MUSYTARI
ISSN: 3025-9495

Neraca Manajemen, Ekonomi
Vol 20 no 10 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

STRATEGI KETAHANAN EKONOMI BCA MELALUI INVESTASI KEAMANAN DIGITAL 2025

Muhammad Agung Ferdiansyah[1], Cantika Amelia[2], Farhan Aditya[3], Oki Iqbal Khair[4]
[1,2,3,4]Program Studi Manajemen, Fakultas Ekonomi dan Bisnis,
Universitas Pamulang, Indonesia
[1]agungmuhamad1928@gmail.com, [2]c4ntikamelia27@gmail.com, [3]farhanadithya7@gmail.com,
[4]dosen01801@unpam.ac.id

Abstract

Global economic uncertainty and increasing cyber threats have driven PT Bank Central Asia Tbk (BCA) to strengthen its digital security strategy in 2025. This study applies a descriptive qualitative approach with a case study on BCA to explore how the company builds economic resilience through increased IT capital expenditure, adoption of artificial intelligence (AI) and biometric authentication, and user-focused digital security education programs. The findings indicate that BCA's 8-10% increase in IT spending is aimed at enhancing cybersecurity infrastructure, deploying AI-based fraud detection systems, and reinforcing multi-factor authentication. Additionally, educational campaigns such as "Tolak Dengan Anggun" (Graceful Rejection) have proven effective in reducing human error, the leading cause of data breaches. This comprehensive strategy not only maintains customer trust but also supports the stability of the national financial system amid global challenges.

Keywords: *Digital Security, BCA, Economic Resilience, AI, Biometric Authentication, Digital Literacy*

Abstrak

Kondisi ekonomi global yang kurang stabil dan risiko kejahatan siber yang semakin meningkat mendorong PT Bank Central Asia Tbk (BCA) untuk memperkuat sistem keamanan digital mereka, terutama menjelang tahun 2025. Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan fokus pada BCA, untuk menggambarkan bagaimana perusahaan tersebut meningkatkan ketahanan ekonominya. Hal ini dilakukan dengan cara menambah investasi di bidang teknologi informasi, menerapkan teknologi kecerdasan buatan (AI) dan penggunaan sistem otentikasi biometrik, serta mengadakan program edukasi tentang keamanan digital bagi para pengguna. Hasil penelitian menunjukkan bahwa peningkatan alokasi dana untuk TI sekitar 8-10% digunakan untuk mengembangkan infrastruktur keamanan, mengimplementasikan sistem deteksi penipuan berbasis AI, serta memperkuat sistem autentikasi ganda. Selain itu, program edukasi seperti "Tolak Dengan Anggun" terbukti efektif dalam meminimalkan kesalahan manusia yang sering menjadi penyebab utama kebocoran data. Langkah-langkah ini tidak hanya bertujuan untuk menjaga kepercayaan nasabah, tetapi juga berperan penting dalam menjaga stabilitas sistem keuangan nasional di tengah berbagai tantangan global yang ada.

Kata kunci: Keamanan Digital, BCA, Ketahanan Ekonomi, AI, Otentikasi Biometrik, Literasi Digital

Article history
Received: Juni 2025
Reviewed: Juni 2025
Published: Juni 2025

Plagirism checker no 80
Doi : prefix doi :
10.8734/musytari.v1i2.365
Copyright : author
Publish by : musytari

This work is licensed under a creative commons attribution-noncommercial 4.0 international license

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 20 no 10 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

PENDAHULUAN

Beberapa tahun belakangan ini, gejolak ekonomi dunia terasa begitu kuat, memberikan dampak yang signifikan bagi pelaku usaha di berbagai sektor, termasuk dunia perbankan. Menurut prediksi terbaru Bank Dunia, pertumbuhan PDB global di tahun 2025 diperkirakan hanya mencapai sekitar 2,3 %, angka terendah sejak krisis tahun 2008, dan menandai periode terlemah dalam beberapa dekade terakhir (Stewart, 2025). Dampak dari ketidakpastian global ini sangat dirasakan oleh perusahaan seperti BCA, baik dari sisi operasional maupun strategi. Perubahan nilai tukar mata uang yang tidak stabil, kenaikan suku bunga yang drastis, serta beban operasional akibat gangguan rantai pasokan (Salami et al. , 2025)membuat bank harus menjaga likuiditas yang cukup dan melakukan penyesuaian pada manajemen risiko secara cepat. Volume transaksi digital yang besar juga meningkatkan risiko serangan siber, terutama dengan kondisi eksternal yang tidak pasti dan ancaman teknologi yang semakin canggih.

Dengan digitalisasi layanan perbankan, BCA menghadapi tantangan yang tidak kecil di bidang keamanan siber, terutama karena jumlah transaksi yang mencapai hampir 100 juta per hari. Bank ini terus menerus berhadapan dengan berbagai jenis serangan, seperti *ransomware, DDoS, Social engineering*, dan *malware*. Untuk mengatasi hal ini, BCA menerapkan pendekatan yang menyeluruh, yaitu "*people process technology*", yang fokus tidak hanya pada peningkatan sistem teknologi, tetapi juga pelatihan intensif bagi karyawan dan edukasi bagi nasabah. Data menunjukkan bahwa sekitar 88 % kasus kebocoran data disebabkan oleh kesalahan manusia, sehingga penting untuk meningkatkan kesadaran dan pemahaman digital. Untuk merespons tekanan ini, BCA menganggarkan dana tambahan sebesar 8–10 % untuk divisi TI di tahun 2025. Investasi ini digunakan untuk memperkuat infrastruktur keamanan siber, mengintegrasikan sistem deteksi ancaman berbasis kecerdasan buatan, serta membentuk tim pemantau yang siap siaga selama 24 jam. Selain itu, BCA juga meningkatkan penggunaan otentikasi ganda (MFA) dan autentikasi biometrik, serta menerapkan standar internasional seperti ISO dan NIST, untuk menjaga keamanan sistem dan kelancaran operasional (Yunianto, 2025).

METODOLOGI PENELITIAN

Studi ini memakai metode kualitatif deskriptif dengan studi kasus di PT Bank Central Asia Tbk (BCA). Alasan penggunaan metode ini adalah untuk menggali lebih dalam strategi serta praktik keamanan digital BCA dalam menciptakan ketahanan ekonomi perusahaan saat menghadapi tantangan ekonomi global dan bahaya dunia maya. Riset ini bertujuan menjabarkan cara BCA membangun dan menjaga ketahanan ekonominya lewat strategi peningkatan anggaran IT, pemakaian teknologi keamanan berbasis AI dan biometrik, serta pengajaran keamanan bagi nasabah, juga menganalisis efek strategi tersebut terhadap stabilitas dan keyakinan nasabah. Teknik analisis data yang dipakai dalam riset ini memakai pendekatan analisis tematik yang meliputi penentuan tema pokok, seperti: keamanan digital, peningkatan infrastruktur IT, literasi digital, serta adaptasi terhadap ancaman teknologi. Kendala akses terhadap data internal perusahaan disiasati dengan memanfaatkan info dari dokumen publik, laporan tahunan, dan hasil kajian akademis.

HASIL DAN PEMBAHASAN

3.1 Peningkatan Alokasi Capex TI

Pada tahun 2025, BCA berencana menambah anggaran belanja modal (capex) untuk bidang TI sekitar 8–10%, fokusnya untuk memperkuat sistem keamanan digital mereka. Langkah ini diambil sebagai respons terhadap maraknya serangan siber serta peningkatan signifikan volume transaksi digital oleh para nasabah (Catriana and Setiawan, 2025). Dana tambahan ini akan dialokasikan untuk berbagai keperluan, seperti pemantauan jaringan secara langsung,

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 20 no 10 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

modernisasi infrastruktur keamanan TI, serta perekrutan ahli TI yang mumpuni. Misalnya, BCA secara berkelanjutan menerapkan teknologi terbaru dan meningkatkan kualitas SDM TI untuk menangkal ancaman siber (Hutauruk Mirayanti Dina, 2025).

Kenaikan investasi di bidang TI ini juga dipengaruhi oleh pertumbuhan jumlah transaksi di BCA. Menurut David Formula, EVP Strategic IT BCA, peningkatan belanja modal terjadi "karena kapasitas dan jumlah transaksi kita terus meningkat", yang menunjukkan bahwa nasabah semakin percaya pada keamanan digital BCA (Catriana and Setiawan, 2025). Oleh karena itu, perluasan kapasitas TI dan investasi capex ini penting untuk memastikan bahwa infrastruktur bank dapat menangani volume transaksi yang terus bertambah, menjaga operasional tetap lancar, dan mempertahankan kepercayaan nasabah dalam jangka panjang.

Selain menaikkan anggaran TI, BCA juga menerapkan strategi yang menggabungkan kebutuhan teknologi dengan tujuan bisnis jangka panjang. Hal ini tercermin dalam penyatuan rencana belanja modal TI ke dalam program transformasi digital 2025 yang berfokus pada tiga aspek utama: operational excellence, customer-centric services, dan risk-resilient systems. TI tidak lagi hanya dianggap sebagai pendukung, tetapi sebagai penggerak utama pertumbuhan bisnis yang fleksibel dan mampu beradaptasi dengan ancaman dari luar. Kebijakan ini juga diperkuat dengan dibentuknya komite manajemen risiko digital yang terdiri dari perwakilan dari divisi teknologi, hukum, dan kepatuhan. Tugas komite ini adalah untuk secara rutin mengevaluasi risiko keamanan digital dan memberikan rekomendasi untuk intervensi strategis, termasuk mengganti vendor, mengembangkan teknologi internal, atau bekerja sama dengan startup teknologi siber dalam negeri.

3.2 Implemntasi AI dan Otentikasi Berlapis

Guna mendeteksi penipuan, BCA menggunakan teknologi "*Artificial Intelligence*" (AI) dalam sistem deteksi adaptif yang mampu menganalisis pola transaksi secara "*real-time*". AI dapat mendeteksi keanehan dan aktivitas yang mencurigakan pada data transaksi nasabah sebelum menyebabkan kerugian (Pratama Galih, 2025). Teknologi AI ini memperkuat sistem perlindungan bank, contohnya dengan otomatis memblokir transaksi mencurigakan tanpa campur tangan manusia. Selain AI, BCA menerapkan sistem "*multi-factor authentication*" yang menggabungkan elemen seperti OTP dan biometrik. Menurut ahli, autentikasi biometrik menjadi solusi utama untuk memastikan keamanan transaksi digital, sebab hanya pemilik data biometrik yang dapat mengakses akun (redaksi, 2024).

Dengan begitu, kombinasi AI canggih dan autentikasi ganda meningkatkan keamanan sistem perbankan dari penipuan. Pemanfaatan teknologi ini terbukti sangat efektif dalam menurunkan tingkat penipuan. Contohnya, laporan kasus di industri keuangan mengungkapkan bahwa penggunaan gabungan aplikasi autentikator dan kunci keamanan fisik berhasil menurunkan upaya pembajakan akun hingga 98%. Hasil ini selaras dengan riset terbaru yang memperlihatkan bahwa bank yang menerapkan MFA dan biometrik secara bersamaan hampir menghilangkan risiko penipuan online. Singkatnya, pemanfaatan AI untuk mendeteksi penipuan beserta lapisan keamanan tambahan seperti MFA dan biometrik sangat efektif menjaga keamanan transaksi digital.

Sebagai upaya memperkuat keamanan digital nasional, BCA juga aktif bekerja sama dengan berbagai pihak seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan perusahaan "*fintech*" lokal. Kolaborasi ini meliputi pertukaran informasi terkait ancaman siber, pelatihan bersama, dan uji penetrasi berkala yang bertujuan menemukan potensi celah keamanan yang mungkin tidak terdeteksi oleh sistem internal. Melalui Forum Komunikasi Industri Jasa Keuangan Digital (FKIJKD), BCA menjadi pelopor dalam mengembangkan standar keamanan minimum API yang digunakan untuk "*Open Banking*".

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 20 no 10 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

Langkah ini krusial untuk mengantisipasi potensi risiko pada sistem pembayaran yang semakin terbuka terhadap integrasi eksternal.

3.3 Edukasi Pengguna dan Penguatan SDM

BCA juga gencar melaksanakan kampanye yang bertujuan mendidik nasabah agar meminimalisir kesalahan pengguna. Contohnya, ada inisiatif "Tolak Dengan Anggun" yang mengajak nasabah untuk tidak memberikan data pribadi (seperti nomor kartu, PIN, OTP, dan lainnya) kepada siapapun yang tidak dikenal. Kampanye ini menjelaskan bahwa permintaan data pribadi itu sudah pasti penipuan, sehingga nasabah pantas disebut sebagai "Duta Tolak Dengan Anggun". Selain itu, HaloBCA (baik *call center* maupun aplikasi *mobile*) dilengkapi fitur edukasi serta pengaduan langsung untuk meningkatkan pemahaman pengguna tentang keamanan digital. Contohnya, aplikasi HaloBCA yang diperbarui di awal tahun 2025 menyediakan fitur pelaporan masalah dan layanan Halo BCA Chat, sebagai langkah aktif memberikan informasi edukatif kepada nasabah untuk mengatasi berbagai modus penipuan.

Edukasi ini sangat penting karena sebagian besar masalah keamanan justru disebabkan oleh ketidakhati-hatian pengguna. Data menunjukkan bahwa sekitar 88% kebocoran data terjadi karena kesalahan manusia, termasuk rekayasa sosial seperti *phishing* dan permintaan OTP palsu. Menanggapi hal ini, pihak manajemen BCA terus mengingatkan agar nasabah selalu waspada saat melakukan transaksi digital: misalnya dengan tidak membagikan kode OTP atau password kepada siapapun serta selalu memeriksa kebenaran pesan mencurigakan. Fokus pada peningkatan literasi digital ini diharapkan bisa menutup celah yang sering dimanfaatkan penipu dan mengurangi potensi kerugian akibat kesalahan pengguna secara signifikan (santosa, 2025).

Aspek *Environmental, Social*, dan *Governance* (ESG) kini menjadi acuan penting dalam merancang strategi keamanan digital BCA. Khususnya dalam hal *Governance*, sistem keamanan digital menjadi salah satu tolok ukur penilaian tata kelola yang baik. Audit TI tahunan sekarang tidak hanya berfokus pada efisiensi, tetapi juga pada transparansi, akuntabilitas, dan kepatuhan terhadap peraturan, misalnya UU Perlindungan Data Pribadi (PDP) yang berlaku di Indonesia sejak 2024. Dalam dimensi *Social*, BCA berusaha meningkatkan kesadaran akan pentingnya keamanan digital melalui program literasi digital yang menyasar pelajar dan UMKM, yang selama ini rentan menjadi korban *phishing* dan pinjaman online ilegal. Dengan menyebarkan materi edukasi ke sekolah dan komunitas bisnis mikro, BCA berperan aktif melindungi kelompok ekonomi yang rentan.

3.4 Kontribusi terhadap Ketahanan Ekonomi

BCA juga berinvestasi di bidang keamanan digital, yang dampaknya sangat baik untuk ketahanan ekonomi dalam jangka panjang. Dana yang dialokasikan untuk belanja TI, yang diperkirakan naik delapan persen pada tahun 2025, khusus digunakan untuk membangun infrastruktur perbankan digital yang tidak hanya aman, tetapi juga bisa diandalkan dan dipercaya (santosa, 2025). Sistem yang kokoh akan membantu bank melayani nasabah dengan baik, bahkan saat terjadi peningkatan transaksi yang signifikan. IMF berpendapat bahwa serangan siber pada lembaga keuangan bisa mengganggu kestabilan sistem keuangan jika kepercayaan masyarakat berkurang. Karena itu, peningkatan keamanan TI oleh BCA membantu mencegah gangguan sistemik yang bisa berdampak besar pada perekonomian secara keseluruhan. Keamanan digital juga dianggap penting untuk menjaga inklusi keuangan.

Menurut OJK (2023), masih adanya kesenjangan dalam literasi dan inklusi keuangan justru menjadi penyebab maraknya kejahatan siber di sektor keuangan (irawati, 2023). BCA turut serta menciptakan lingkungan finansial yang lebih inklusif dengan mengurangi kesenjangan ini melalui edukasi dan perlindungan teknologi. Nasabah akan lebih percaya pada layanan digital yang aman, dan ini akan mendorong lebih banyak orang untuk memanfaatkan layanan perbankan formal. Alhasil, sistem perbankan yang kuat dan inklusif akan meningkatkan

stabilitas ekonomi negara, karena semakin banyak masyarakat yang terlibat dalam siklus ekonomi formal tanpa perlu khawatir akan penipuan.

Investasi di bidang keamanan digital mungkin tidak langsung menunjukkan hasil dalam waktu singkat. Oleh karena itu, BCA menggunakan *Key Performance Indicators* (KPI) *non-finansial*, seperti seberapa berhasil upaya mitigasi insiden, berapa lama waktu yang dibutuhkan untuk pemulihan setelah insiden, dan bagaimana indeks kepercayaan nasabah. Berdasarkan survei internal yang dilakukan pada 2025, tingkat kepuasan terhadap layanan digital BCA naik dari 88% menjadi 92% setelah fitur keamanan baru diterapkan. Ini menunjukkan bahwa ada hubungan yang baik antara keamanan dan loyalitas pelanggan. Selain itu, BCA juga mengevaluasi indikator ketahanan ekonomi internal, seperti peningkatan efisiensi operasional berkat otomasi dalam mendeteksi penipuan, serta penurunan biaya perkara hukum terkait kebocoran data.

KESIMPULAN

Guna mengatasi tantangan ekonomi dan kemajuan teknologi di tahun 2025, BCA telah menerapkan taktik keamanan digital yang mendalam. Melalui peningkatan anggaran TI, pemanfaatan teknologi AI dan sistem autentikasi yang lebih baik, serta peningkatan kesadaran pengguna, BCA membuktikan bahwa dana yang dialokasikan untuk keamanan digital adalah aspek krusial untuk menjaga mutu sistem perbankan modern. Studi ini menyarankan agar pengukuran ROI keamanan digital dievaluasi secara rutin dan diperluas ke bidang regulasi serta privasi seiring dengan perkembangan *AI generatif*. Strategi keamanan digital yang diterapkan BCA untuk tahun 2025 bukan sekadar tanggapan terhadap risiko dunia maya, melainkan bagian dari perubahan besar untuk memperkokoh fondasi ekonomi dalam jangka panjang. Dengan metode yang komprehensif termasuk investasi TI, penerapan teknologi AI dan biometrik, peningkatan pemahaman digital, kerjasama antar sektor, serta penerapan prinsip ESG—BCA mampu membangun sistem perbankan yang kuat dan berkesinambungan. Studi ini menegaskan bahwa keamanan digital bukan hanya alat pelindung, tetapi juga sumber keunggulan dalam persaingan. Oleh karena itu, disarankan agar bank lain di Indonesia mengikuti jejak ini dengan menyesuaikan kemampuan organisasi dan ciri khas pasar yang mereka layani. Penilaian ROI keamanan juga perlu mencakup aspek sosial dan nama baik, mengingat kepercayaan nasabah adalah aset berharga dalam dunia ekonomi digital saat ini.

DAFTAR PUSTAKA

Catriana, E., & Setiawan, D. R. S. (2025). Belanja Modal BCA untuk Keamanan Naik hingga 10 Persen pada 2025 Artikel ini telah tayang di Kompas.com dengan judul "Belanja Modal BCA untuk Keamanan Naik hingga 10 Persen pada 2025.

Hutauruk Mirayanti Dina. (2025). BCA Pastikan Layanan Digitalnya Sanggup Memproses Transaksi Jumbo Per Detik.

Irawati. (2023). Gap Inklusi dan Literasi Keuangan Picu Maraknya Kejahatan Siber.

Pratama Galih. (2025). Kombinasi AI dan NoSQL Tangkal Kejahatan Siber di Sektor Perbankan Digital.

Redaksi. (2024). Otentikasi Biometrik jadi Kunci Hadapi Penipuan Digital.

Salami, I. A., Popoola, A. D., Gbadebo, M. O., Kolo, F. H. O., & Adesokan-Imran, T. O. (2025). AI- Powered Behavioural Biometrics for Fraud Detection in Digital Banking: A Next-Generation Approach to Financial Cybersecurity. Asian Journal of Research in Computer Science, 18(4), 473–494. https://doi.org/10.9734/ajrcos/2025/v18i4632

Santosa, edi. (2025). Inilah Strategi di Balik Sistem Keamanan yang Tangguh dan Layanan haloBCA.

MUSYTARI
ISSN: 3025-9495
Neraca Manajemen, Ekonomi
Vol 20 no 10 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

Stewart, H. (2025). Bank Dunia: Tahun 2020-an akan menjadi dekade terlemah bagi ekonomi global sejak 1960-an. https://www.theguardian.com/business/2025/jun/10/world-economy-world-bank-donald-trump-tariffs?

Yunianto, K. T. (2025). Tingkatkan Kemanan Transaksi Digital, BCA Naikkan Belanja Modal IT 8%.