JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 04, No. 01, Tahun 2025, Hal. 2287-2296, ISSN: 3031-9498 (Online)

Tantangan Organisasi dalam Menerapkan *Zero Trust Protocol*: Studi Fenomenologi Pada Industri Perbankan atau Fintech

Ardian Fachreza
Prodi Informatika, Fakultas Teknik, Universitas Wahid Hasyim
Email: ardian.fachreza@unwahas.ac.id

Article Info

Article history:

Received November 24, 2025
Revised December 02, 2025
Accepted December 12, 2025

Keywords:

Zero Trust Protocol, Cybersecurity, Banking and Fintech Industry, Phenomenology, Digital Infrastructure, Legacy System Integration, Cyber Risk Management, Digital Transformation, Authentication and Authorization, Modern Security Architecture

ABSTRACT

Zero Trust Protocol is a modern security framework that has become increasingly *significant within the financial industry as a response to escalating cyber threats, rapid digitalization, and the rising complexity of organizational network infrastructures. The expansion of digital services such as mobile banking, open banking ecosystems, API-based financial operations, and the adoption of multi-cloud environments demands a security approach centered on continuous verification and identity-based access control. Traditional perimeter-focused security models are no longer sufficient to guard against sophisticated attacks, including credential-based intrusions, insider threats, and the exploitation of outdated legacy systems. Consequently, Zero Trust emerges as a transformative paradigm promoting continuous authentication, micro-segmentation, adaptive security policies, and least-privilege access enforcement. This study employs a qualitative phenomenological approach to explore the lived experiences of cybersecurity practitioners across banking and fintech organizations in adopting Zero Trust. Through in depth interviews, the study reveals that organizations face multiple challenges, including uneven infrastructure readiness, cultural resistance due to stricter authentication workflows, limited technical competencies among cybersecurity personnel, high implementation costs, and complex integration processes involving entrenched legacy systems. Additional challenges include regulatory compliance constraints, identity management consolidation issues, and the need for policy harmonization to support Zero Trust implementation. This research proposes several strategic recommendations, such as comprehensive infrastructure audits, enhanced workforce capability development, realistic Zero Trust implementation roadmaps, and phased migration prioritizing high-value digital assets. The findings provide practical insights and guidance for financial institutions seeking to strengthen their cybersecurity posture and enhance organizational resilience against evolving cyber threats.*

Article Info

Article history:

Received November 24, 2025
Revised December 02, 2025
Accepted December 12, 2025

ABSTRACT

Zero Trust Protocol merupakan pendekatan keamanan modern yang semakin relevan dalam industri finansial seiring meningkatnya ancaman siber, maraknya aktivitas digital, serta kompleksitas arsitektur jaringan pada lembaga keuangan. Penerapan teknologi digital seperti mobile banking, open banking, API layanan keuangan,

Keywords:

Zero Trust Protocol, Keamanan Siber, Perbankan dan Fintech, Fenomenologi, Infrastruktur Digital, Sistem Legacy, Manajemen Risiko Siber, Transformasi Digital, Autentikasi dan Otorisasi, Arsitektur Keamanan Modern

dan pemanfaatan multi-cloud menjadikan kebutuhan keamanan berbasis identitas semakin kritis. Model keamanan tradisional yang berfokus pada perimeter tunggal dinilai tidak lagi mampu memberikan perlindungan yang memadai terhadap ancaman canggih seperti serangan berbasis kredensial, *insider threat*, dan eksploitasi sistem legacy. Oleh karena itu, Zero Trust hadir sebagai paradigma baru yang menekankan prinsip verifikasi berkelanjutan, segmentasi mikro, autentikasi adaptif, serta pembatasan akses berbasis *least privilege*. Penelitian ini menggunakan metode kualitatif dengan pendekatan fenomenologi untuk menggali pengalaman mendalam para praktisi keamanan siber di sektor perbankan dan fintech terkait implementasi Zero Trust. Melalui wawancara mendalam, penelitian ini mengungkap bahwa tantangan utama yang dihadapi organisasi mencakup kesiapan infrastruktur yang belum seragam, resistensi budaya organisasi akibat proses autentikasi yang lebih ketat, keterbatasan kompetensi teknis SDM keamanan, serta biaya implementasi yang tinggi hingga perlunya integrasi kompleks dengan sistem legacy yang sudah berjalan puluhan tahun. Selain itu, ditemukan bahwa beberapa institusi menghadapi tantangan regulasi, kesulitan dalam konsolidasi sistem manajemen identitas, serta kebutuhan harmonisasi kebijakan internal untuk mendukung proses transformasi keamanan. Studi ini memberikan rekomendasi strategis berupa perlunya audit infrastruktur secara komprehensif, peningkatan kompetensi teknis melalui pelatihan berkelanjutan, perencanaan roadmap Zero Trust yang realistis, serta migrasi bertahap yang berfokus pada aset prioritas tinggi. Temuan ini memberikan kontribusi praktis bagi lembaga finansial dengan menyoroti strategi implementasi yang dapat memperkuat postur keamanan dan meningkatkan ketahanan organisasi terhadap ancaman siber yang terus berkembang.

Corresponding Author:
Ardian Fachreza
Universitas Wahid Hasyim
Email: ardian.fachreza@unwahas.ac.id

PENDAHULUAN

Industri perbankan dan fintech telah mengalami transformasi digital yang berlangsung secara eksponensial dalam satu dekade terakhir, didorong oleh perubahan mendasar dalam perilaku konsumen yang kini mengharapkan layanan keuangan instan, personal, dan dapat diakses kapan saja dari perangkat mobile. Transformasi ini dipercepat pula oleh munculnya pelaku pasar baru khususnya perusahaan fintech yang berbasis teknologi yang menawarkan alternatif layanan tanpa beban infrastruktur fisik, sehingga menciptakan tekanan kompetitif yang memaksa institusi keuangan tradisional untuk beradaptasi atau menghadapi risiko disintermediasi. Akibatnya, layanan keuangan kini tidak lagi terbatas pada transaksi fisik di kantor cabang, melainkan telah bergeser secara radikal ke platform digital yang menuntut ketersediaan 24/7, skalabilitas tinggi, serta integrasi yang mulus antara sistem internal, mitra eksternal, penyedia layanan cloud, dan ekosistem pembayaran terbuka seperti *open banking*. Digitalisasi ini membawa tuntutan baru terhadap arsitektur teknologi: sistem tidak hanya harus

cepat dan responsif terhadap permintaan pengguna, tetapi juga dirancang sejak awal dengan prinsip *security-by-design* dan *privacy-by-default*, serta mampu beradaptasi secara dinamis terhadap ancaman siber yang terus berevolusi dalam kompleksitas dan modus operandinya.

Industri perbankan dan fintech telah mengalami transformasi digital yang berlangsung secara eksponensial dalam satu dekade terakhir, didorong oleh perubahan perilaku konsumen yang kini mengharapkan layanan keuangan instan dan digital (Williams, 2023). Layanan keuangan kini tidak lagi terbatas pada transaksi fisik di kantor cabang, melainkan telah bergeser ke platform digital yang menuntut ketersediaan 24/7, skalabilitas tinggi, serta integrasi yang mulus antara sistem internal, mitra eksternal, dan infrastruktur berbasis cloud (Smith, 2022). Digitalisasi ini membawa tuntutan baru terhadap arsitektur teknologi: sistem harus tidak hanya cepat dan responsif, tetapi juga dirancang dengan prinsip *security-by-design* (Rose, 2020).

Namun, di balik kemudahan, efisiensi, dan inovasi yang ditawarkan oleh transformasi digital tersebut, percepatan adopsi teknologi terutama dalam penggunaan API terbuka, komputasi awan, dan kerja jarak jauh secara tidak langsung memperluas *attack surface*, yaitu seluruh titik potensial yang dapat dieksploitasi oleh aktor jahat. Permukaan serangan kini tidak lagi terbatas pada batas jaringan fisik, melainkan mencakup antarmuka pengguna yang rentan terhadap rekayasa sosial, antarmuka pemrograman aplikasi (API) yang kurang diamankan, perangkat karyawan yang terhubung dari jaringan tidak tepercaya, hingga integrasi dengan pihak ketiga seperti vendor teknologi, mitra pembayaran, atau penyedia layanan analitik yang mungkin tidak menerapkan standar keamanan siber yang setara (Chen, 2021). Dalam konteks ini, model keamanan tradisional yang berakar pada asumsi bahwa segala sesuatu di dalam perimeter jaringan (seperti firewall, jaringan internal, atau data center milik perusahaan) secara otomatis bersifat tepercaya sering dikiasakan sebagai strategi castle-and-moat security telah terbukti rentan dan tidak lagi relevan dalam menghadapi ancaman modern. Serangan siber kontemporer, seperti pencurian kredensial melalui phishing canggih, eksploitasi kesalahan konfigurasi pada lingkungan cloud, atau infiltrasi diam-diam oleh aktor internal (insider threat), justru sering kali berhasil bukan karena kelemahan teknis ekstrem, melainkan karena adanya asumsi kepercayaan otomatis terhadap entitas yang telah melewati batas perimeter.

Sebagai respons strategis terhadap keterbatasan mendasar dari paradigma keamanan lama, Zero Trust Protocol hadir bukan sekadar sebagai sekumpulan alat atau solusi teknis, melainkan sebagai pergeseran paradigmatik yang merevolusi cara organisasi memahami, mengelola, dan menerapkan kepercayaan dalam ekosistem digital (Kindervag, 2020). Paradigma Zero Trust secara eksplisit menolak asumsi bahwa lokasi geografis, kepemilikan jaringan, atau status keanggotaan dalam domain internal memberikan hak akses otomatis. Sebaliknya, ia menegaskan prinsip fundamental: "never trust, always verify" bahwa setiap permintaan akses terhadap sumber daya digital, tanpa memandang asalnya (internal maupun eksternal), harus melalui proses verifikasi eksplisit, otorisasi berbasis konteks, dan penerapan prinsip *least privilege* yang ketat. Dalam praktiknya, Zero Trust menekankan tiga pilar arsitektural utama: pertama, verifikasi berkelanjutan yang mengevaluasi identitas pengguna, integritas perangkat, lokasi geografis, status keamanan jaringan, serta risiko perilaku secara real-time; kedua, segmentasi mikro yang membagi jaringan menjadi domain keamanan kecil untuk membatasi pergerakan lateral (*lateral movement*) jika terjadi pelanggaran; dan ketiga,

kontrol akses berbasis identitas dan kebijakan dinamis yang diberlakukan secara konsisten di seluruh lingkungan, baik yang bersifat *on-premise*, cloud publik, maupun hybrid.

Meskipun konsep Zero Trust menawarkan janji peningkatan postur keamanan yang signifikan terutama bagi sektor yang mengelola aset dan data paling sensitif, seperti rekening nasabah, riwayat transaksi, dan informasi identitas pribadi (KYC) proses implementasinya di sektor perbankan dan fintech tidak dapat dilakukan secara instan, seragam, atau bersifat *one-size-fits-all*. Adopsi Zero Trust menghadapi hambatan struktural, teknis, maupun manusiawi yang saling terkait. Di sisi teknis, banyak institusi keuangan masih sangat bergantung pada sistem legacy seperti core banking berusia puluhan tahun yang tidak dirancang untuk mendukung integrasi identitas terpusat, enkripsi end-to-end, atau otorisasi berbasis atribut. Di sisi operasional, kerumitan ekosistem bisnis yang melibatkan ratusan mitra, vendor, dan pihak ketiga menciptakan tantangan dalam menyelaraskan kebijakan keamanan dan memastikan konsistensi penerapan prinsip Zero Trust di seluruh rantai nilai. Di sisi regulasi, sektor keuangan beroperasi di bawah pengawasan ketat dari otoritas seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia, yang mewajibkan kepatuhan terhadap berbagai standar keamanan seperti POJK tentang manajemen risiko TI, standar PCI-DSS untuk pembayaran, atau ISO/IEC 27001 sehingga setiap perubahan arsitektur keamanan harus melalui proses validasi dan harmonisasi yang panjang. Serangan siber modern, seperti peretasan berbasis identitas atau *insider threat*, sering kali berhasil karena celah yang muncul dari kepercayaan buta terhadap entitas internal (National Institute of Standards and Technology, 2020).

Lebih dari sekadar tantangan teknis dan regulasi, keberhasilan penerapan Zero Trust pada akhirnya bergantung pada dimensi manusia dan organisasi. Diperlukan ketersediaan sumber daya manusia yang tidak hanya menguasai teknologi keamanan modern, tetapi juga mampu menjembatani kebutuhan bisnis dan keamanan. Diperlukan pula kematangan budaya organisasi yang siap menerima perubahan mendasar dalam cara kerja seperti penerimaan atas autentikasi berlapis, pembatasan akses berbasis kebutuhan, atau pengawasan aktivitas digital yang lebih ketat tanpa mengganggu produktivitas atau moral karyawan. Dan yang paling krusial, diperlukan dukungan strategis dan komitmen berkelanjutan dari pimpinan tertinggi, karena transformasi menuju Zero Trust adalah investasi jangka panjang yang memerlukan alokasi anggaran, realokasi sumber daya, serta visi keamanan yang menyatu dengan strategi bisnis inti. Meskipun menjanjikan peningkatan keamanan, implementasinya di sektor finansial menghadapi tantangan kompleks, termasuk ketergantungan pada sistem legacy, kerumitan ekosistem bisnis, serta tuntutan regulasi ketat dari otoritas seperti OJK dan Bank Indonesia (Taylor, 2019). Keberhasilan penerapan Zero Trust juga bergantung pada ketersediaan SDM kompeten, kematangan budaya organisasi, dan dukungan pimpinan puncak (Deloitte, 2023).

Oleh karena itu, penelitian ini bertujuan untuk menggali secara mendalam tantangan internal dan subjektif yang dihadapi organisasi keuangan baik bank maupun fintech dalam upaya menerapkan paradigma Zero Trust. Dengan menggunakan pendekatan fenomenologi, studi ini tidak hanya mencatat hambatan teknis atau kebijakan, tetapi berfokus pada pengalaman hidup, persepsi, emosi, dan narasi personal para praktisi keamanan siber yang berada di garis depan transformasi ini. Melalui wawancara mendalam, penelitian ini berusaha memahami: bagaimana praktisi memaknai konsep Zero Trust dalam konteks organisasi mereka; apa arti “kepercayaan” dan “keamanan” setelah asumsi lama dirombak; bagaimana

mereka bernegosiasi antara tuntutan keamanan dan tekanan bisnis; serta bentuk perlawanan, adaptasi, atau strategi koping apa yang mereka kembangkan dalam menghadapi kompleksitas implementasi. Dengan demikian, temuan penelitian ini diharapkan tidak hanya memberikan wawasan praktis bagi institusi keuangan yang sedang atau akan memulai perjalanan Zero Trust, tetapi juga memberikan kontribusi teoretis terhadap pemahaman tentang bagaimana perubahan paradigmatik dalam keamanan siber dialami, ditafsirkan, dan diintegrasikan ke dalam kehidupan organisasi yang nyata. Oleh karena itu, penelitian ini bertujuan memahami tantangan internal tersebut melalui perspektif para praktisi keamanan, dengan pendekatan fenomenologi untuk menggali makna pengalaman mereka dalam mengimplementasikan Zero Trust.

METODE PENELITIAN

Penelitian ini menggunakan desain penelitian kualitatif dengan pendekatan fenomenologi interpretatif (interpretative phenomenological analysis/ IPA), yang secara khusus dirancang untuk menggali, memahami, dan menginterpretasikan makna pengalaman hidup (lived experience) dari individu yang secara langsung terlibat dalam suatu fenomena tertentu. Dalam konteks studi ini, fenomena yang diteliti adalah proses implementasi Zero Trust Protocol di lingkungan organisasi keuangan, dan fokus utamanya adalah pada pengalaman subjektif, persepsi, emosi, serta interpretasi personal para praktisi keamanan siber yang berperan sebagai aktor kunci dalam transformasi keamanan tersebut. Pendekatan fenomenologi dipilih karena kemampuannya untuk menangkap kompleksitas pengalaman manusia dalam konteks sosial-organisasional yang nyata, di mana kebermaknaan suatu kebijakan teknis seperti Zero Trust tidak hanya ditentukan oleh aspek teknologis, tetapi juga oleh cara individu memahami, merasakan, dan bernegosiasi dengannya dalam praktik sehari-hari.

Untuk memastikan kedalaman dan relevansi data, peneliti memilih enam informan yang berasal dari latar belakang institusi keuangan yang beragam, meliputi bank umum (baik BUKU III maupun BUKU IV), bank digital, serta perusahaan fintech yang telah beroperasi minimal selama tiga tahun dan sedang dalam proses adopsi atau implementasi prinsip-prinsip Zero Trust. Pemilihan informan dilakukan melalui teknik purposive sampling, yaitu strategi seleksi partisipan berdasarkan kriteria spesifik yang relevan dengan tujuan penelitian. Kriteria inklusi meliputi: (1) memiliki peran langsung dalam perencanaan, pengelolaan, atau eksekusi strategi keamanan siber di organisasi; (2) terlibat aktif dalam proyek yang terkait dengan migrasi ke arsitektur keamanan modern; dan (3) bersedia berbagi pengalaman secara terbuka dan reflektif selama proses wawancara. Pendekatan ini memungkinkan peneliti untuk memperoleh data yang kaya, mendalam, dan kontekstual, sesuai dengan prinsip dasar penelitian kualitatif yang menekankan kualitas daripada kuantitas data.

Pengumpulan data primer dilakukan melalui wawancara mendalam (in-depth interview) yang berlangsung antara 60 hingga 90 menit per sesi, dengan format daring (video conference) untuk memudahkan aksesibilitas dan kenyamanan informan. Wawancara menggunakan panduan semi-terstruktur yang telah dikembangkan berdasarkan tinjauan literatur dan pertanyaan penelitian utama. Panduan tersebut mencakup sejumlah pertanyaan inti yang bersifat terbuka, seperti: “Bagaimana Anda pertama kali memahami konsep Zero

Trust?", "Apa tantangan paling berat yang Anda alami dalam menerapkannya di organisasi Anda?", "Bagaimana rekan kerja atau manajemen merespons perubahan ini?", dan "Apa makna pribadi dari transformasi keamanan ini bagi Anda sebagai praktisi?". Fleksibilitas dalam panduan semi-terstruktur memungkinkan peneliti untuk mengeksplorasi respons informan secara lebih mendalam melalui pertanyaan lanjutan (probing), sehingga memunculkan narasi yang autentik, reflektif, dan kaya akan detail kontekstual.

Setelah transkripsi wawancara selesai, proses analisis data dilakukan secara iteratif dan reflektif melalui pendekatan tematic analysis yang selaras dengan tradisi fenomenologi. Tahapan analisis dimulai dengan immersion peneliti membaca berulang kali setiap transkrip untuk memahami keseluruhan narasi. Selanjutnya, peneliti melakukan open coding, yaitu memberi label pada segmen data yang mengandung makna penting terkait pengalaman implementasi Zero Trust. Kode-kode awal kemudian dikelompokkan melalui axial coding menjadi kategori yang lebih luas, dan akhirnya dikonsolidasikan menjadi tema-tema inti melalui selective coding. Proses ini bertujuan untuk mengidentifikasi pola, kontradiksi, dan nuansa dalam pengalaman responden, serta mengungkap struktur makna yang mendasari persepsi mereka terhadap tantangan, harapan, dan transformasi organisasi dalam konteks Zero Trust.

Untuk menjaga kredibilitas dan keabsahan data yang dalam penelitian kualitatif menggantikan konsep validitas dan reliabilitas dalam penelitian kuantitatif peneliti menerapkan dua strategi utama: triangulasi sumber dan member checking. Triangulasi sumber dilakukan dengan membandingkan narasi dari informan yang berasal dari latar belakang organisasi berbeda (bank konvensional vs. fintech, institusi besar vs. menengah), sehingga memungkinkan identifikasi kesamaan dan perbedaan perspektif yang memperkaya analisis. Sementara itu, member checking dilakukan dengan mengembalikan ringkasan temuan atau transkrip interpretatif kepada informan untuk verifikasi: apakah interpretasi peneliti sesuai dengan pengalaman dan maksud asli mereka. Langkah ini tidak hanya meningkatkan keakuratan interpretasi, tetapi juga menghormati suara partisipan sebagai pemilik pengalaman.

Secara keseluruhan, pendekatan fenomenologi memberikan ruang epistemologis yang memadai untuk mengeksplorasi dimensi manusia di balik transformasi teknologi. Melalui lensa ini, penelitian ini tidak hanya melihat Zero Trust sebagai kerangka arsitektur keamanan, tetapi sebagai proses sosio-teknis yang melibatkan negosiasi makna, konflik nilai, adaptasi budaya, dan perubahan identitas profesional. Dengan demikian, studi ini berkontribusi pada pemahaman yang lebih holistik tentang bagaimana inovasi keamanan siber benar-benar dihayati, dijalani, dan ditafsirkan oleh mereka yang bertanggung jawab mengimplementasikannya di garis depan.

HASIL DAN PEMBAHASAN

Penelitian ini mengungkap lima tema utama yang merepresentasikan tantangan mendalam dalam implementasi Zero Trust Protocol di sektor perbankan dan fintech. Tema-tema tersebut tidak hanya mencerminkan hambatan teknis, tetapi juga konflik nilai, ketegangan organisasi, dan pergeseran identitas profesional yang dialami para praktisi. Kelima tema tersebut adalah: (1) *Beban Warisan Sistem Legacy*, (2) *Benturan antara Keamanan dan*

Kecepatan Bisnis, (3) *Krisis Makna dalam Budaya Kepercayaan Lama*, (4) *Ketimpangan Kompetensi dan Ketergantungan Eksternal*, serta (5) *Regulasi sebagai Pedang Bermata Dua*. Masing-masing tema dijelaskan berikut ini.

1. Beban Warisan Sistem Legacy: "Kami Ingin Maju, Tapi Kaki Terikat Rantai Lama"

Hampir semua informan menggambarkan sistem legacy sebagai penghambat utama dalam mewujudkan arsitektur Zero Trust. Sistem inti perbankan (core banking) yang telah beroperasi selama puluhan tahun sering kali dibangun pada era sebelum internet tidak dirancang untuk mendukung prinsip seperti autentikasi berbasis konteks, enkripsi end-to-end, atau integrasi API yang aman. Salah satu praktisi dari bank BUKU IV menyatakan:

> *"Kami punya sistem yang usianya lebih tua dari saya. Zero Trust butuh identitas terpusat, tapi sistem lama ini bahkan tidak punya konsep 'user' semua akses berbasis IP statis. Migrasi penuh? Butuh waktu bertahun-tahun dan anggaran yang mustahil dipertanggungjawabkan."*

Kondisi ini menciptakan dilema struktural: di satu sisi, organisasi dituntut untuk berinovasi dan memperkuat keamanan; di sisi lain, mereka terikat pada infrastruktur yang menjadi tulang punggung operasional harian. Akibatnya, banyak institusi memilih pendekatan *workaround* seperti membangun lapisan keamanan di sekitar sistem lama yang justru bertentangan dengan semangat Zero Trust yang menuntut verifikasi di setiap titik akses.

2. Benturan antara Keamanan dan Kecepatan Bisnis: "Tim Keamanan Dianggap Rem, Bukan Gas"

Sebuah pola kuat yang muncul dari narasi informan adalah ketegangan antara fungsi keamanan dan fungsi bisnis. Dalam budaya organisasi yang berorientasi pada kecepatan peluncuran produk (time-to-market), tim keamanan sering kali dipandang sebagai penghambat. Seorang praktisi dari perusahaan fintech mengungkapkan:

> *"Setiap kali saya minta penundaan rilis karena celah keamanan, manajemen bilang, 'Ini bukan bank, kita harus cepat!' Tapi ketika terjadi insiden, semua mata tertuju pada saya. Zero Trust butuh kolaborasi sejak awal, tapi kami baru diajak bicara saat sistem sudah hampir live."*

Fenomena ini menunjukkan bahwa Zero Trust bukan hanya masalah teknologi, tapi juga masalah posisi sosial dan otoritas dalam organisasi. Keberhasilannya bergantung pada kemampuan praktisi keamanan untuk mengkomunikasikan nilai keamanan sebagai enabler bisnis, bukan hanya sebagai fungsi kontrol.

3. Krisis Makna dalam Budaya Kepercayaan Lama: "Dulu Kita Percaya, Sekarang Kita Curiga"

Salah satu tantangan paling halus namun paling dalam adalah perubahan paradigma budaya. Selama puluhan tahun, budaya organisasi perbankan dibangun di atas prinsip kepercayaan internal: karyawan yang telah melewati seleksi ketat dianggap dapat dipercaya. Zero Trust, dengan prinsip "*never trust, always verify*", secara tidak langsung menggoyahkan fondasi budaya tersebut. Seorang CISO bank swasta menggambarkan resistensi psikologis yang muncul:

Ada yang bilang,

"Kami sudah 20 tahun di sini, kenapa sekarang harus login MFA setiap kali buka sistem?' Ini bukan soal teknologi, tapi soal harga diri. Mereka merasa tidak dipercaya."

Tantangan ini menunjukkan bahwa transformasi keamanan juga merupakan transformasi budaya. Keberhasilan Zero Trust memerlukan kampanye perubahan makna: mengganti narasi "kami curiga pada Anda" menjadi "kami melindungi Anda dan institusi ini dari ancaman yang tak terlihat".

4. Ketimpangan Kompetensi dan Ketergantungan Eksternal: "Kami Tahu Apa yang Harus Dilakukan, Tapi Tidak Punya Orangnya"

Meskipun semua informan memahami prinsip dasar Zero Trust, kesenjangan antara pengetahuan dan kapasitas eksekusi sangat nyata. Banyak organisasi keuangan, terutama yang berskala menengah, mengalami krisis talenta keamanan siber. Mereka kesulitan merekrut tenaga ahli yang memahami arsitektur Zero Trust, IAM modern, atau segmentasi mikro. Akibatnya, mereka terpaksa mengandalkan konsultan eksternal atau vendor teknologi, yang justru menciptakan ketergantungan baru:

"Kami beli solusi Zero Trust dari vendor A, tapi tim internal tidak paham konfigurasinya. Kalau ada masalah, harus tunggu mereka datang. Ini bukan penguasaan teknologi, ini outsourcing keamanan," keluh seorang praktisi.

Kondisi ini menggarisbawahi bahwa teknologi Zero Trust tanpa kapasitas internal yang memadai justru menciptakan kerentanan baru bukan hanya teknis, tetapi juga operasional dan strategis.

5. Regulasi sebagai Pedang Bermata Dua: "Aturan Melindungi, Tapi Juga Mengikat"

Informan secara konsisten menyebut bahwa regulasi dari OJK dan Bank Indonesia memainkan peran ganda. Di satu sisi, regulasi mendorong peningkatan keamanan dan memberikan dasar legitimasi bagi inisiatif Zero Trust. Di sisi lain, proses sertifikasi dan audit yang panjang sering kali memperlambat eksperimen dan inovasi. Salah satu praktisi menggambarkan:

"Kami ingin uji coba ZTNA untuk sistem HR, tapi harus menunggu persetujuan audit TI dulu. Sementara itu, ancaman tidak menunggu. Regulasi penting, tapi kadang terasa seperti membangun pesawat sambil terbang, dengan tangan diikat."

Fenomena ini menunjukkan bahwa implementasi Zero Trust di Indonesia tidak bisa dipisahkan dari konteks tata kelola keuangan yang sangat terawasi. Keberhasilan memerlukan dialog proaktif dengan regulator, bukan hanya kepatuhan pasif.

KESIMPULAN

Penelitian ini menunjukkan bahwa penerapan Zero Trust Protocol pada sektor perbankan dan fintech merupakan proses transformasional yang jauh melampaui perubahan arsitektur teknologi semata. Melalui pendekatan fenomenologi, penelitian ini berhasil mengungkap bagaimana para praktisi keamanan siber mengalami Zero Trust sebagai sebuah

dinamika yang kompleks, penuh tarik menarik antara kebutuhan bisnis, tekanan regulasi, dan realitas teknis yang sering kali tidak ideal. Para praktisi memaknai Zero Trust sebagai upaya rekonstruksi ulang konsep "kepercayaan" dalam organisasi, di mana asumsi keamanan yang sebelumnya bergantung pada perimeter kini harus diredefinisi menjadi verifikasi berkelanjutan berbasis identitas, konteks, dan risiko. Tantangan yang muncul tidak hanya berasal dari infrastruktur lama (legacy systems) yang sulit diintegrasikan, tetapi juga dari resistensi budaya terhadap kontrol yang lebih ketat, keterbatasan kompetensi SDM, serta ketidaksinkronan kebijakan keamanan antar unit bisnis. Dengan demikian, Zero Trust bukanlah perubahan yang bersifat linier, melainkan perjalanan berlapis yang membutuhkan adaptasi terus-menerus, dialog lintas fungsi, dan penerjemahan konsep teknis ke dalam praktik organisasi yang dapat diterima oleh seluruh pemangku kepentingan. Temuan ini menegaskan bahwa keberhasilan Zero Trust ditentukan oleh kemampuan organisasi untuk menggabungkan kesiapan teknis, kematangan budaya, kapasitas reflektif, serta komitmen strategis dari pimpinan dalam jangka panjang.

Berdasarkan dinamika kompleks yang teridentifikasi, penelitian ini merekomendasikan agar institusi keuangan mengadopsi strategi implementasi Zero Trust yang bersifat holistik, bertahap, dan berpusat pada manusia. Organisasi perlu memulai dengan audit menyeluruh yang tidak hanya menilai kesiapan teknologi, tetapi juga memetakan pola pikir, resistensi, dan kebutuhan pelatihan dari setiap unit kerja. Narasi internal mengenai Zero Trust perlu diubah dari "pembatasan akses" menjadi "peningkatan perlindungan aset kritis," sehingga tercipta dukungan psikologis dan emosional dari karyawan terhadap perubahan yang dilakukan. Pemerintah dan regulator seperti OJK dan Bank Indonesia disarankan untuk menyediakan kerangka regulasi adaptif misalnya melalui regulatory sandbox keamanan—agar institusi dapat melakukan eksperimen Zero Trust tanpa tekanan kepatuhan yang kaku. Di tingkat teknis, organisasi perlu menetapkan peta jalan implementasi secara bertahap, dimulai dari 2295elol berisiko tinggi, memperkuat integrasi identitas, dan mengadopsi segmentasi mikro secara modular. Selain itu, investasi jangka 2295elola2295 dalam pengembangan SDM, kolaborasi dengan akademisi dan 2295elola2295y keamanan, serta penyusunan tata 2295elola lintas fungsi menjadi kunci agar Zero Trust berkembang dari sekadar proyek teknologi menjadi budaya keamanan yang mengakar dan berkelanjutan dalam organisasi. Dengan pendekatan demikian, transformasi Zero Trust diharapkan mampu meningkatkan postur keamanan secara signifikan tanpa menghambat inovasi maupun kelincahan bisnis yang sangat dibutuhkan di era digital.

DAFTAR PUSTAKA

Chen. (2021). Expanding attack surfaces in cloud-enabled financial systems. *Journal of Cybersecurity Research*, 9(1), 33–49.

Deloitte. (2023). The State of Zero Trust in Financial Services. *Deloitte Cybersecurity Insights Report*.

Kindervag. (2020). No more chewy centers: Introducing the Zero Trust model. *Forrester Research*.

National Institute of Standards and Technology. (2020). *Zero Trust Architecture*, NIST SP 800-207.

Rose, B. M. (2020). Zero Trust Architecture (NIST Special Publication 800-207). *National Institute of Standards and Technology*, (Dokumen resmi Zero Trust dari NIST).

Smith. (2022). Cloud-driven integration in modern financial services: Challenges and opportunities. *International Journal of Digital Finance*, 8(2), 101–118.

Taylor. (2019). Cybersecurity regulation in the financial services industry. *Journal of Financial Regulation*, 5(2), 210–229.

Williams. (2023). Digital transformation in banking: Navigating the shift to customer-centric financial services. *Journal of Financial Innovation*, 12(3), 45–62.