Everpure

The new standard for banking resilience



Cyber resilience is measured by how well banks recover.

Executive summary

Cyber and operational resilience have become foundational requirements for modern banks. Regulators, boards, and customers now expect banks to demonstrate that critical services can withstand cyberattacks and other disruptions, recover within defined tolerances, and produce evidence of resilience on demand. Key considerations include:

Regulatory compliance.

Regulatory expectations such as DORA in Europe, CPS 230 in Australia, and evolving U.S. supervisory guidance are raising the bar for operational resilience and recoverability. Documenting operational resilience is no longer enough. Banks must demonstrate the ability to consistently meet defined recovery objectives and impact tolerances.

Customer trust.

Visible disruptions erode customer confidence when customers lose access to accounts, payments, or critical services. Ensuring consistent uptime, fast recovery, and clear communications during an incident can help alleviate concerns.

Cyber insurance leverage.

Insurers are tightening underwriting standards and scrutinizing resilience capabilities more closely. Maintaining a stronger, tested resilience architecture may support a better insurance posture.

Despite these clear priorities, significant gaps persist in core data and storage infrastructure across banks. As a result, resilience architectures are constrained by fragmented tooling, slow and unpredictable recovery, backup systems that have become ransomware targets, and limited ability to prove recoverability under real-world conditions and regulator-accepted timelines. The biggest cost is not the attack itself. It is the failure to recover clean, current data fast enough to restore critical operations.

In this dossier, we'll discuss the cyber risks facing banks today, the short- and long-term ramifications of an attack, and how operational resilience can help banks recover critical services, maintain trust, and prove control during disruption.





Cyberattacks put critical banking operations under pressure

Banks are not just frequent victims of cyberattacks; they are strategic targets where disruption has immediate operational and customer impact. According to the IMF's Global Financial Stability Report, nearly one-fifth of global cyber incidents target the financial sector, with banks among the most frequently attacked.

Bad actors are drawn to these institutions because they combine three high-value attributes: direct access to money, sensitive data, and a systemic importance to the global economy. A successful attack can halt transactions and block customer access. The longer a breach lasts, the greater the potential damage. The pressure to restore operations quickly is immense, making it more likely that banks will pay a ransom to regain control.

The financial industry isn't alone in being targeted by attackers. What makes the threat uniquely acute for banks is the intent and impact of a breach. Modern attacks are designed to maximize operational disruption by targeting identity systems, backup environments, and recovery workflows, effectively undermining the bank's ability to restore services. This shifts the challenge from preventing access to restoring clean, trusted data and critical services under pressure.

The implication is clear: Cyberattacks are now operational resilience events shaped by regulatory expectations around continuity, recoverability, and control.

According to the Global Financial Stability Report from the IMF[1], nearly one-fifth of global cyber incidents target the financial sector, with banks among the most frequently attacked institutions.



Resilience must be proven under pressure

Cyberattacks test a bank's resilience in real time. Recovery speed, and the ability to prove it, determine regulatory, customer, and market outcomes.



Regulatory impact:

Regulatory expectations such as DORA in Europe, CPS 230 in Australia, and evolving U.S. supervisory guidance are raising the bar for operational resilience and recoverability. Banks must prove recoverability, maintain data control, and produce audit-ready evidence on demand. Manual processes break down under scrutiny, making automated validation, regular testing, and evidence capture essential.



Customer and market impact:

Customers expect continuous access to critical banking services such as payments, core banking, fraud systems, and customer access. When recovery is delayed, disruption becomes customer-facing—driving negative press, eroding trust, and impacting revenue in real time. Reputation is defined by performance under pressure.

Can your bank prove recovery under scrutiny?

Ask your compliance lead:

What evidence do regulators/auditors request most often, and how long does it take to assemble it today?

Where do we currently struggle to prove recoverability (test artifacts, logs, chain of custody, retention, immutability)?

Ask your security lead:

How do we demonstrate that recovery copies remain protected during credential compromise or insider risk scenarios?

What would, "audit ready by default" look like for resilience evidence in our organization?

When was the last time we tested recovery under realistic cyberattack conditions?

Operating through a cyberattack with a Minimum Viable Bank model

During a cyberattack, the question is not whether every system can come back at once. It is whether the bank can keep its most critical services operating while it recovers safely.

A Minimum Viable Bank (MVB) model helps define the systems, data, dependencies, and recovery evidence required to maintain customer trust, reduce disruption, and restore with control.

The requirements necessary to achieve MVB include:

Continuous availability to ensure resilience mechanisms do not degrade production performance.

Predictable recovery across on-premises, hybrid, and cloud environments to demonstrate there are no performance gaps.

Immutable clean recovery copies to protect against alteration or deletion, including during credential compromise.

Dependency mapping across identities, network, application, and data layers to ensure critical systems are restored in the correct order.

Recovery testing and evidence to validate Recovery Time Objectives (RTOs) / Recovery Point Objectives (RPOs) performance under real conditions and logs and artifacts to demonstrate recovery ability.

Audit-ready evidence of recoverability to present during audits and reviews.

Can your bank operate at minimum viable service during an attack?

Ask your IT team:

Which services must stay available first?

Can we recover clean data without reinfection?

Do we know which dependencies could delay restoration?

Can we prove recovery is tested, controlled, and audit-ready?





Preparation defines MVB readiness



During a cyberattack, recovery speed depends on preparation. Banks need protected recovery data, isolated recovery environments, and regular testing to restore minimum viable services with confidence.

Protect recovery copies from compromise

Prevents attackers from encrypting, deleting, or tampering with recovery data.

Why it's important:

Ensure clean recovery data cannot be encrypted, deleted, or altered, even if privileged credentials are compromised.

Isolate recovery environments

Limits cyber blast radius and prevents lateral movement during incidents.

Why it's important:

Separate recovery from compromised production systems to limit blast radius, prevent reinfection, and support controlled restoration.

Test recovery under real conditions

Ensures RTO/RPO targets can be met under real-world conditions.

Why it's important:

Validate recovery time and recovery point targets regularly, using realistic operating conditions, dependencies, and pressure scenarios.

Together, these actions help banks prove that minimum viable services can be restored cleanly, predictably, and with evidence.



Recovery must be clean, isolated, and fast

During a disruption, recovery is not just about restoring data. Banks need to restore trusted services in the right order, from clean recovery copies, without spreading compromise back into production.

That requires more than backup. It requires protected recovery data, isolated validation, rapid restore paths, and evidence that recovery can be executed cleanly and consistently.

For security, infrastructure, risk, and audit teams, confidence comes from proving that restoration is controlled, repeatable, and ready for regulatory scrutiny.

Immutable Snapshot Recovery

Recover clean data from protected, immutable snapshots.

Clean Room Recovery

Validate systems safely before restoring production services.

Cyber Resilient Vault

Protect recovery data in an isolated recovery vault.

Production Rapid Restore

Restore priority banking services quickly and predictably.



Five ways recovery failure impacts banking confidence

1

Customers lose access to essential financial services[2]

When core services go down, customers cannot access funds, make payments, or complete transactions, driving immediate dissatisfaction. Prolonged outages can lead to customer attrition.

2

The issue becomes public (news, socials)[3]

Negative news coverage can spread quickly, amplified by social media posts from frustrated customers. This can shape market perception before the bank can respond.

3

The bank does not appear to be in control[2]

Breakdowns in system integrity and data isolation can expose gaps in core controls. External scrutiny may reinforce the perception that the institution is not in control.

4

Regulators require banks to provide evidence[2]

Regulatory bodies such as the Federal Reserve, DORA, and UK Financial Conduct Authority require auditable proof of impact, containment, and recovery. Evidence that is delayed or incomplete may increase scrutiny.

5

Trust erodes across customers and the market[2]

Doubts about system reliability and data integrity may persist beyond the incident, weakening the bank's reputation. Market confidence may weaken as operational risk and leadership credibility are reassessed.

Everpure helps banks restore critical service faster, protect recovery data, and prove recovery is predictable and controlled.

Can your bank contain the impact of a disruption?

Ask your IT team:

If a critical service failed today, which customers, markets, and operations would feel it first?

Where would fragmented recovery workflows slow down response or increase risk?

Everpure helps banks reduce the business impact of disruption

When recovery breaks down, the impact extends beyond IT. Customer access, payment continuity, regulatory confidence, and market trust can all be affected.

Everpure helps banks protect recovery data, restore critical services faster, and produce evidence that recovery is clean, tested, and controlled.

Deterministic recovery

Predictable recovery performance that meets defined RTO / RPO targets under real-world failure conditions

Rapid restore and failover for Tier 0 and Tier 1 banking systems

Recommended Everpure products:

FlashArray™
FlashBlade®
SafeMode™ Snapshots
ActiveDR™

Operational resilience by design

Immutable recovery copies that cannot be altered or deleted, even by privileged users

Isolation of recovery environments to limit cyber and operational blast radius

Recommended Everpure products:

SafeMode™ Snapshots
FlashBlade®
FlashArray™
Portworx®

Unified recovery & evidence platform

Single platform for protection, recovery, testing, and audit evidence

Integrated recovery validation to prove resilience before incidents occur

Recommended Everpure products:

FlashBlade®
FlashArray™
Pure1®
Portworx®

Take action to build your bank's resilience

Recovery readiness cannot wait for an incident. Banks should identify the services that must remain available, validate recovery paths, and ensure they can prove control before disruption occurs.

Recommended next steps

1. Evaluate your bank's resilience assumptions using the guidance and questions in this dossier.
2. Identify critical services and recovery dependencies to ensure your organization is prepared to restore in the correct order.
3. Assess whether your current environment can prove control, recovery, and data trustworthiness.
4. Contact an Everpure representative to learn more about resilient solutions for your bank.

Visit Our Website | 800.379.PURE

Everpure

©2026 Everpure, the Everpure P Logo, Pure Storage, Portworx, and the marks in the Everpure Trademark List are trademarks or registered trademarks of Everpure, Inc. or its licensed subsidiaries in the U.S. and/or other countries. The Trademark List can be found at everpuredata.com/trademarks. Other names may be trademarks of their respective owners.

Sources:
1. Global Financial Stability Report, International Monetary Fund, April 2024
2. UK lawmakers question Lloyds over account glitch that exposure customers' details, Reuters, March 17, 2026
3. From compliance to excellence: Elevating risk management practices, McKinsey & Company, December 2024