Satu Perangkat Rusak, 128 Bank Lumpuh: Pelajaran untuk Perbankan Indonesia

Oleh: Yoda Pralandono – email: dryapralandono@gmail.com
(*Mahasiswa Doktoral Manajemen Teknologi, Institut Teknologi Sepuluh Nopember, Surabaya*)

Pekan lalu, tidak ada peretas yang membobol bank di Jepang maupun Indonesia. Namun ribuan kantor cabang berhenti melayani dan nasabah tak bisa menyentuh uangnya. Itulah pelajaran yang paling mudah dilupakan: ancaman terbesar bagi bank digital bukan selalu musuh dari luar, tetapi titik rapuh di dalam sistemnya sendiri.

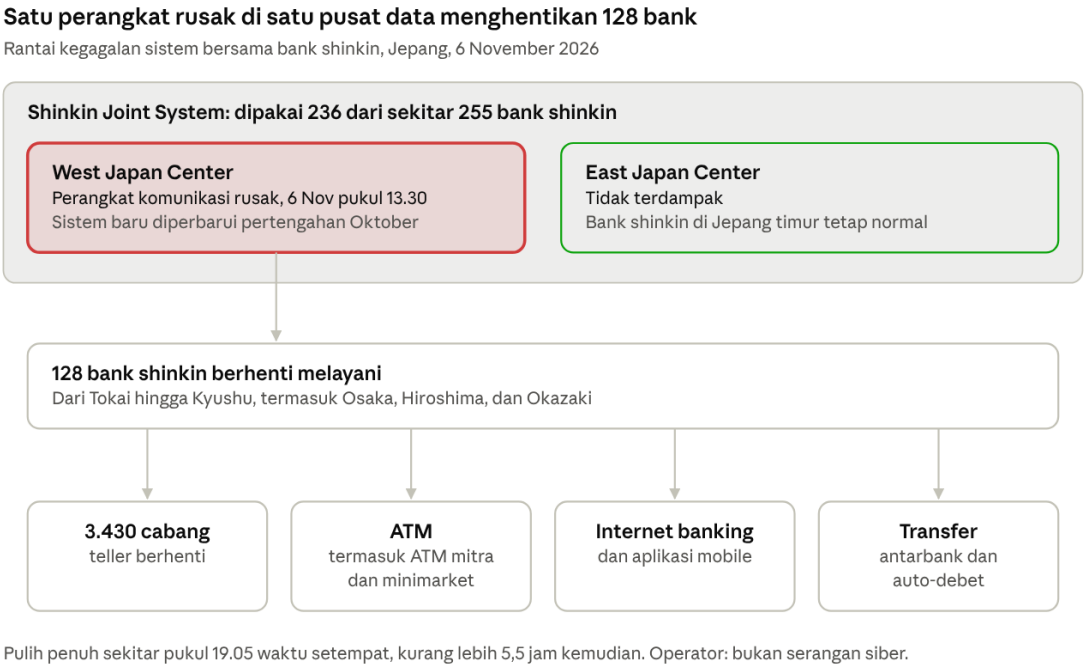
Jumat siang, 6 November 2026, sekitar pukul 13.30 waktu Jepang, layanan transaksi di 128 bank shinkin di Jepang bagian barat berhenti [1], [2]. Nasabah tidak bisa menarik maupun menyetor uang tunai di ATM, termasuk di Osaka, Hiroshima, dan Okazaki [3]. Transaksi di loket 3.430 kantor cabang terhenti, dan internet banking ikut lumpuh [2]. Penyebabnya bukan serangan siber, melainkan kerusakan perangkat komunikasi di pusat data Jepang bagian barat [1], [3].

Jumat sore, menjelang akhir pekan, adalah waktu terburuk bagi ATM untuk mati. Empat hari sebelumnya, nasabah sebuah bank swasta nasional di Indonesia juga mengeluhkan hambatan transfer dan pembatasan penarikan tunai di kantor cabang [4].

Dua peristiwa ini berbeda sebab, tetapi mengirim pesan yang sama. Di era ketika hampir semua transaksi berlangsung lewat layar, **ketersediaan layanan adalah bentuk keamanan yang paling dirasakan nasabah**. Bank yang tidak bisa diakses, bagi orang yang membutuhkan uangnya hari itu, sama buruknya dengan bank yang diretas.

Apa yang terjadi di Jepang

Kegagalan ini bukan soal 128 bank yang masing-masing rusak, melainkan satu sistem bersama yang berhenti. Platform bersama Shinkin Joint System melayani 236 dari sekitar 255 bank shinkin di Jepang, dan arsitekturnya dibagi ke dua pusat data, satu untuk Jepang timur dan satu untuk Jepang barat [1].



Gambar 1. Rantai kegagalan sistem bersama bank shinkin. Ilustrasi penulis berdasarkan [1]–[3], [7], [8].

Gangguan hanya mengenai jaringan barat, sementara bank yang memakai jaringan timur tetap beroperasi normal [5]. Pada pukul 15.00, operator menyelesaikan pemeriksaan awal, menemukan kerusakan fisik jaringan, dan menyatakan tidak ada peretasan [6]. Sistem bank shinkin di Jepang barat baru diperbarui pada pertengahan Oktober [7], dan laporan awal TV Asahi mengaitkan gangguan dengan kegagalan perangkat setelah pembaruan sistem ATM [8]. Hingga kini, vendor perangkat yang rusak, mekanisme kegagalan, dan kinerja sistem cadangan belum diungkap ke publik [1], [8].

Seluruh layanan pulih sesaat setelah pukul 19.00 waktu setempat [3]. Pelajaran pentingnya: efisiensi sistem bersama juga menciptakan kerentanan bersama. Kasus serupa pernah terjadi di Amerika Serikat: pada Januari 2025, gangguan listrik dan kerusakan perangkat keras di penyedia teknologi FIS mengganggu layanan sejumlah lembaga, termasuk Capital One, dan FIS menyatakan gangguan itu tidak terkait serangan siber [9].

Jejak gangguan: pola yang terus berulang

Insiden Jepang bukan anomali. Dalam tiga setengah tahun terakhir, gangguan besar perbankan di Indonesia dan dunia lebih sering bersumber dari kegagalan teknis, pembaruan sistem, atau vendor, daripada dari peretas.



Gambar 2. Jejak gangguan layanan perbankan 2023–2026. Ilustrasi penulis berdasarkan [1], [4], [9]–[16].

Serangan siber tetap yang paling ditakuti: gangguan BSI pada Mei 2023 sempat diduga akibat ransomware [10] dan berlangsung hingga empat hari [11]. Namun daftar gangguan lain lebih panjang. Pembaruan perangkat lunak CrowdStrike yang cacat pada Juli 2024 mengganggu layanan Barclays, HSBC, Bank of America, Wells Fargo, dan JPMorgan Chase [12]. Gangguan listrik dan perangkat keras di vendor FIS pada Januari 2025 mengganggu layanan Capital One [9]. Laporan stabilitas keuangan IMF bahkan mencatat satu insiden di penyedia layanan cloud pada 2023 yang memadamkan 60 credit union di Amerika Serikat secara bersamaan [17]. Bagi nasabah, ancaman nyata adalah apa pun yang membuat uang tak bisa diakses, apa pun penyebabnya.

Gambar 2 menyusun delapan gangguan secara kronologis dari atas ke bawah, mulai Mei 2023 hingga November 2026. Setiap titik mewakili satu kasus, dan warnanya menunjukkan penyebab menurut pengelola atau laporan media. Merah berarti diduga serangan siber, kuning berarti penyebab belum diumumkan, dan abu-abu berarti kegagalan teknis yang dinyatakan bukan serangan. Pita abu-abu di bagian bawah menandai dua gangguan yang terjadi pekan lalu.

Ada tiga temuan dari gambar ini. **Pertama, enam dari delapan kasus berwarna abu-abu.** Hanya gangguan BSI pada 2023 yang diduga terkait ransomware [10], dan hanya Bank Jambi yang penyebabnya belum diumumkan karena layanan ditutup untuk audit forensik [15]. Sisanya dinyatakan sebagai kendala sistem

atau kegagalan perangkat, mulai dari pembaruan perangkat lunak CrowdStrike [12], gangguan listrik dan perangkat keras di FIS [9], kendala sistem BCA [14], hingga kerusakan perangkat komunikasi di pusat data bank shinkin [1].

Kedua, separuh kasus teknis berasal dari luar bank. CrowdStrike, FIS, dan pusat data bersama bank shinkin adalah pihak ketiga atau infrastruktur bersama [1], [9], [12]. Artinya, bank yang sistem internalnya sehat tetap bisa lumpuh karena masalah di vendor atau mitra yang dipakai bersama.

Ketiga, jarak antarkejadian makin rapat. Dalam gambar ini, kasus pertama dan kedua terpisah 14 bulan, sedangkan dua kasus terakhir hanya terpisah empat hari. Temuan ini perlu dibaca hati-hati: Gambar 2 adalah pilihan kasus yang diberitakan luas, bukan daftar lengkap semua gangguan. Label "teknis" juga merujuk pada versi pengelola. Pada kasus Bank DKI, misalnya, gangguan yang berulang membuat pemerintah provinsi melaporkannya ke Bareskrim [15].

Daftar bank terdampak, dalam dan luar negeri

Tabel berikut merangkum bank yang terdampak gangguan pekan lalu dan kasus sebanding sebelumnya. Penyebab dicantumkan sesuai pernyataan pengelola atau laporan media, tanpa penilaian penulis.

Negara	Bank atau lembaga terdampak	Waktu	Layanan terdampak	Penyebab menurut pengelola atau laporan	Ref.
Jepang	Okazaki Shinkin Bank (Aichi), Osaka City Shinkin Bank (Osaka), Hiroshima Shinkin Bank (Hiroshima)	6 Nov 2026	Tarik dan setor tunai di ATM	Kerusakan perangkat keras; bukan serangan siber	[3]
Jepang	Osaka Shinkin Bank, Nara Shinkin Bank	6 Nov 2026	Transaksi loket, ATM	Kerusakan perangkat komunikasi di West Japan Center	[2]
Jepang	Gifu Shinkin Bank	6 Nov 2026	ATM, internet banking, aplikasi, sebagian layanan loket	Gangguan sistem bersama; investigasi berjalan	[18]
Jepang	Chunichi Shinkin Bank	6 Nov 2026	Transaksi cabang, ATM, internet banking, Densai Net	Gangguan sistem sementara	[19]
Jepang	Total: 128 bank shinkin, 3.430 cabang; ATM mitra	6 Nov 2026	Loket, ATM, internet banking, auto-debet	Kerusakan perangkat komunikasi; tidak ada akses tanpa izin	[2], [7]

Negara	Bank atau lembaga terdampak	Waktu	Layanan terdampak	Penyebab menurut pengelola atau laporan	Ref.
	dan minimarket ikut terdampak				
Indonesia	MNC Bank	Sejak 2 Nov 2026	Aplikasi mobile banking, transfer, QRIS; nasabah melaporkan pembatasan tarik tunai di cabang	Pemulihan layanan digital; bank membantah masalah likuiditas	[4], [16], [20]
Indonesia	Bank Syariah Indonesia (BSI)	Mei 2023	Mobile banking; ATM dan cabang sempat terganggu	Diduga ransomware	[10], [11]
Global	Barclays, HSBC, Bank of America, Wells Fargo, JPMorgan Chase	Jul 2024	Pemrosesan pembayaran, akses layanan perbankan	Pembaruan perangkat lunak CrowdStrike yang cacat	[12]
Amerika Serikat	Capital One dan lembaga lain pengguna FIS	Jan 2025	Akses setoran langsung, pemrosesan pembayaran	Gangguan listrik dan perangkat keras vendor; bukan serangan siber	[9]
Indonesia	Bank DKI	30 Mar–7 Apr 2025	ATM, mobile banking, QRIS	Manajemen menyatakan tidak ada serangan peretas	[13], [15]
Indonesia	Bank Central Asia (BCA)	29 Sep 2025	myBCA, BCA mobile, transfer, QRIS, top up Flazz	Kendala sistem	[14]
Indonesia	Bank Jambi	Feb 2026	ATM dan mobile banking ditutup sementara	Audit forensik; penyebab belum diumumkan	[15]

Ulasan daftar bank terdampak

Tabel di atas memperlihatkan dua wajah gangguan pekan lalu. Di Jepang, gangguan bersifat luas: satu kejadian mengenai 128 bank di banyak prefektur sekaligus, dari Aichi, Osaka, Nara, dan Hiroshima hingga

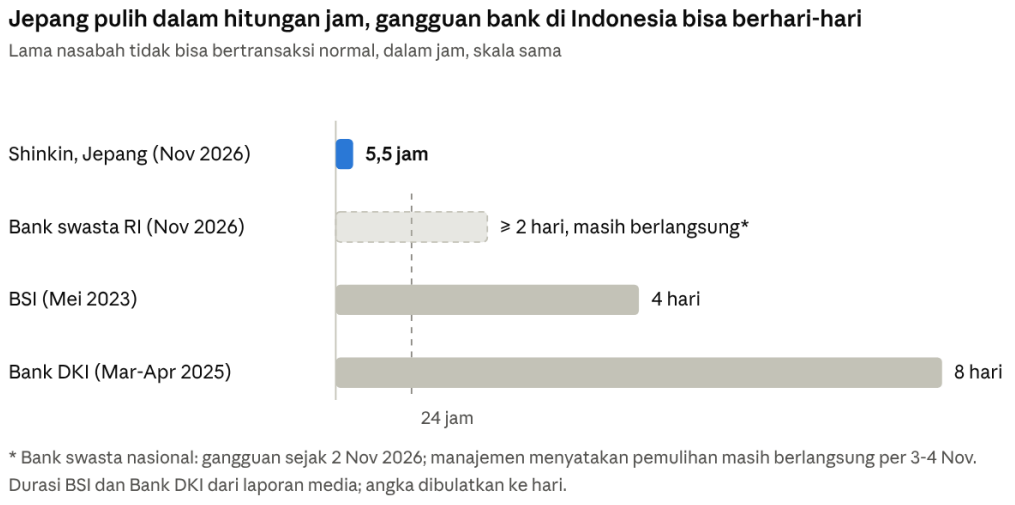
Gifu [2], [3], [18]. Di Indonesia, gangguan bersifat dalam: hanya satu bank, tetapi pemulihannya belum tuntas berhari-hari [21]. Keduanya sama-sama merugikan, dengan cara yang berbeda.

Kolom layanan terdampak menunjukkan bahwa kanal fisik ternyata bergantung pada sistem digital yang sama. Di Jepang, bukan hanya internet banking yang berhenti; transaksi di loket dan ATM juga ikut lumpuh [2]. Dampaknya bahkan meluas ke luar bank itu sendiri: ATM mitra, ATM di minimarket, dan auto-debet ikut terganggu [7]. Di Indonesia, QRIS muncul di tiga baris, yakni Bank DKI, BCA, dan bank swasta nasional [13], [14], [20]. Hal ini mencerminkan betapa luasnya ekosistem pembayaran yang bergantung pada satu aplikasi bank.

Tabel ini juga menunjukkan bahwa ukuran bank bukan jaminan kekebalan. Bank-bank global terbesar seperti Barclays, HSBC, Bank of America, Wells Fargo, dan JPMorgan Chase ikut terganggu ketika satu vendor keamanan merilis pembaruan yang cacat [12]. Di Indonesia, gangguan menimpa beragam jenis bank: bank syariah, bank pembangunan daerah, dan bank swasta besar [10], [13]–[15]. Dari 12 baris, hanya satu yang penyebabnya diduga serangan siber [10]. Pesan utamanya: daftar risiko bank tidak boleh berhenti pada peretas.

Berapa lama nasabah terputus

Perbedaan terbesar antara Jepang dan kasus-kasus di Indonesia bukan pada penyebab, tetapi pada lama pemulihan.



Gambar 3. Lama gangguan layanan. Data dari [3], [9], [11], [13], [21].

Gangguan di Jepang berlangsung sekitar lima setengah jam [9]. Gangguan BSI berlangsung hingga empat hari [11], dan layanan digital Bank DKI terganggu dari 30 Maret hingga 7 April 2025 [13]. Untuk bank swasta nasional yang terdampak pekan lalu, manajemen menyatakan pemulihan layanan digital masih berlangsung per 4 November tanpa kepastian waktu normal [21]. Garis 24 jam di grafik adalah pegangan yang masuk akal: lewat dari itu, gangguan teknis mulai berubah menjadi krisis kepercayaan.

Membaca Gambar 3

Gambar 3 membandingkan lama gangguan empat kasus dalam satuan jam dengan skala yang sama, sehingga panjang batang bisa dibandingkan langsung. Batang biru adalah gangguan bank shinkin, sekitar 5,5 jam [9]. Batang putus-putus adalah bank swasta nasional; panjangnya hanya batas bawah, yaitu sedikitnya dua hari, karena pemulihan masih berlangsung saat data terakhir tersedia [21]. Batang BSI mewakili sekitar empat hari atau 96 jam [11], dan Bank DKI sekitar delapan hari atau 192 jam [13]. Garis putus-putus vertikal menandai batas 24 jam sebagai pembanding.

Selisihnya mencolok. Berdasarkan angka tersebut, gangguan BSI kira-kira 17 kali lebih lama daripada gangguan di Jepang, dan gangguan Bank DKI kira-kira 35 kali lebih lama. Hanya kasus Jepang yang selesai di bawah garis 24 jam.

Salah satu penjelasan yang mungkin adalah kecepatan diagnosis. Di Jepang, operator menemukan kerusakan fisik jaringan dan menyingkirkan dugaan peretasan sekitar satu setengah jam setelah gangguan dimulai [6]; pusat data timur juga tetap berjalan [5]. Penyebab yang cepat diketahui membuat perbaikan lebih terarah. Sebaliknya, kasus yang diduga serangan siber atau memerlukan audit forensik cenderung butuh waktu lebih lama untuk dipulihkan dengan aman [10], [15]. Ini adalah tafsiran penulis, bukan kesimpulan resmi pengelola.

Ada dua keterbatasan data. Durasi diambil dari laporan media, dan definisi "pulih" bisa berbeda antarkasus: sebagian layanan, seperti ATM atau cabang, kerap kembali lebih dulu daripada aplikasi. Meski begitu, gambaran besarnya jelas: bagi nasabah, perbedaan antara hitungan jam dan hitungan hari adalah perbedaan antara ketidaknyamanan dan krisis. Konsep *impact tolerance* yang dipakai regulator Inggris lahir dari logika yang sama, yakni menetapkan batas gangguan sebelum kerugian nasabah tidak lagi dapat dipulihkan [28].

Mengapa Indonesia harus waspada

Indonesia kini sangat bergantung pada layar. Bank Indonesia mencatat **48,98 miliar transaksi pembayaran digital** dalam sembilan bulan pertama 2026, naik 38,28% secara tahunan, dan aplikasi wondr by BNI saja telah mencapai 16,6 juta pengguna [22]. Semakin besar ketergantungan, semakin mahal setiap menit gangguan.

Gangguan di sebuah bank swasta nasional pekan lalu memperlihatkan bagaimana kendala teknis bisa cepat berubah menjadi krisis kepercayaan. Nasabah melaporkan tidak bisa memakai layanan tarik tunai, QRIS, maupun transfer melalui aplikasi bank tersebut [20]. Bank membantah gangguan dipicu masalah likuiditas dan menyebutnya kendala yang sedang dipulihkan [16]. Namun hingga 3 November, manajemen belum memberi penjelasan teknis terperinci maupun kepastian waktu pemulihan [20]. Otoritas Jasa Keuangan (OJK) kemudian menegaskan bahwa gangguan itu bukan disebabkan masalah solvabilitas [23], sekaligus meminta bank menyiapkan langkah konkret untuk memulihkan layanan dan memenuhi hak nasabah [24].

Waktunya pun genting. Pada pekan yang sama, sektor perbankan, keuangan, dan asuransi tercatat sebagai sasaran aktivitas serangan siber tertinggi di Indonesia, sekitar 761.000 aktivitas [25]. Pemantauan lain mencatat sekitar 999.000 serangan ke sektor ini dalam 24 jam [26]. Badan Siber dan Sandi Negara

(BSSN) membentuk Tim Tanggap Insiden Siber (TTIS) sektor keuangan, dan OJK meminta bank siaga 24 jam [25]. OJK dan Bank Indonesia telah mengaktifkan TTIS sejak 6 November 2026 [27].

Ada pula kemiripan struktural dengan Jepang. Bank shinkin adalah lembaga keuangan kecil yang berbagi satu sistem inti; di Indonesia, padanannya adalah BPR dan bank daerah. Anggota Komisi XI DPR, Hasanuddin Wahid, mendesak OJK membentuk pusat pemantauan keamanan siber bersama untuk melindungi BPR, BPRS, dan BPD [27]. Pelajaran dari Jepang menambahkan satu catatan: pusat bersama memang efisien, tetapi juga bisa menjadi satu titik yang menjatuhkan semuanya sekaligus.

Solusi: dari "jangan sampai diretas" ke "jangan sampai berhenti"

Pelajaran dari Jepang dan Jakarta bisa diringkas menjadi lima langkah. Masing-masing menjawab satu titik rapuh yang terlihat pekan lalu.

1. **Bank: tetapkan batas waktu padam yang bisa ditoleransi.** Basel Committee on Banking Supervision meminta bank memperhitungkan toleransi gangguan dalam kerangka ketahanan operasionalnya, sejalan dengan konsep *impact tolerance* regulator Inggris [28]. Di Uni Eropa, Digital Operational Resilience Act (DORA) mewajibkan program pengujian ketahanan operasional digital sebagai bagian dari manajemen risiko TIK [29]. Untuk layanan penting seperti tarik tunai, transfer, dan QRIS, batas ini perlu ditetapkan, diuji, dan dipenuhi.
2. **Bank: uji sistem cadangan sungguhan, bukan di atas kertas.** Peninjauan internal di Jepang kini berfokus pada penggantian perangkat yang rusak dan pemeriksaan protokol yang seharusnya mengalihkan layanan ke server cadangan [6]. Latihan failover harus rutin, termasuk bersama vendor dan bank lain yang memakai infrastruktur yang sama.
3. **Vendor dan bank: disiplin saat memperbarui sistem.** Sistem bank shinkin di Jepang barat baru diperbarui pada pertengahan Oktober, beberapa pekan sebelum gangguan [7]. Pembaruan sebaiknya dilakukan bertahap, dengan rencana kembali ke versi lama, dan tidak menjelang periode transaksi puncak.
4. **Regulator: awasi risiko konsentrasi.** Ketentuan ketahanan digital OJK sudah mewajibkan bank melakukan uji penetrasi, simulasi serangan siber, dan audit TI [30]. Langkah berikutnya adalah memetakan penyedia teknologi yang dipakai bersama oleh banyak bank, terutama BPR dan BPD, lalu menuntut cadangan yang benar-benar independen. Pusat pemantauan siber bersama yang diusulkan DPR [27] harus dirancang tanpa satu titik kegagalan.
5. **Bank dan regulator: komunikasi cepat dan jujur.** Di Jepang, pengelola sistem segera menyampaikan permohonan maaf, menegaskan bukan serangan siber, dan memulihkan layanan di hari yang sama [3]. OJK juga telah berkoordinasi dengan personel TI seluruh bank dan mengirim surat berisi langkah preventif kepada direksi [31]. Aturan praktis bagi bank: dalam satu jam, jelaskan layanan apa yang terganggu, kanal apa yang masih bisa dipakai, dan kapan informasi berikutnya keluar.

Untuk nasabah, ada tiga kebiasaan sederhana. Pertama, jangan simpan seluruh dana di satu bank atau satu aplikasi; punya rekening cadangan di bank lain. Kedua, simpan sedikit uang tunai untuk keadaan darurat. Ketiga, waspadai penipuan: saat layanan terganggu, penipu sering menyamar sebagai petugas bank. Bank tidak pernah meminta PIN atau kode OTP.

Kesimpulan: ukur bank dari seberapa cepat bank bisa bangkit

Selama ini kita menilai keamanan bank dari satu pertanyaan: bisakah bank diretas? Pekan lalu memberi pertanyaan kedua yang sama penting: **berapa lama bank bisa berhenti beroperasi, dan seberapa cepat bank bisa bangkit?** Jepang menjawabnya dalam sekitar lima setengah jam [9], dengan penjelasan terbuka. Itu bukan prestasi, tetapi setidaknya batas yang jelas.

Indonesia punya modal yang baik: aturan siber OJK, tim tanggap insiden yang sudah aktif, dan industri yang tumbuh cepat. Yang belum ada adalah kebiasaan memperlakukan gangguan teknis seserius serangan peretas. Tanpa itu, pertumbuhan transaksi digital justru memperbesar taruhan.

Ingat rumus sederhananya: **satu titik rapuh, ribuan nasabah terdampak; satu jam tanpa penjelasan, satu hari rumor.** Bank yang membangun cadangan sebelum dibutuhkan, menguji sebelum dipaksa, dan berbicara sebelum ditanya adalah bank yang akan tetap dipercaya, saat perangkat berikutnya rusak.

Referensi

Format IEEE. Seluruh tautan diakses pada 13 November 2026. Rujukan [1]–[9], [16], [18]–[27], [30], dan [31] terbit dalam satu bulan terakhir; rujukan lain dipakai untuk kasus historis dan kerangka regulasi.

[1] Glitchwire, "Communications failure knocks out ATMs and banking at 128 Japanese credit unions," *Glitchwire*, Nov. 2026. [Online]. Available: https://glitchwire.com/news/communications-failure-knocks-out-atms-and-banking-at-128-japanese-credit-unions/

[2] Insider Paper, "Japan banking outage hits 128 banks, disrupts 3,430 branches," *Insider Paper*, Nov. 6, 2026. [Online]. Available: https://insiderpaper.com/japan-banking-outage-hits-128-banks-disrupts-3430-branches/

[3] Liputan6.com, "Sistem ATM di 128 bank Jepang lumpuh, pengelola: Bukan serangan siber," *Liputan6.com*, Nov. 7, 2026. [Online]. Available: https://www.liputan6.com/bisnis/read/8330495/sistem-atm-di-128-bank-jepang-lumpuh-pengelola-bukan-serangan-siber

[4] CNBC Indonesia, "Kronologi nasabah MNC Bank sulit tarik dana hingga disorot OJK-BEI," *CNBC Indonesia*, Nov. 8, 2026. [Online]. Available: https://www.cnbcindonesia.com/market/20261108180830-17-783310/kronologi-nasabah-mnc-bank-sulit-tarik-dana-hingga-disorot-ojk-bei

[5] Indonesiakini, "Gangguan sistem hentikan layanan 128 bank regional Jepang," *Indonesiakini.id*, Nov. 9, 2026. [Online]. Available: https://indonesiakini.id/2026/11/09/gangguan-sistem-hentikan-layanan-128-bank-regional-jepang/

[6] L. H. Costa, "128 Shinkin banks in western Japan lose ATMs and counters after failure," *Mix Vale*, Nov. 6, 2026. [Online]. Available: https://www.mixvale.com.br/2026/11/06/128-shinkin-banks-in-western-japan-lose-atms-and-counters-after/

[7] BigGo Finance, "Japan's Shinkin Joint Center outage halts ATMs, counters at 128 Shinkin banks in western Japan," *BigGo Finance*, Nov. 6, 2026. [Online]. Available: https://finance.biggo.com/news/bd0e17d1-4053-4933-84db-72953ab524fe

[8] Mezha.net, "A shared system outage halted ATMs at 128 credit cooperatives in Japan," *Mezha.net*, Nov. 2026. [Online]. Available: https://mezha.net/eng/news/03130571_a_shared_system_outage/

[9] J. Gapusan, "Over 100 banks disrupted: What the Shinkin outage teaches U.S. banks," *Forbes*, Nov. 9, 2026. [Online]. Available: https://www.forbes.com/sites/jeffgapusan/2026/11/09/over-100-banks-disrupted-what-the-shinkin-outage-teaches-us-banks/

[10] Bisnis.com, "Nasabah keluhkan BSI Mobile eror tiga hari, kena ransomware?," *Bisnis.com*, May 10, 2023. [Online]. Available: https://finansial.bisnis.com/read/20230510/231/1654509/nasabah-keluhkan-bsi-mobile-eror-tiga-hari-kena-ransomware

[11] Infobanknews, "Gangguan sampai 4 hari, BSI perkuat sistem keamanan siber," *Infobanknews*, May 2023. [Online]. Available: https://infobanknews.com/gangguan-sampai-4-hari-bsi-perkuat-sistem-keamanan-siber/

[12] Panax, "CrowdStrike outage: Lessons for finance leaders," *Panax*, Jul. 2024. [Online]. Available: https://www.panax.com/blog/crowdstrike-outage-lessons-for-finance-leaders

[13] Fortune IDN, "Layanan IT Bank DKI eror sejak Lebaran, pengamat: IT BPD masih lemah," *Fortune Indonesia*, Apr. 2025. [Online]. Available: https://www.fortuneidn.com/finance/layanan-it-bank-dki-eror-sejak-lebaran-pengamat-it-bpd-masih-lemah-00-ccw2k-rfwcm5

[14] Republika, "Aplikasi myBCA dan BCA Mobile sudah pulih usai gangguan pagi ini," *Republika*, Sep. 29, 2025. [Online]. Available: https://ekonomi.republika.co.id/berita/t3c0rj370/aplikasi-mybca-dan-bca-mobile-sudah-pulih-usai-gangguan-pagi-ini

[15] Bisnis.com, "Gangguan sistem layanan kembali 'hantui' bank daerah," *Bisnis.com*, Feb. 24, 2026. [Online]. Available: https://finansial.bisnis.com/read/20260224/90/1955276/gangguan-sistem-layanan-kembali-hantui-bank-daerah

[16] Periskop.id, "MNC Bank bantah gangguan MotionBank akibat masalah likuiditas," *Periskop.id*, Nov. 3, 2026. [Online]. Available: https://periskop.id/perbankan/20261103/mnc-bank-gangguan-motionbank

[17] IDM, "Rising cyber threats heighten financial stability risks, IMF warns," *Information & Data Manager*, Apr. 2024. [Online]. Available: https://idm.net.au/node/14718

[18] Cedar News, "Japan bank outage hits 128 Shinkin banks, disrupting ATMs and branch transactions," *Cedar News*, Nov. 6, 2026. [Online]. Available: https://cedarnews.net/newstasks/1117704/japan-bank-outage-hits-128-shinkin-banks-disrupting-atms-and-branch-transactions/

[19] Kumparan, "128 bank di Jepang gangguan dan ATM-internet banking sempat lumpuh, kena serangan siber?," *Kumparan*, Nov. 8, 2026. [Online]. Available: https://kumparan.com/kumparantekno/128-bank-di-jepang-gangguan-dan-atm-internet-banking-sempat-lumpuh-kena-serangan-siber-28WeCKyNRnl

[20] Generasi.co, "MNC Bank akui layanan digital masih dipulihkan, nasabah keluhkan akses dana," *Generasi.co*, Nov. 3, 2026. [Online]. Available: https://generasi.co/ekonomi/mnc-bank-akui-layanan-digital-masih-dipulihkan-nasabah-keluhkan-akses-dana/

[21] S. A. Bannar, "Nasabah MNC Bank keluhkan sulit tarik uang, OJK turun tangan," *Topik.id*, Nov. 4, 2026. [Online]. Available: https://www.topik.id/nasabah-mnc-bank-keluhkan-sulit-tarik-uang-ojk-turun-tangan

[22] Demokratis, "Transaksi digital BTN, BNI dan Mandiri tumbuh pesat pada 2026," *Demokratis.co.id*, Nov. 2026. [Online]. Available: https://demokratis.co.id/transaksi-digital-bank-tumbuh-2026

[23] Monitor Indonesia, "Nasabah MNC Bank tak bisa transfer, tarik tunai dibatasi Rp2 juta," *Monitor Indonesia*, Nov. 4, 2026. [Online]. Available: https://monitorindonesia.com/ekonomi/read/2026/11/638057/nasabah-mnc-bank-tak-bisa-transfer-tarik-tunai-dibatasi-rp2-juta

[24] Liputan6.com, "OJK minta MNC Bank segera pulihkan layanan dan hak nasabah," *Liputan6.com*, Nov. 5, 2026. [Online]. Available: https://www.liputan6.com/bisnis/read/8329312/ojk-minta-mnc-bank-segera-pulihkan-layanan-dan-hak-nasabah

[25] Kompas.com, "Perbankan jadi target utama serangan siber, BSSN dan OJK minta bank siaga 24 jam," *Kompas.com*, Nov. 10, 2026. [Online]. Available: https://tekno.kompas.com/read/2026/11/10/13450067/perbankan-jadi-target-utama-serangan-siber-bssn-dan-ojk-minta-bank-siaga-24-jam

[26] H. A. Pasya, "Ratusan ribu serangan siber targetkan perbankan di Indonesia, OJK imbau bank-bank siaga dari ancaman hacker," *tvOnenews.com*, Nov. 10, 2026. [Online]. Available: https://www.tvonenews.com/berita/nasional/477475-ratusan-ribu-serangan-siber-targetkan-perbankan-di-indonesia-ojk-imbau-bank-bank-siaga-dari-ancaman-hacker

[27] Kompas.com, "Serangan siber di sektor keuangan, anggota dewan desak OJK lindungi BPR dan bank daerah," *Kompas.com*, Nov. 11, 2026. [Online]. Available: https://nasional.kompas.com/read/2026/11/11/11385711/serangan-siber-di-sektor-keuangan-anggota-dewan-desak-ojk-lindungi-bpr-dan

[28] Protiviti, "Supervisory authorities and Basel Committee refine operational resilience approaches, align on expectations for firms," *Protiviti Insights*, 2021. [Online]. Available: https://www.protiviti.com/gl-en/blogs/supervisory-authorities-and-basel-committee

[29] DLA Piper, "Application of the Digital Operational Resilience Act (DORA): Key considerations," *DLA Piper Insights*, Feb. 28, 2025. [Online]. Available: https://www.dlapiper.com/en/insights/publications/2025/02/application-of-the-digital-operational-resilience-act---dora

[30] E. Nordiansyah, "OJK peringatkan bank soal ancaman serangan siber, masyarakat diimbau tenang," *Medcom.id*, Nov. 10, 2026. [Online]. Available: https://www.medcom.id/ekonomi/bisnis/MkM51XVk-ojk-peringatkan-bank-soal-ancaman-serangan-siber-masyarakat-diimbau-tenang

[31] Kompas.id, "Bagaimana bank melawan serangan siber?," *Kompas.id*, Nov. 2026. [Online]. Available: https://www.kompas.id/artikel/bagaimana-bank-melawan-serangan-siber

Biodata Penulis:

Yoda Agung Pralandono, SE, MM, MSI adalah Mahasiswa **Doktoral Manajemen Teknologi, Institut Teknologi Sepuluh Nopember**, Surabaya. Selain itu sebagai professional bidang Teknologi Informasi di Bank Umum Nasional (**Bank Danamon Indonesia, Tbk as Assistant Vice President**) sekaligus sebagai **Dosen** di STIE Hidayatullah dan beberapa kampus swasta di Jabodetabek. Aktif memberikan kuliah mengenai IT, Banking dan Financial Management. Dapat dihubungi via WA 0815.183.2004 dan email: dryapralandono@gmail.com