi, dan serangan rantai pasok tidak masuk dalam radar keamanan perusahaan. Padahal, ancaman geopolitik memiliki karakteristik yang lebih tersembunyi, terorganisasi, dan didukung sumber daya besar sehingga sulit dideteksi tanpa sistem monitoring dan threat intelligence yang memadai. Dengan kondisi keamanan yang lemah, seperti tidak adanya monitoring, kontrol akses longgar, dan penyebaran data yang tidak terkontrol, perusahaan justru menjadi target yang sangat rentan bagi serangan strategis tersebut.

c. Implikasi Berjenjang:

Titik buta geopolitik perusahaan tidak hanya berdampak pada level korporat, tetapi juga dapat meluas ke tingkat sektoral dan nasional. Pada level perusahaan, pencurian data strategis seperti harga kontrak

dan jaringan buyer dapat menghancurkan keunggulan kompetitif bisnis. Pada level sektoral, kerentanan serupa pada perusahaan agribisnis lain dapat memicu gangguan sistematis terhadap rantai pasok dan perdagangan komoditas Indonesia. Sementara pada level nasional, data yang bocor dapat dimanfaatkan oleh aktor negara lain untuk kepentingan ekonomi dan politik, seperti menekan posisi Indonesia dalam diplomasi perdagangan atau merusak reputasi produk Indonesia di pasar global. Oleh karena itu, penelitian ini menegaskan bahwa keamanan siber sektor swasta harus dipahami sebagai isu keamanan non-tradisional yang berkaitan erat dengan politik internasional dan ketahanan ekonomi nasional.

Perusahaan Swasta sebagai Weak Link dalam Infrastruktur Kritis Nasional: Sebuah Analisis Politik

Temuan yang menggambarkan praktik tata kelola yang rapuh di PT Bawi Kameloh Sukses Mandiri harus dibaca melampaui konteks korporatnya semata. Perusahaan ini, dalam posisinya sebagai simpul perdagangan komoditas strategis, tidak beroperasi dalam ruang hampa. Ia adalah bagian dari suatu infrastruktur ekonomi nasional yang vital. Dengan demikian, kerentanannya bukan hanya risiko bisnis privat, tetapi juga merupakan sebuah kerentanan dalam jaringan ketahanan nasional. Pembahasan ini akan menganalisis temuan melalui lensa politik dan teori governance, menempatkan perusahaan swasta sebagai aktor yang posisinya paradoks: secara de facto kritis, namun secara de jure dan operasional tidak dianggap sebagai bagian dari arsitektur keamanan nasional.

a. Reinterpretasi posisi perusahaan menunjukkan bahwa PT Bawi Kameloh Sukses Mandiri tidak lagi sekadar entitas bisnis biasa, melainkan bagian dari simpul infrastruktur kritis nasional karena berperan dalam rantai pasok agribisnis dan perdagangan global. Kerentanan tata kelola data perusahaan, seperti penyimpanan dokumen strategis yang tidak aman dan komunikasi digital yang rentan, tidak hanya berisiko terhadap rahasia dagang perusahaan, tetapi juga dapat memengaruhi stabilitas ekonomi nasional, termasuk fluktuasi harga komoditas, kontinuitas ekspor, serta reputasi Indonesia sebagai pemasok global. Dengan demikian, perusahaan swasta di sektor strategis harus dipahami sebagai bagian dari infrastruktur kritis berbasis data dan fungsi ekonomi digital.
b. Konsep “Liability Chain” menunjukkan bahwa kerentanan keamanan siber perusahaan dapat menyebar melalui hubungan rantai pasok digital. Penggunaan media komunikasi tidak aman, seperti WhatsApp untuk pengiriman dokumen bisnis, bukan hanya membahayakan data perusahaan sendiri tetapi juga membuka peluang serangan terhadap mitra logistik, perbankan, hingga jaringan perdagangan yang lebih luas. Kondisi ini mencerminkan kegagalan multi-level governance, karena tidak adanya mekanisme yang efektif untuk menjembatani strategi keamanan siber nasional dengan implementasi operasional di sektor swasta. Akibatnya, perusahaan bergerak berdasarkan logika efisiensi bisnis semata tanpa integrasi dengan kepentingan keamanan nasional.
c. Implikasi politik dari temuan ini menunjukkan bahwa digitalisasi ekonomi Indonesia masih memiliki fondasi keamanan yang lemah. Ketergantungan perusahaan terhadap platform asing dan minimnya perlindungan data strategis menandakan bahwa kedaulatan ekonomi digital belum sepenuhnya terbangun. Di sisi lain, konsep kemitraan pemerintah dan swasta (public-private partnership) dalam keamanan siber juga menghadapi hambatan karena perusahaan swasta masih berada pada posisi rentan dan belum siap menjadi mitra strategis negara. Oleh sebab itu, penguatan tata kelola keamanan siber pada perusahaan swasta sektor strategis bukan hanya kebutuhan bisnis, tetapi juga langkah politik penting untuk memperkuat ketahanan ekonomi dan keamanan nasional Indonesia di era digital.

Dari Keterbatasan Teknis ke Myopia Strategis: Membongkar Akar Budaya Organisasi yang Rapuh

Temuan penelitian menunjukkan bahwa masalah keamanan siber di PT Bawi Kameloh Sukses Mandiri kerap disederhanakan menjadi masalah "kurangnya antivirus" atau "kelalaian karyawan". Namun, analisis yang lebih dalam mengungkap bahwa ini adalah gejala dari myopia strategis (rabun jauh strategis) yang berakar pada budaya organisasi. Budaya "kepercayaan antarindividu" dan orientasi "efisiensi pragmatis" yang dominan justru telah menciptakan lingkungan yang secara sistemik mengorbankan ketahanan jangka panjang untuk keuntungan operasional jangka pendek.

a) Dekonstruksi Narasi “Human Error” dan “Kurangnya Alat”:

Penelitian menunjukkan bahwa masalah keamanan siber di PT Bawi Kameloh Sukses Mandiri tidak semata-mata disebabkan oleh kelalaian individu atau kurangnya perangkat keamanan, tetapi berakar

pada budaya organisasi yang lebih menghargai kecepatan dan efisiensi dibanding keamanan. Perilaku karyawan yang menggunakan WhatsApp atau mengabaikan prosedur keamanan muncul karena organisasi tidak memiliki aturan formal, sistem penghargaan, maupun kontrol yang mendorong perilaku aman. Akibatnya, "human error" sebenarnya merupakan hasil dari sistem budaya kerja yang tidak membangun kesadaran keamanan secara kolektif.

b) Efisiensi Pragmatis vs. Ketahanan Strategis:

Budaya kerja perusahaan yang menekankan fleksibilitas dan efisiensi praktis mendorong penggunaan perangkat pribadi, aplikasi chat, dan cloud publik karena dianggap murah dan cepat. Namun, pilihan tersebut dilakukan tanpa analisis risiko yang memadai sehingga perusahaan lebih fokus pada keuntungan operasional jangka pendek dibanding ketahanan strategis jangka panjang. Kondisi ini mencerminkan myopia strategis, yaitu kemampuan melihat manfaat langsung tetapi gagal menyadari ancaman besar yang dapat muncul akibat lemahnya perlindungan data dan keamanan digital.

c) Implikasi: Dari Perbaikan Teknis ke Transformasi Budaya:

Temuan ini menunjukkan bahwa solusi keamanan siber tidak cukup hanya dengan membeli perangkat lunak atau memberikan pelatihan teknis, tetapi memerlukan transformasi budaya organisasi. Perusahaan perlu membangun norma baru bahwa keamanan data adalah tanggung jawab bersama, memberikan penghargaan terhadap praktik kerja yang aman, serta menunjukkan komitmen pimpinan dalam menerapkan budaya keamanan. Tanpa perubahan budaya tersebut, kebijakan dan teknologi keamanan hanya akan menjadi formalitas yang mudah dilemahkan oleh kebiasaan kerja lama yang terlalu berorientasi pada efisiensi pragmatis.

Sintesis: PT Bawi Kameloh Sukses Mandiri sebagai Cermin Dilema Tata Kelola Siber Indonesia

Temuan bahwa PT Bawi Kameloh Sukses Mandiri hanya mengenali. Studi kasus ini, ketika ditempatkan dalam kerangka analisis yang lebih luas, berfungsi sebagai cermin yang memperbesar dilema fundamental tata kelola keamanan siber Indonesia. Perusahaan ini bukan anomali; ia adalah contoh tipikal (archetype) dari kondisi sektor swasta menengah yang terintegrasi global. Sintesis pembahasan menghasilkan tiga proposisi kritis:

a. Proposisi 1:

Celah antara Globalisasi Operasional dan Lokalisasi Kesadaran Risiko: Penelitian menunjukkan bahwa PT Bawi Kameloh Sukses Mandiri merepresentasikan perusahaan swasta Indonesia yang telah terhubung dengan perdagangan dan rantai pasok global, tetapi masih memiliki kesadaran risiko dan tata kelola keamanan yang bersifat lokal, teknis, dan sederhana. Perusahaan telah mengadopsi digitalisasi operasional secara cepat, namun belum diimbangi dengan pemahaman terhadap ancaman siber global yang bersifat strategis. Kondisi ini menciptakan kesenjangan tata kelola (governance gap) yang membuat perusahaan rentan terhadap ancaman lintas negara dan eksploitasi digital yang lebih kompleks.

b. Proposisi 2:

Kegagalan Negara dalam Memperluas Perimeter Keamanan Nasional: Temuan penelitian memperlihatkan bahwa keamanan siber nasional Indonesia masih terlalu berfokus pada sektor pemerintah dan infrastruktur formal, sementara perusahaan swasta strategis belum diposisikan sebagai bagian penting dari perimeter keamanan nasional. Padahal, data, server, dan sistem komunikasi perusahaan seperti PT Bawi Kameloh Sukses Mandiri telah menjadi bagian dari infrastruktur ekonomi digital nasional. Ketiadaan perlindungan dan pengawasan yang memadai terhadap sektor swasta menyebabkan fondasi ketahanan siber nasional menjadi rapuh dan membuka celah keamanan yang luas.

c. Proposisi 3:

Tata Kelola Siber sebagai Prasyarat Kedaulatan Ekonomi Digital: Penelitian ini menegaskan bahwa tata kelola keamanan siber bukan sekadar pelengkap transformasi digital, tetapi merupakan syarat utama bagi terciptanya kedaulatan ekonomi digital. Digitalisasi dan peningkatan ekspor tanpa perlindungan data yang kuat justru dapat menimbulkan kebocoran informasi strategis yang mengancam kepentingan ekonomi nasional. Oleh karena itu, penguatan tata kelola keamanan siber di perusahaan swasta harus dipandang sebagai fondasi utama dalam membangun pertumbuhan ekonomi digital yang aman, berkelanjutan, dan berdaulat.

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa tata kelola keamanan siber di PT Bawi Kameloh Sukses Mandiri masih berada pada tingkat yang belum optimal dan menunjukkan adanya

kesenjangan antara transformasi digital operasional dengan kesiapan keamanan siber perusahaan. Temuan penelitian menunjukkan bahwa perusahaan telah memanfaatkan teknologi digital dalam aktivitas administrasi, komunikasi bisnis, dan perdagangan internasional, namun implementasi tata kelola keamanan siber masih bersifat informal, reaktif, dan bergantung pada kesadaran individu. Ketiadaan kebijakan formal, lemahnya manajemen risiko, belum adanya unit khusus keamanan siber, serta penggunaan media komunikasi dan perangkat pribadi tanpa kontrol keamanan yang memadai menyebabkan perusahaan memiliki tingkat ketahanan siber yang rendah. Penelitian ini juga menemukan bahwa ancaman siber di perusahaan masih dipahami sebatas ancaman teknis umum seperti phishing dan malware, sementara ancaman strategis seperti espionase ekonomi, supply chain attack, dan Advanced Persistent Threats belum dipandang sebagai risiko bisnis yang serius. Selain itu, penelitian menegaskan bahwa perusahaan swasta sektor agribisnis dan perdagangan internasional memiliki posisi strategis sebagai bagian dari infrastruktur ekonomi digital nasional, sehingga kerentanan keamanan sibernya tidak hanya berdampak pada perusahaan, tetapi juga berpotensi memengaruhi stabilitas rantai pasok, perdagangan, dan ketahanan ekonomi nasional. Dengan demikian, penelitian ini memperlihatkan bahwa tata kelola keamanan siber harus dipahami sebagai bagian penting dari strategi bisnis, keamanan non-tradisional, dan kedaulatan ekonomi digital Indonesia.

Meskipun demikian, penelitian ini memiliki beberapa keterbatasan. Pertama, penelitian hanya berfokus pada satu perusahaan sehingga hasil penelitian belum dapat digeneralisasikan untuk seluruh perusahaan swasta di Indonesia. Kedua, penelitian menggunakan pendekatan kualitatif studi kasus dengan jumlah informan yang terbatas sehingga temuan sangat dipengaruhi oleh konteks internal perusahaan dan persepsi informan. Ketiga, penelitian lebih menitikberatkan pada aspek tata kelola, budaya organisasi, dan persepsi manajemen tanpa melakukan pengujian teknis terhadap sistem keamanan perusahaan seperti penetration testing atau audit keamanan digital secara mendalam. Selain itu, keterlibatan peneliti sebagai bagian dari perusahaan juga berpotensi menimbulkan subjektivitas meskipun telah diantisipasi melalui refleksivitas dan triangulasi data.

Oleh karena itu, penelitian selanjutnya disarankan untuk memperluas cakupan studi dengan melibatkan lebih banyak perusahaan dari berbagai sektor strategis agar dapat menghasilkan gambaran yang lebih komprehensif mengenai tata kelola keamanan siber sektor swasta di Indonesia. Penelitian berikutnya juga dapat menggunakan pendekatan mixed methods atau kuantitatif untuk mengukur tingkat kesiapan keamanan siber perusahaan secara lebih objektif dan terukur. Selain itu, kajian mendatang diharapkan mampu mengintegrasikan analisis teknis keamanan digital dengan perspektif hubungan internasional, ekonomi politik, dan kebijakan publik agar dapat memahami keterkaitan antara keamanan siber perusahaan, ketahanan ekonomi nasional, serta dinamika geopolitik digital secara lebih mendalam. Penelitian lebih lanjut juga penting untuk mengkaji efektivitas kolaborasi pemerintah dan sektor swasta dalam membangun sistem keamanan siber nasional yang lebih inklusif, adaptif, dan berkelanjutan di era transformasi digital global.

DAFTAR PUSTAKA

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). *The SAGE handbook of qualitative research* (5th ed.). SAGE Publications.

Dunn Cavelty, M. (2018). Cybersecurity in international relations. In R. Burke (Ed.), *Routledge handbook of security studies* (2nd ed.). Routledge.

Flick, U. (2018). *An introduction to qualitative research* (6th ed.). SAGE Publications.

Flyvbjerg, B. (2013). *Case study research: Principles and practice*. Routledge.

Israel, M., & Hay, I. (2015). *Research ethics for social scientists*. SAGE Publications.

Klimburg, A. (2017). *The darkening web: The war for cyberspace*. Penguin Press.

Kvale, S., & Brinkmann, S. (2015). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). SAGE Publications.

Limba, T., et al. (2019). Cybersecurity governance and digital transformation in ASEAN context. *(Detail publikasi tidak lengkap dalam naskah asli)*

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE Publications.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*(9), 1212–1222.

Nugraha, A., & Syarif, R. (2020). Cybersecurity challenges and governance in Indonesia. *(Detail publikasi tidak lengkap dalam naskah asli)*

Nye, J. S. (2017). *Deterrence and dissuasion in cyberspace*. International Security, 41(3), 44–71.

Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). SAGE Publications.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Taddeo, M. (2017). Trusting digital technologies correctly. *Philosophy & Technology, 30*, 1–6.

World Economic Forum. (2023). *Global cybersecurity outlook 2023*. World Economic Forum.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.