TECH HIVE
ADVISORY

How
Ransomware Attacks
Disrupted BridgePay and Exposed Payment Infrastructure Risks

The recent disruption at BridgePay Network Solutions, a US payment gateway provider is a sobering reminder of how ransomware attacks on payment infrastructure can freeze real-world commerce in seconds. In the early hours of 6 February 2026, what began as degraded performance across gateway systems quickly escalated into a confirmed ransomware incident. Within hours, merchants across the country found themselves unable to process card payments, effectively cutting off their primary revenue stream.

Although early forensic investigations confirmed that no payment card data was compromised, the operational disruption had already taken its toll. Modern ransomware attacks do not rely solely on data theft to create impact. In highly interconnected payment environments, even limited system interference or containment measures can disrupt transaction processing at scale. For businesses that depend on seamless transaction processing, availability isn't just a technical metric, it is survival.

This incident highlights a critical shift in the nature of ransomware attacks. Modern threat actors are no longer focused solely on data theft. Instead, they are targeting availability and operational continuity, particularly within high-dependency sectors like financial services and payment processing. When a payment gateway goes offline, the consequences ripple outward—impacting retailers, service providers, consumers, and financial institutions simultaneously.

How ransomware attacks on payment infrastructure occur

Incidents like the BridgePay outage follow a predictable structure. Ransomware attacks rarely begin with encryption. Instead, attackers move methodically through several stages before triggering disruption.

Typically, the process involves:

- Gaining initial access through phishing, stolen credentials or exposed remote services.
- Escalating privileges to obtain administrative control.
- Conducting internal reconnaissance of APIs, gateways and backup systems.
- Disabling monitoring or security controls where possible.
- Deploying encryption across critical operational systems.

In payment environments, attackers prioritise systems that directly affect transaction processing. By targeting gateways and APIs, they maximise pressure without necessarily touching cardholder database.

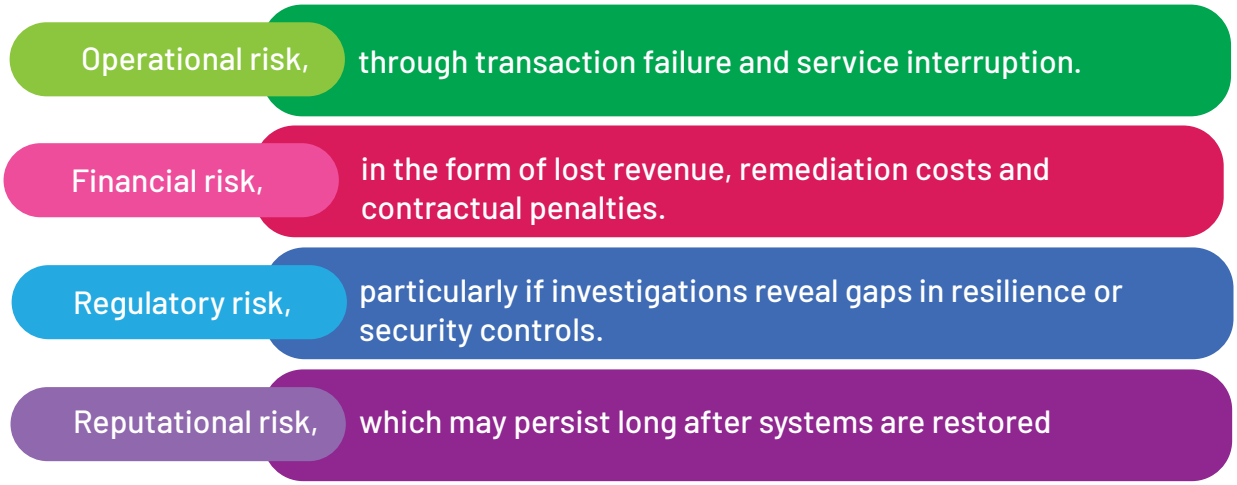
Why Payment Processors Are Prime Targets

Ransomware attacks on payment infrastructure are increasing because payment processors sit at a uniquely vulnerable intersection of urgency, interconnection and economic dependency. Unlike many other sectors, downtime in payment systems is not merely inconvenient it is commercially unsustainable. Merchants rely on continuous transaction processing, which means restoration becomes urgent within hours, not days.

Payment gateways are also deeply interconnected. APIs link retailers, software vendors, municipalities, financial institutions and service providers into a tightly integrated ecosystem. When a single gateway is compromised, the disruption does not remain contained. It ripples outward, affecting thousands of dependent entities simultaneously.

Attackers understand this dynamic. In infrastructure environments, encryption of operational systems can be as damaging as data exfiltration. Availability is often the most critical asset. By targeting gateway APIs, virtual terminals or transaction routing systems, threat actors create immediate economic pressure without necessarily stealing sensitive cardholder data.

The consequences extend far beyond technical failure. Even where no payment data is compromised, ransomware attacks on payment infrastructure generate layered risk, including:



TECH HIVE ADVISORY

The BridgePay incident illustrates this clearly. The disruption was not confined to one organisation; it spread across cities, businesses and service providers. In such cases, encryption itself becomes the crisis. When payment infrastructure is halted, commerce stalls and that is precisely the leverage attackers seek.

Preventing ransomware attacks on payment infrastructure

Preventing ransomware attacks on payment infrastructure requires far more than traditional endpoint protection or perimeter firewalls. Payment ecosystems are not typical enterprise networks, they are high-availability environments where even minutes of disruption can translate into immediate financial loss. Security in this context must be engineered for resilience, not just defense.

Unlike conventional IT systems, payment gateways and routing platforms operate in real time, processing thousands of transactions per second. That makes them attractive targets and high-pressure victims. Effective prevention strategies must therefore assume that attackers will attempt to gain access—and focus on limiting how far they can move once inside.

Organisations operating payment infrastructure should prioritise structural safeguards such as:

- Segmentation of critical gateway and API systems to prevent lateral movement between transaction processing environments and corporate networks
- Mandatory multi-factor authentication (MFA) for privileged access, particularly for administrative accounts and remote access points
- Continuous monitoring of anomalous administrative activity, including unusual login patterns or privilege escalation
- Immutable, offline backups that are routinely tested through full recovery simulations—not just theoretical tabletop exercises
- Strict third-party and integrator access controls, including time-bound credentials and zero-trust principles
- Routine penetration testing of payment routing environments to uncover misconfigurations and hidden exposure points

However, preventive controls alone are not enough. In modern ransomware attacks, the true danger lies in dwell time—the period attackers remain undetected within a network. The longer adversaries operate silently, the more systems they can map, the more credentials they can harvest, and the greater the operational blast radius once disruption occurs.

Early detection must therefore be treated as a core resilience function. Behavioral analytics, real-time log analysis, and continuous threat hunting significantly reduce the window of opportunity for attackers. In payment environments, speed is everything—not only in processing transactions, but in identifying intrusions.

Ultimately, preventing ransomware attacks on payment infrastructure is about containment. You may not stop every intrusion attempt, but you can design systems so that a breach does not become a shutdown. And in a world where digital payments underpin everyday commerce, that distinction makes all the difference.

Building resilience after a payment gateway ransomware attack

The BridgePay response highlights a critical truth about ransomware attacks on payment infrastructure: recovery is rarely simple, and it cannot be rushed. Unlike standard IT outages, payment gateway incidents require layered validation before systems can safely return online. Every restored component must undergo forensic review, integrity checks, and security clearance to ensure attackers no longer have access and that transaction data remains trustworthy.

In high-stakes financial environments, bringing systems back too quickly can be as dangerous as the initial disruption. A premature restoration risks reinfection, corrupted transaction processing, or loss of stakeholder confidence. That's why resilience planning must extend well beyond backup restoration.

TECH HIVE ADVISORY

Organisations operating payment infrastructure should maintain:

- Clear incident response playbooks tailored specifically to payment disruption scenarios, not just generic cyber incident plans
- Pre-established relationships with digital forensics teams, legal counsel, and law enforcement partners to accelerate coordinated response
- Transparent communication protocols for merchants, financial institutions, and public stakeholders, ensuring accurate and timely updates
- Regular disaster recovery exercises conducted under simulated outage conditions, including full failover testing of payment routing systems

These measures transform chaos into structured response. When ransomware attacks strike payment gateways, uncertainty becomes the biggest risk. Structured playbooks and rehearsed procedures reduce decision paralysis and shorten recovery timelines.

However, resilience is not simply about restoring servers or reconnecting APIs. In the payment ecosystem, integrity is everything. Merchants must trust that transactions are accurate. Banks must trust settlement processes. Customers must trust that their financial data remains secure.

True resilience, therefore, means restoring confidence in the system itself. It means demonstrating that controls worked, that data remains intact, and that future ransomware attacks will meet stronger defenses. In payment infrastructure, recovery is not complete when systems come back online—it is complete when trust is fully rebuilt.

TECH HIVE ADVISORY

References

Chase Snow, '(TLP:CLEAR) Ransomware Attack at Payment Platform Provider BridgePay Causes Disruptions at Water Utilities Nationwide' (WaterISAC, 12 February 2026) https://www.waterisac.org/tlpclear-ransomware-attack-at-payment-platform-provider-bridgepay-causes-disruptions-at-water-utilities-nationwide

Radiflow, 'Ransomware Preparedness in Critical Infrastructure' (Radiflow) https://www.radiflow.com/ot-cyber-knowledge/ransomware-preparedness-in-critical-infrastructure/

Unitrends, 'Ransomware Recovery: Options and Best Practices' (Unitrends, 2 May 2022) https://www.unitrends.com/blog/ransomware-recovery/

Guru Baran, 'BridgePay Payment Gateway Hit by Ransomware, Causing Nationwide Outages' (CyberSecurityNews.com, 7 February 2026) https://cybersecuritynews.com/bridgepay-ransomware-attack/