CASE STUDY

How Proactive Disaster Recovery Planning Helped a Small Business Avoid Major Cyber Downtime

When a cyber incident threatened operations, TISDCS protected critical data, accelerated recovery, and kept downtime from escalating.

INDUSTRY: Small Business | **LOCATION:** Fairfield, NJ | **SERVICES:** Managed IT Services, Cybersecurity Services

EXECUTIVE SUMMARY

When a cyber incident threatened to disrupt operations, this small business needed more than reactive support—it needed a clear path to protect data and restore service fast. Technical Integration Services delivered data protection and disaster recovery planning aligned to business continuity. The result was a faster recovery, protected critical information, and major downtime avoided.

CHALLENGES

- A cyber incident threatened to halt daily operations and create costly downtime across the business.
- Critical data needed stronger protection to reduce the risk of loss, exposure, or delayed recovery.
- Without a clear recovery plan, the business faced uncertainty around restoring systems under pressure.
- Leadership needed confidence that operations could resume quickly without prolonged client or staff disruption.
- The organization could not afford reactive IT decisions during an active security event.

TECHNICAL INTEGRATION SERVICES'S APPROACH

KEY ACTIONS

- TIS assessed continuity risks and prioritized the systems and data most critical to day-to-day operations.
- The team formalized disaster recovery procedures so stakeholders had a clear path for response and restoration.
- TIS strengthened data protection practices to support secure recovery when the cyber incident occurred.
- During the disruption, technicians guided containment and coordinated recovery steps to reduce business impact.
- TIS stayed aligned with leadership throughout the event, providing responsive support and practical next actions.

SOLUTIONS

- A business continuity approach combined data protection with a recovery plan built around operational priorities.
- Structured disaster recovery processes gave the client a defined, repeatable path to restore critical services.
- Security-focused response support helped protect sensitive data while recovery efforts moved forward.
- Proactive planning reduced reliance on improvised decisions during a high-pressure cyber event.
- Ongoing guidance turned IT from a reactive function into a more resilient foundation for the business.

RESULTS

- **The business avoided major downtime during a cyber incident and maintained greater operational continuity.**
- **Critical data was secured and recovery efforts moved forward with less confusion and lower business risk.**
- **Systems were brought back online quickly, limiting disruption to employees, customers, and daily workflows.**
- **Leadership gained confidence that the organization could respond to future incidents with a clearer plan.**
- **The engagement strengthened long-term resilience by tying IT preparedness directly to business continuity.**

WHAT CLIENT SAYS

"Their data protection and disaster-recovery planning saved us from major downtime during a cyber incident. TISDCS knew exactly how to secure our data and get us back online quickly. These guys truly understand business continuity."

PROTECT OPERATIONS BEFORE DISRUPTION HITS

Build a stronger recovery strategy with proactive IT and cybersecurity support before the next disruption tests your business.

Schedule a Consultation

tisdcs.com

(888) 587-5459