

Kompleksitas dalam Ruang Siber: Sebuah Seruan untuk Pemimpin yang Mengutamakan Keamanan

Penulis : Tjok Istri Sintawati
Penyunting : Achmed Faiz Yudha Siregar



Pendahuluan

Di era kecerdasan buatan saat ini, pemimpin yang memiliki kepedulian terhadap keamanan perlu untuk strategi siber secara komprehensif dan mencapai ketahanan siber (cyber resilience) dalam organisasi serta ekosistemnya. Dengan adanya dualitas transformasi digital—di satu sisi memberikan manfaat yang besar bagi bisnis, tetapi di sisi lain juga menimbulkan ancaman siber (cyberthreats)—pemimpin perlu untuk menavigasikan kompleksitas ruang siber. Sebuah call-to-action untuk para pemimpin global dinyatakan dalam laporan Global Cybersecurity Outlook 2025 yang dipublikasikan oleh World Economic Forum (WEF). Laporan ini mencoba untuk menguraikan kompleksitas dunia maya yang berkembang saat ini dan menjelaskan peran strategis yang harus diambil oleh para pemimpin.

Risiko siber (cyber risk), sebagaimana yang disebutkan oleh 72% responden dalam Global Cybersecurity Outlook (GCO) 2025—terdiri atas 321 pemimpin dari 57 negara—dilaporkan mengalami peningkatan. Sebelumnya dalam Chief Risk Officers Outlook yang dipublikasikan pada Oktober 2024, para pemimpin juga menilai risiko siber sebagai ancaman terbesar ke-3 yang dapat mengancam sebuah organisasi. Evolusi kejahatan siber (cyber crime) yang semakin meningkat dari segi modus operandi dan frekuensinya juga menjadi ancaman serius bagi para pemimpin organisasi.



Risiko Siber	How Can It Become More Sophisticated
Serangan Ransomware	Ransomware—yang dapat mencegah kita untuk mengakses sistem, data, ataupun berkas kita sendiri—berkembang jauh lebih inovatif. Komoditisasi model ransomware semakin kuat, ditambah dengan pertumbuhan model RaaS (<i>Ransomware - as-a-Service</i>) yang terus berlanjut.
Penipuan yang bersumber dari ruang siber (seperti <i>phishing</i> , peretasan email bisnis, <i>vishing</i>)	Teknologi GenAI berdampak pada phishing yang lebih canggih dengan biaya yang lebih rendah. Ada pula <i>Cybercrime-as-a-service</i> (CaaS) yang berkembang pesat dan memungkinkan individu/kelompok tanpa keahlian teknis khusus untuk dapat terlibat dalam aktivitas daring ilegal hanya dengan membeli perangkat dan dukungan.
Pencurian Identitas	Deepfake, yang didukung oleh teknologi GenAI, dapat menciptakan peniruan yang meyakinkan dari segi suara, video, gambar, hingga gaya penulisan dari para pemimpin senior dalam organisasi.

Mengurangi Risiko yang Mendasari Rantai Pasok yang Lebih Saling Terhubung

Para ahli siber dan organisasi menyadari bahwa tantangan terbesar dalam kompleksitas ruang siber adalah kerentanan yang muncul dalam rantai pasok yang saling terhubung. Di antara beberapa masalah rantai pasok yang saling terhubung, yang paling mengkhawatirkan sebagaimana dikemukakan oleh organisasi yakni berpusat pada manajemen pihak ketiga. Terdapat beberapa risiko yang terkait dengan pihak ketiga yang terkadang diabaikan.

Risiko yang Tidak Dapat Dihindari Berkaitan dengan Pihak Ketiga	Dampak Lebih Besar yang Tidak Diinginkan yang Mungkin Terjadi
Kerentanan perangkat lunak yang mungkin berasal dari pihak ketiga atau vendor.	Memanfaatkan kelemahan dalam rantai pasok, seperti penyebaran malware.



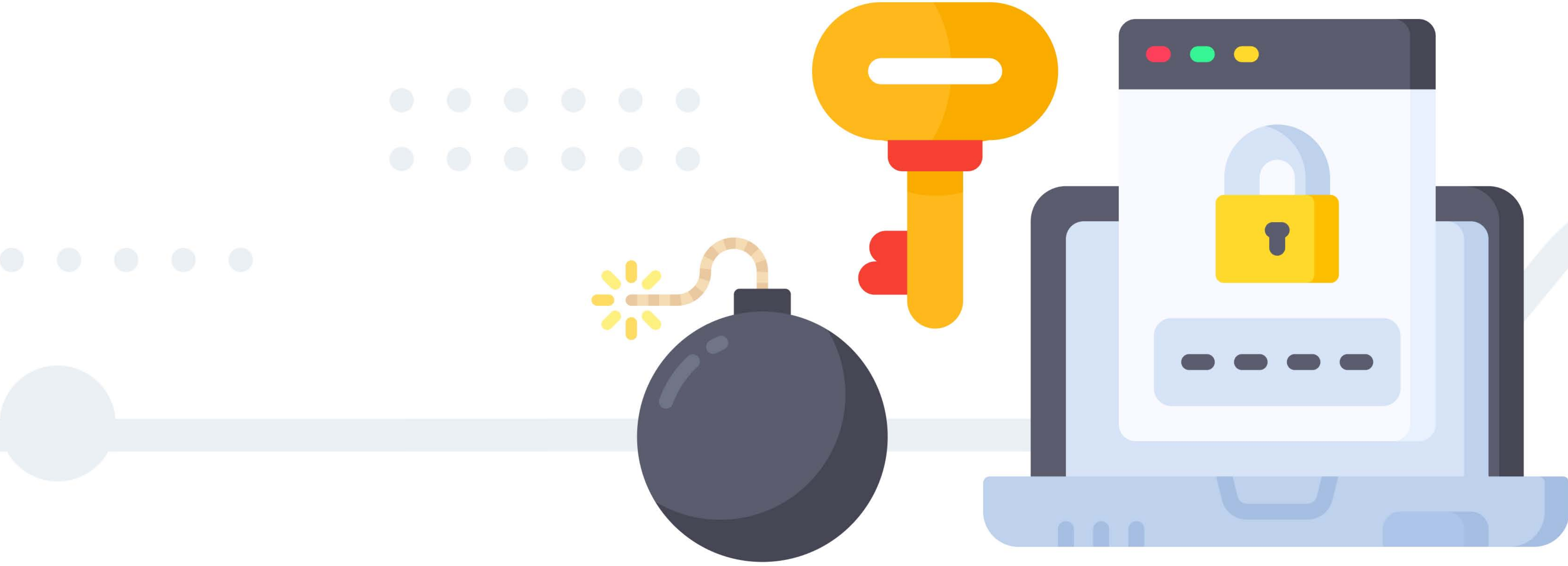
Risiko yang Tidak Dapat Dihindari Berkaitan dengan Pihak Ketiga	Dampak Lebih Besar yang Tidak Diinginkan yang Mungkin Terjadi
Kurangnya visibilitas melalui standar keamanan pihak ketiga dapat menyebabkan derajat kematangan dalam sistem keamanan yang berbeda.	Lebih sulit menerapkan regulasi siber dan mendapatkan ketahanan siber.
Ketergantungan pada terbatasnya jumlah penyedia penting dapat menjadi titik kegagalan sistemik	Setiap kerentanan yang terjadi pada penyedia akan berdampak langsung pada basis klien secara luas dan mungkin memiliki efek domino terhadap seluruh ekosistem.

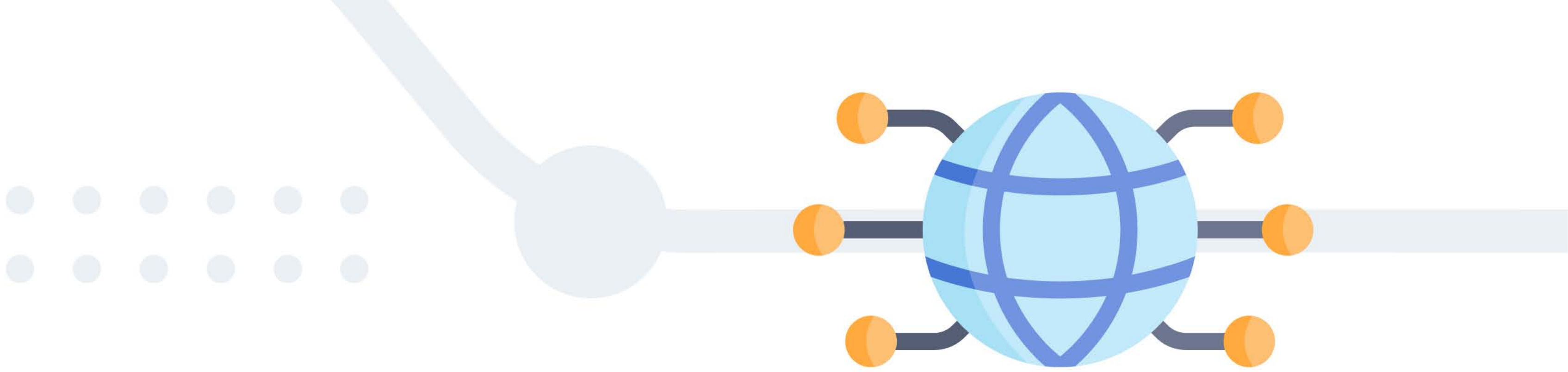
Risiko dari rantai pasok yang lebih saling terhubung semakin bertambah pelik dengan meningkatnya ketidakadilan di ruang siber. Ketimpangan di seluruh ekosistem ruang siber—antara mereka yang memiliki sumber daya untuk beradaptasi dan mereka yang tidak—akan mempengaruhi ketahanan ekosistem secara keseluruhan karena setiap insiden yang terjadi pada organisasi yang kurang matang juga akan berdampak pada seluruh rantai pasok.

Aktor	Disparitas
Organisasi besar vs organisasi kecil	- Organisasi-organisasi kecil hampir mendekati titik kritis di mana mereka tidak dapat lagi secara efektif mengamankan diri terhadap meningkatnya kompleksitas risiko siber. Di sisi lain, ketahanan siber di organisasi besar dilaporkan sudah memadai. - Fakta bahwa permintaan global untuk profesional keamanan siber melebihi pasokan juga membuat organisasi-organisasi kecil lebih rentan dalam kasus ini. - Asuransi siber menjadi lebih matang dalam beberapa tahun terakhir, tetapi organisasi-organisasi yang lebih besar tampaknya mendapatkan lebih banyak manfaat karena mereka lebih mampu membayarnya daripada organisasi-organisasi kecil.

Aktor	Disparitas
Negara maju vs negara berkembang	Organisasi-organisasi di belahan bumi selatan, seperti di Afrika dan Amerika Latin, cenderung kurang percaya diri dalam mendeklarasikan ketahanan siber dibandingkan organisasi di belahan bumi utara, seperti Eropa dan Amerika Utara.
Multi sektoral	- Organisasi-organisasi di sektor keuangan lebih maju dalam hal keamanan siber dibandingkan dengan sektor manufaktur yang masih dalam tahap awal membangun ketahanan siber. - Organisasi di sektor publik juga menyatakan bahwa mereka belum cukup mampu mencapai ketahanan siber dibandingkan dengan organisasi di sektor swasta.

Ketahanan siber merupakan mandat yang harus diwujudkan bagi seluruh ekosistem, baik organisasi besar maupun kecil, dalam rantai pasok yang semakin saling terhubung. Kondisi ini memerlukan strategi kepemimpinan untuk menangani keamanan siber, seperti melalui pengawasan, yang mana anggota dewan direksi menerima pembaruan berkala tentang insiden siber, tren, kerentanan, dan prediksi risiko baik dari pihak ketiga internal maupun eksternal, yang terbukti dapat meningkatkan ketahanan siber. Berkaca pula pada kondisi ketidakadilan yang terjadi, tindakan kolektif juga diperlukan untuk mencapai ketahanan siber karena dalam ekosistem yang saling terhubung, ketahanan secara keseluruhan bergantung pada mata rantainya yang paling lemah. Organisasi besar mungkin dapat memberikan insentif yang membantu organisasi yang lebih kecil untuk mencapai ketahanan siber yang akan berdampak pada ketahanan seluruh ekosistem. Kolaborasi internasional juga penting sebagai upaya kolektif untuk menangani kejahatan siber yang semakin canggih dan tanpa batas.





Menghadapi Dinamika Geopolitik di Era Kecerdasan Buatan

Perkembangan ancaman siber dan meningkatnya ketegangan geopolitik menimbulkan risiko signifikan berupa gangguan terhadap infrastruktur vital yang dapat membahayakan keselamatan manusia. Berdasarkan wawancara dengan para pemimpin untuk laporan ini, seorang Chief Information Security Officer (CISO) menyatakan bahwa penyerang yang disponsori negara semakin tidak hanya menargetkan pemerintah, tetapi juga mencoba mengganggu perekonomian dan infrastruktur penting, sehingga menciptakan kekacauan dalam sistem global. Dalam hal ini, ancaman siber dapat menyerang sistem kontrol dan membahayakan data infrastruktur penting, yaitu fasilitas air dan infrastruktur komunikasi, yang menjamin kehidupan masyarakat luas. Beberapa kasus ancaman siber terkait ketegangan geopolitik yang pernah terjadi dan membahayakan nyawa manusia dapat menjadi refleksi bagi para pemimpin dalam meningkatkan ketahanan siber.

Area Berisiko Tinggi	Ancaman yang Muncul
Fasilitas air	Serangan siber terhadap perusahaan air terbesar di Amerika Serikat terjadi pada tahun 2024 yang menyebabkan gangguan dalam operasional. Serangan siber ini juga meningkatkan kewaspadaan terhadap keamanan infrastruktur penting, seperti sistem OT (titik akses jarak jauh dan perangkat lunak yang sudah ketinggalan zaman).
Biosecurity	Pada tahun 2024, dua laboratorium di Afrika Selatan dan Inggris menjadi target serangan siber. Ada kekhawatiran yang meningkat tentang kemampuan serangan siber untuk melumpuhkan sistem laboratorium yang penting, mengganggu operasi, dan menyebabkan hilangnya integritas data, yang dapat membahayakan protokol keselamatan.
Infrastruktur komunikasi	Infrastruktur komunikasi penting, seperti infrastruktur telekomunikasi, satelit, dan kabel bawah laut sering menjadi sasaran serangan siber. Serangan siber terhadap infrastruktur komunikasi, misalnya jaringan satelit ViaSat di Eropa; 124 operasi siber di sektor luar angkasa yang terkait dengan konflik Ukraina-Rusia; dan insiden kabel bawah laut di Laut Baltik.
Iklim dan energi	Berkembangnya sistem energi terbarukan—yang penting untuk mendukung teknologi modern—perlu dirancang dengan sistem keamanan sebagai salah satu prioritas mendasar. Ini merupakan kebutuhan mendesak karena sistem energi telah menjadi target yang sangat menarik bagi para penjahat ruang siber.

Sebagai konsekuensi dari dunia yang semakin saling terhubung, muncul pula risiko kerusakan tambahan. Dalam situasi ini, memahami dinamika geopolitik itu sendiri menjadi penting untuk manajemen risiko jangka panjang yang efektif. Hal ini tidak hanya terbatas pada keterampilan tingkat lanjut dalam keamanan siber tetapi juga pada penerapan manajemen risiko kuno. Manajemen ini mengharuskan untuk menganalisis masalah dari perspektif dampak bisnis terlebih dahulu sebelum mengelola dan menerima risiko yang tersisa.

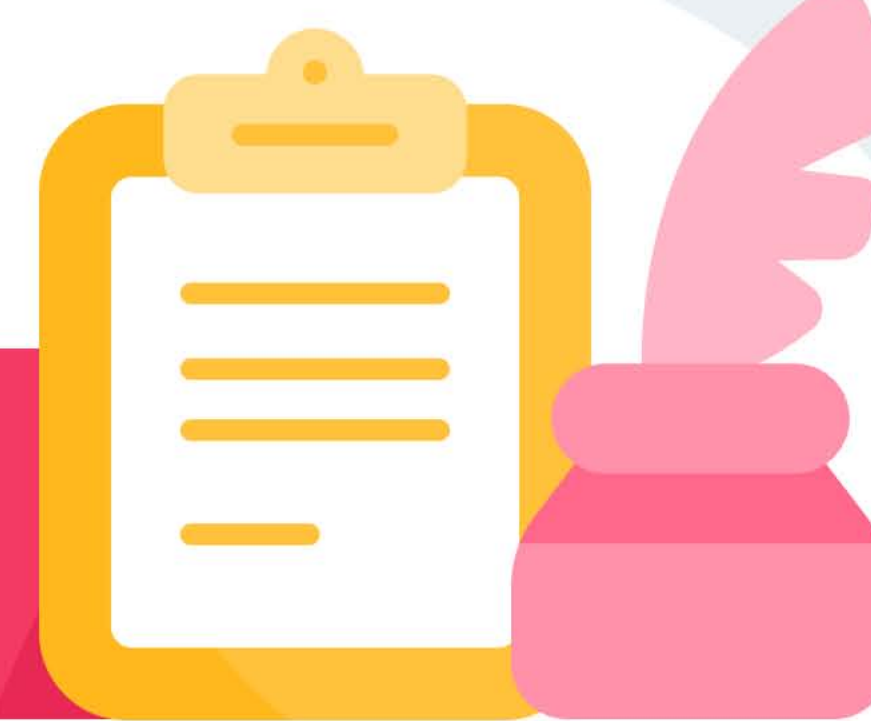
Berusaha untuk Membentuk Regulasi yang Lebih Baik guna Memastikan Keamanan Siber Secara Global

Regulasi dianggap sebagai salah satu pendorong terpenting untuk memperoleh ketahanan siber oleh 78% CISO dan 87% CEO yang disurvei dalam laporan ini. Meskipun regulasi siber penting sebagai kerangka hukum untuk mengamankan praktik keamanan siber, pada kenyataannya terdapat pula tantangan yakni regulasi yang tumpang tindih di seluruh dunia yang berimplikasi pada bertambahnya kompleksitas pada strategi keamanan siber.

Kawasan	Regulasi
Amerika	Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), Brazil’s General Data Protection Law (LGPD)
Afrika	Nigeria’s Data Protection Regulation (NDPR)
Asia-Pasifik	Japan’s Act on the Protection of Personal Information (APPI), Singapore’s Cybersecurity Act
Eropa	The Network and Information System Directive 2 (NIS2), the EU’s General Data Protection Regulation (GDPR), Digital Operations Resilience Act (DORA)

Dalam situasi di mana peraturan bersifat kompleks dan banyak, yang menyebabkan kelelahan di antara perusahaan dan mengurangi efektivitas tujuan mereka, kerja sama publik-swasta penting untuk mencapai harmonisasi peraturan global. Upaya ini dapat menciptakan standar keamanan siber yang dapat diterapkan di seluruh wilayah secara lebih konsisten dan efektif. Organisasi juga dapat lebih fleksibel untuk beradaptasi dengan ancaman dan teknologi yang muncul.

Kekuatan dan Kelemahan dari Report



Kekuatan



Kelengkapan dan Cakupan Data yang Luas

Data dalam studi ini diperoleh menggunakan metode campuran yang membuat data menjadi kaya. Cakupan data dalam studi ini juga luas karena partisipan yang terlibat berasal dari 57 negara dan mencakup berbagai pemangku kepentingan seperti eksekutif, pemimpin industri, pemerintah, akademisi, dan masyarakat sipil.



Memberikan Wawasan Strategis untuk Pemimpin

Studi ini mengungkap kompleksitas ruang siber dan kekhawatiran pemimpin dari berbagai industri terkait meningkatnya risiko dunia maya. Hal ini dapat berguna bagi para pemimpin global untuk mengambil langkah pertama dalam mewujudkan ketahanan ruang siber.

Kelemahan



Kurangnya Analisis Mendalam pada Setiap Isu yang Dibahas

Di sisi lain, melimpahnya data dalam penelitian ini juga mengakibatkan analisis yang dilakukan pada setiap isu yang dibahas menjadi kurang komprehensif.



Terlalu Menekankan Persepsi Pemimpin di Level Eksekutif

Data dalam penelitian ini sebagian besar diperoleh dari partisipan tingkat eksekutif, sehingga hanya mencakup sedikit perspektif dari individu di hierarki bawah, seperti yang terkait dengan kendala di lapangan yang mungkin mereka alami.



Referensi

World Economic Forum. (2024, October). Chief risk officers outlook: October 2024. <https://www.weforum.org/publications/chief-risk-officers-outlook-october-2024/#:~:text=Chief%20risk%20officers%20are%20most,anticipating%20volatile%20conditions%20has%20increased.>