11:11 Cyber Incident Recovery Platform

11:11 SYSTEMS

Onity Strengthens Cyber Recovery Readiness with 11:11 Systems

ONITY®

Challenges:

- Enhance preparedness for ransomware and cyber breach scenarios while reinforcing existing security controls
- Establish and maintain a documented, operational recovery strategy for critical applications
- Ensure ongoing business continuity in a highly regulated mortgage environment
- Strengthen confidence that systems could be restored quickly in an isolated environment

Solution:

- 11:11 Cyber Incident Recovery Platform

Benefits:

- Strong assurance of operational continuity during a cyber event
- Proven, reliable recovery processes enabled by automation and rigorous testing
- Consistent recovery execution that outpaced planned timelines
- A collaborative partnership focused on shared success and outcomes

Profile

Onity Mortgage Corporation ("Onity") helps consumers and business clients achieve their homeownership and financial goals through a wide range of servicing and lending programs powered by a technology-enabled, customer-centric platform.

Because Onity operates in a highly regulated industry and manages a significant mortgage origination and servicing portfolio, operational resilience is critical. With ongoing customer, financial and regulatory obligations to meet, the company was proactively looking to further strengthen its cyber recovery strategy beyond prevention and establish a tested framework for restoring critical systems if a disruptive cyber event occurred.

Looking Beyond Prevention

With multiple layers of protection already built into its security posture, including perimeter security, firewall controls, endpoint protections, multifactor authentication and VPN connectivity, Onity understood that even a strong defensive posture does not remove risk entirely. If those controls were somehow breached, the team needed a clear plan for how it would respond and recover.

"Cybersecurity has always been an important business consideration because resilience directly affects our ability to serve customers and meet our obligations," said Dennis Zeleny, Onity's Chief Administrative Officer. "We understand that defense systems in every industry are being challenged, and it's imperative that we consistently prepare for scenarios that could disrupt the business."

Although Onity had not experienced a direct event itself, the frequency of breaches within the broader mortgage industry heightened the company's focus on recovery preparedness as part of the strategy.

Evaluating the Right Partner

As Onity evaluated potential providers, 11:11 Systems differentiated itself through both its expertise and its hands-on approach. During the evaluation process, the teams participated in an assessment workshop led by 11:11, giving Onity the opportunity to dig into the operational realities of cyber recovery before making a final decision. The workshop helped the company understand the potential impact of an incident, how recovery would work in practice, and which systems would need to be included in scope.

"During our evaluation, 11:11 distinguished itself through both its experience and its approach," said Parveen Aery, Onity's Chief Information Officer. "The onsite assessment workshop helped us understand the technology architecture, recovery dependencies, and how the solution would operate within our environment."

For Onity, experience mattered. The company was not looking for a theoretical answer to cyber recovery. It needed a partner with proven capability and the necessary expertise to restore operations from backup data in a worst-case scenario.

"For us, it came down to security maturity, operational discipline, and confidence in execution," said Ravi Hirolikar, Onity's Chief Information Security Officer. "We needed a partner that understood how to recover critical operations securely in a high-pressure scenario, and 11:11 demonstrated that capability."

Third-party validation also supported the decision. Along with internal due diligence and peer research, 11:11's Gartner Voice of the Customer reviews were a meaningful proof point during Onity's evaluation process, which included industry benchmarks and informal research through trusted peers.

"The industry benchmarks mattered, and so did the feedback we received from trusted peers who had been through this process before," said Mr. Hirolikar. "Those inputs helped validate that our recovery strategy aligned with strong information security practices."

A Phased Approach to Cyber Recovery

Because Onity was already operating in a public cloud environment, 11:11 was able to build its clean room recovery strategy on that existing foundation. The team provided guidance on industry-standard best practices to strengthen the backup environment and supported the design of secure clean room environments in AWS and Oracle Cloud. Together, the teams established an isolated environment, separate from production, purpose-built to enable secure testing and recovery operations.

"What helped a great deal was that we as an enterprise were already operating out of a public cloud," said Mr. Aery. "That gave us a strong technology foundation to build the clean room and restore services in an isolated environment that is air-gapped from production."

Rather than deploy everything at once, Onity took a phased approach, beginning with smaller exercises before progressing to broader recovery tests. The company completed multiple partial tests before moving to a larger-scale recovery event involving the broader application environment. That progression allowed the team to learn, refine, and build confidence at each stage.

Executing the Program

Once the program was underway, the goal was to complete a full test by year-end. To achieve this, 11:11 and Onity followed a structured approach encompassing discovery, solution design, implementation, and testing. 11:11 developed tailored cyber recovery plans, procedures, and runbooks to guide the process. A critical step was aligning the teams on the recovery testing calendar early in the year, enabling both organizations to effectively coordinate change controls, staffing, and execution windows in advance.

“One of the most valuable decisions we made was locking in the testing schedule early in the year,” said Rishi Gupta, Onity’s VP of Infrastructure. “Having those dates agreed to in advance made the entire program easier to manage, staff, and execute.”

From there, the teams moved through a regular cadence of exercises, lessons learned, and refinements. The work included intensive testing periods with frequent checkpoints and close coordination across both teams. As the Onity and 11:11 teams gained experience from earlier tests, the efficiency and effectiveness of recovery execution improved.

“The results were satisfying because we were able to restore applications ahead of the plan,” said Mr. Gupta. “That experience helped the engineering teams refine execution and keep recovery speed well ahead of the scheduled timeline.”

A Critical Business Benefit: Continuity

For Onity, the greatest value of the program is continuity. In mortgage servicing and lending, downtime is not simply an IT issue. The company supports a large volume of customers, handles sensitive financial information, and must continue meeting regulatory commitments.

“Because of the number of customers we support and the ongoing regulatory obligations of our business, continuity has to be treated as a business strategy priority,” said Mr. Zeleny. “Being out of operation for any meaningful period of time is simply not an option.”

A Collaborative Relationship

Onity also emphasized the nature of the working relationship with 11:11. Throughout the engagement, and especially during intensive testing cycles, the two teams operated with a shared focus on the objective rather than on company lines or ownership boundaries.

“What stood out was how open and collaborative the relationship was throughout the process,” Mr. Aery said. “It always felt like one team working toward the same goal.”

That spirit of partnership helped reinforce confidence in the program itself. In a high-stakes recovery scenario, the ability to work as one coordinated team can be just as important as the underlying technology.

“During the 72-hour drills, we had structured checkpoints every four hours,” Mr. Gupta noted. “The team stayed focused on the shared objective from start to finish.”

Enhanced Operational Capability

By partnering with 11:11 Systems, Onity was able to achieve its objective of strengthening its cyber incident recovery capabilities. Through an assessment-led evaluation, a phased testing strategy, and a collaborative working model, the company is now even more confident that it can restore critical applications and maintain continuity if a cyber event occurs. For an organization operating at the intersection of customer trust, financial data, and regulatory responsibility, that confidence is essential.