Everpure

Cyber resilience in banking: Building the Minimum Viable Bank

Prepare, protect, and restore critical banking services with confidence

Ponemon Institute research shows that 36% of stored data is mission-critical[1], yet recovery takes 12 days on average after a data security incident.

This brief explains why legacy recovery models fall short in banking, what Minimum Viable Bank (MVB) means in practice, and what banks must do to stay operational under pressure.

Executive summary

Banks operate in a true zero-failure environment; any disruption to critical applications or data can halt operations instantly. Yet many institutions still rely on infrastructure-led recovery models designed for outages, not today's cyber threats. That mismatch is now a growing risk. As attacks increasingly target data, resilience can no longer be defined by how quickly systems come back online. It requires a cyber-resilient approach that ensures continuous access to clean, trusted data and the ability to maintain operations when it matters most.

Cyber resilience is no longer an IT initiative; it is a business capability that underpins continuity, compliance, and market confidence.

In this brief, you will learn why traditional recovery models are falling short in banking, what Minimum Viable Bank means in practice, and how banks can build a modern, data-centric resilience strategy for today's threat landscape. The brief applies key findings from the Ponemon Institute's State of Cyber Resilience report to the banking resilience challenge. We'll also share perspective from Michael Russo, Senior Director, Global Alliance Partnerships, Financial Services, at Everpure, and Rob Glanzman, Global Strategic Alliances Principal Architect, Financial Services, at Everpure.

Mission-critical application recovery takes 12 days on average, too long to sustain core banking operations[2].

31% of total attack costs are tied to recovering clean, current data, making data integrity the primary driver of recovery success[2].

Only 41% of organizations are confident managing data across environments, exposing a critical gap in hybrid and multi-cloud resilience[2].

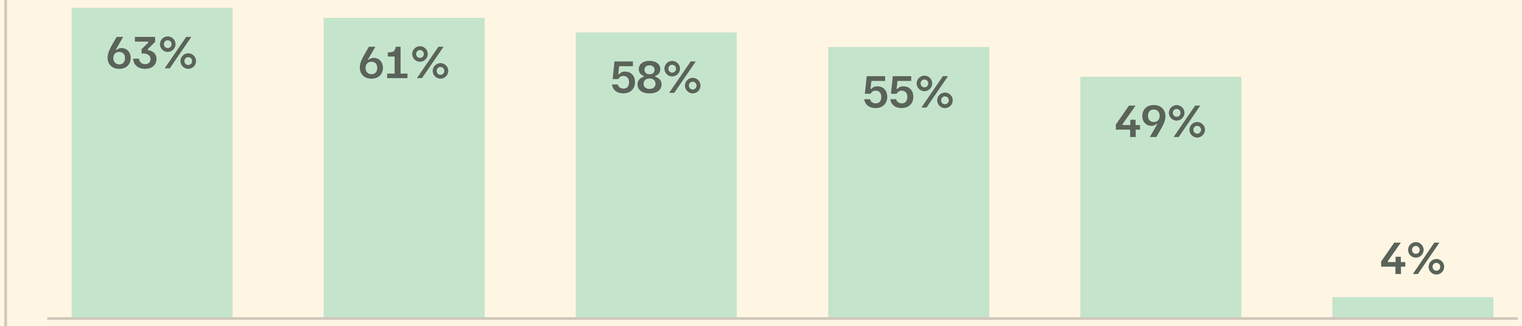
Cyberattacks are increasing in frequency and impact

High-value transactions and deeply interconnected ecosystems make banks a prime target for bad actors, and successful breaches are on the rise as attacks become both more creative and sophisticated. Ransomware remains the best known form factor, but it's not the only threat. Attackers use phishing or smishing to steal credentials, gaining access to the network. With all these and more threats at hand, banks must operate under the assumption that both their production and recovery environments may be compromised.

The impact of a successful breach is immediate and operational. Services are frozen, impacting customers and the market. Disruption doesn't just delay processes—it halts payments, interrupts market activity, and puts the bank's ability to operate at risk in real time. Major attacks cost millions, with recovery as the largest driver of that cost. More critically, restoring mission-critical applications can take nearly two weeks—far beyond what core banking operations can sustain. Every hour of delay compounds exposure.

Extended recovery timelines increase regulatory scrutiny, trigger financial penalties, and amplify reputational damage. In a highly regulated industry, the inability to recover quickly and with confidence is not simply an operational failure—it is a business and systemic risk with broad market implications.

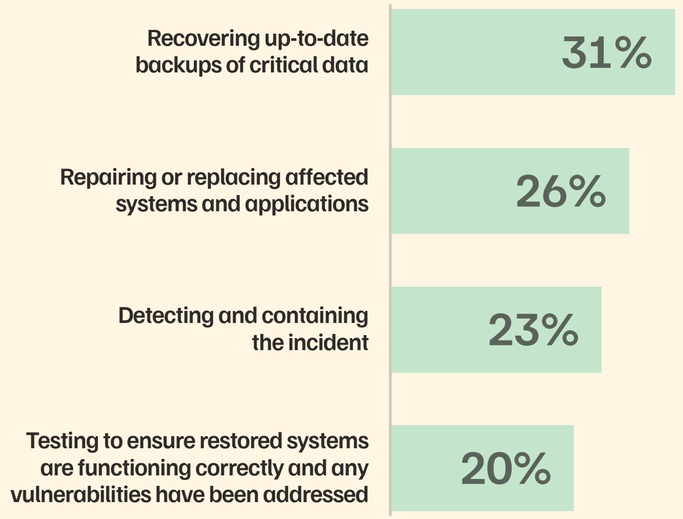
> "What most banks still think of as resilience—disaster recovery and failover—was built for outages, not cyberattacks. And that model no longer works."
>
> **Rob Glanzman, Global Strategic Alliances Principal Architect, Financial Services, Everpure**



Source: The State of Cyber Resilience, Ponemon Institute LLC, October 2025

Why recovery now starts with Minimum Viable Bank

A cyber event changes what recovery means for a bank. Recovering mission-critical applications can take an average of nearly two weeks[1], costing millions of dollars. A survey of IT and IT security practitioners across the United States reveals the top four costs of recovering from a cyberattack:



Source: The State of Cyber Resilience, Ponemon Institute LLC, October 2025

Traditional disaster recovery was built to restore everything from a stored backup. In a cyber event, that is not enough. Banks need to restore the critical services that keep the institution operating, starting with clean, trusted data and a recovery path they can validate under pressure.

This requires a fundamental shift in objectives. Traditional recovery focused on restoring everything as quickly as possible. Today, there's a better approach: the Minimum Viable Bank (MVB) recovery model. MVB prioritizes the rapid restoration of core operations from clean, immutable data—enabling banks to resume critical customer services and meet regulatory obligations in hours, not days, before full system recovery is complete.

Surveys show that 36% of data is considered mission critical[1]. Inability to access this data can prohibit basic commerce activities.

> "Everpure is focused on giving banks the confidence that they can recover their Minimum Viable Bank from clean data in hours, not days—and you can actually stand behind it."
>
> **Michael Russo, Senior Director Global Alliance Partnerships, Financial Services, Everpure**

The first step is identifying which operations are considered core, and which ones can be restored later in the process. This is a question for executive leadership and core IT staff to solve together, but considerations should include:

- **Core customer services**: Payments, account access, and digital channels must be restored first to maintain customer trust and continuity of service.
- **Regulatory requirements**: Recovery priorities must align with obligations to maintain critical services, meet disruption tolerances, and demonstrate resilience under stress.
- **Critical dependencies**: Foundational systems and data services must be restored first, as they enable all downstream applications and operations to come back online.

Everpure enables this shift by aligning recovery to business priorities, not infrastructure constraints. With access to clean, immutable data and built-in validation of recoverability, banks can restore critical services first, sustain operations through disruption, and prove resilience with confidence—meeting both operational demands and regulatory expectations.

Different regulations. Same pressure.

The Americas

- NYDFS Cybersecurity Regulation
- FFIEC operational resilience guidance
- OSFI B-13
- CNBV and Banxico cybersecurity and operational resilience oversight

Europe

- Digital Operational Resilience Act (DORA)
- European Banking Authority (EBA)
- NIS2 Directive
- Prudential Regulation Authority (PRA)

Asia/Pacific

- APRA CPS 230
- HKMA OR-2
- MAS Technology Risk Management Guidelines
- RBI IT Governance Directions
- Japan FSA resilience guidance

Africa

- South Africa Joint Standard 2 of 2024: Cybersecurity and Cyber Resilience Requirements
- Central Bank of Nigeria Risk-Based Cybersecurity Framework

Regulatory frameworks may differ across regions, but expectations are converging

While frameworks vary, the direction is consistent: Documented plans are no longer enough. Regulators worldwide require demonstrable proof that banks can maintain critical services and operate with confidence while recovering from an attack. This may include the provision of audit-ready evidence that resilience holds under real-world conditions.

In practice, this means demonstrating five non-negotiable capabilities:

Recoverability

Proven ability to restore critical services within defined timeframes. Not just as a plan, but as a validated outcome.

Clean, trusted data

Assurance that recovered data is accurate, current, and free from compromise.

Testing

Continuous validation of recovery processes under real-world conditions.

Evidence

Clear, auditable proof that resilience capabilities work as intended both before and during an incident.

Third-party control

Visibility and governance across vendors and dependencies to ensure external risk does not become operational failure.

While frameworks vary, the direction is consistent:

In Europe

Digital Operational Resilience Act (DORA)

DORA is raising the bar, requiring rigorous testing, formalized resilience programs, and stronger oversight of third-party risk.

Across Asia Pacific and Japan

Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 230

Standards such as APRA CPS 230 and Technology Risk Management guidance emphasize continuity of critical services, resilience through disruption, and tighter operational control across environments.

Across the Americas

Federal Financial Institutions Examination Council (FFIEC), Office of the Comptroller of the Currency (OCC), New York Department of Financial Services (NYDFS), Office of the Superintendent of Financial Institutions (OSFI)

The guidance from these institutions reinforces operational continuity, governance, and the ability to recover and sustain critical services under disruption.

Why choose Everpure

When critical banking services are down, the question is not whether you can get everything back eventually. It is whether you can restore the services that keep the bank running, from clean data, and prove it.

Everpure helps banks meet regulatory expectations by enabling recovery of critical services from clean, trusted data, with built-in validation and audit-ready evidence. Everpure supports this with immutable recovery copies, isolated recovery environments, continuous recovery validation, and evidence that can be used for audit and supervisory review.

This is supported by an ecosystem of resellers, global system integrators, managed service providers, and technology partners, including Commvault, helping banks implement and operate resilience strategies across regions with consistent outcomes.

Learn more

Sources:
1. Ponemon Institute, The State of Cyber Resilience, October 2025, p. 1.
2. Ponemon Institute, The State of Cyber Resilience, October 2025, p.2.

Visit Our Website | **800.379.PURE**

Everpure