



Case Study:

“Our Law Firm Was One Click Away From a Data Breach”

How CDN Technologies Helped a Law Firm Secure Confidential Client Data, Modernize Their IT Environment, and Protect Their Business



Industry: Law Firm

Location: Oakville, Ontario Canada

Services Provided: Comprehensive Network Assessment, Managed IT Services, Microsoft 365 Migration & Tenant Hardening, Microsoft OneDrive & SharePoint Implementation, Business Continuity & Disaster Recovery (BCDR), Microsoft 365 Backup Protection, Cisco Meraki Firewall & Secure Business WiFi, Endpoint Detection & Managed Detection & Response (MDR), Windows Patch Management, Network Infrastructure Upgrades, Ongoing Cybersecurity Monitoring & Maintenance



The Challenge

Like many small law firms, this practice had accumulated technology over many years without an overall IT strategy.

Although the firm was operating day to day, several critical technology and cybersecurity issues placed confidential client information at unnecessary risk. There were no reliable backups, no offsite disaster recovery, and no way to quickly recover from ransomware, accidental deletion, or hardware failure. Staff stored important legal documents on local desktops, used Dropbox to share files, and shared documents directly from one workstation to another, creating multiple security and compliance concerns.

The office network relied on powerline networking, transmitting data through the building's electrical wiring instead of dedicated network cabling. This resulted in inconsistent performance, slower network speeds, and unnecessary security risks.

The office was also operating two separate internet connections. Depending on which network employees were connected to, computers, printers, and scanners often couldn't communicate with one another, leading to daily productivity issues.

From a cybersecurity perspective, Windows updates were inconsistent, antivirus protection varied from computer to computer, and there was no business-grade firewall protecting the firm's network.

For a law firm entrusted with confidential client files, privileged communications, contracts, and financial records, these weaknesses represented a significant business and cybersecurity risk.



The Assessment

CDN Technologies went onsite and performed a comprehensive network and infrastructure audit to identify the root causes of the issues.

Our assessment uncovered several critical technology and cybersecurity risks that placed the firm's operations and confidential client information at unnecessary risk, including:

- No reliable business continuity or disaster recovery solution
- No offsite backups to protect against fire, theft, ransomware, or hardware failure
- Employees storing legal documents on local desktops
- Dropbox being used for business file storage without centralized management or backup
- Files being shared directly from one workstation instead of a secure centralized platform
- Powerline networking transmitting business data through the building's electrical system
- Two separate internet connections creating network communication issues between devices

- Missing Windows security patches exposing computers to known vulnerabilities
- Inconsistent antivirus protection across workstations
- No centralized monitoring or management of endpoint security
- No business-grade firewall protecting the office from modern cyber threats
- Microsoft 365 security settings that had never been properly secured or hardened
- No centralized cloud collaboration platform for document management
- No proactive monitoring, maintenance, or strategic IT management

The assessment showed that while the firm's technology had evolved over time, it lacked the security, resilience, and management required to adequately protect confidential legal information and support a modern law practice.



The Solution

Based on the findings of the assessment, CDN Technologies developed a comprehensive modernization and cybersecurity plan that addressed each identified risk while improving the firm's overall productivity and resilience.

Business Continuity & Disaster Recovery

We implemented a fully managed Business Continuity and Disaster Recovery (BCDR) solution to protect the firm's servers, workstations, and legal data.

The solution included:

- Image-based backups of entire systems
- Encrypted offsite backup replication
- Daily automated backup verification with screenshot validation
- Rapid restoration of complete systems or individual files
- Continuous monitoring of backup health and recovery readiness

The firm can now quickly recover from ransomware, accidental deletion, hardware failure, or other disasters with minimal disruption.

Microsoft 365 Modernization & Security

We migrated documents from local desktops, Dropbox, and unsecured workstation shares into Microsoft OneDrive and SharePoint, providing a modern and secure collaboration platform.

This included:

- Secure cloud storage for individual user files using Microsoft OneDrive
- Centralized document management with Microsoft SharePoint
- Secure remote access to files from any location
- Granular permissions to protect confidential legal documents
- Version history and document recovery
- Automatic synchronization across devices

- Microsoft 365 cloud backup protection

We also secured and hardened the firm's Microsoft 365 tenant by implementing Microsoft's recommended security best practices, including:

- Securing administrator accounts
- Enforcing Multi-Factor Authentication (MFA)
- Configuring Conditional Access policies
- Removing legacy authentication protocols
- Strengthening Microsoft 365 security configurations
- Improving email security to reduce phishing and business email compromise
- Monitoring sign-in activity for suspicious behaviour
- Applying least-privilege access controls throughout the organization

The result was a secure Microsoft 365 environment that protects confidential client information while allowing employees to work safely from anywhere.

Network Modernization

We redesigned the firm's network infrastructure to improve both reliability and security.

This included:

- Replacing powerline networking with dedicated network cabling
- Eliminating the second internet connection
- Standardizing the office on the faster Bell internet service
- Improving communication between workstations, printers, and scanners
- Simplifying network management and increasing performance

Employees now have a faster, more reliable network that supports their work without unnecessary interruptions.

Cybersecurity & Managed IT Services

To provide continuous protection, we implemented a layered cybersecurity strategy supported by ongoing Managed IT Services.

This included:

- Cisco Meraki cloud-managed firewall
- Secure business WiFi
- Managed Endpoint Detection and Response (MDR)
- Automated Windows patch management
- Continuous device monitoring
- Centralized security alerting and reporting
- Proactive maintenance and remediation
- Ongoing IT support and strategic technology management

Rather than waiting for problems to occur, the firm's technology is now continuously monitored, maintained, and protected.



The Results

Following the implementation, the law firm now benefits from:

- Secure, verified backups with rapid disaster recovery
- A fully secured and hardened Microsoft 365 environment
- Confidential legal documents centrally managed in Microsoft OneDrive and SharePoint
- Secure remote access for lawyers and staff
- Significantly reduced risk of ransomware, phishing, and business email compromise
- Faster and more reliable office networking
- Business-grade firewall protection and secure wireless networking
- Fully patched, monitored, and protected workstations
- Improved collaboration and document management
- Proactive IT support that prevents issues before they impact the business
- Greater confidence that confidential client information is protected, recoverable, and secure



Why This Matters for Law Firms

Law firms are entrusted with some of the most sensitive information a business can possess. Client records, legal documents, contracts, financial information, and privileged communications are all attractive targets for cybercriminals and must be protected accordingly.

Unfortunately, many law firms still rely on aging technology, inconsistent security practices, and outdated file-sharing methods that increase the risk of ransomware, data breaches, downtime, and compliance issues.

A modern legal practice requires more than someone to fix computers when they break. It requires secure systems, proactive maintenance, reliable backups, and ongoing cybersecurity management to ensure confidential client information remains protected and accessible.



About CDN Technologies

At CDN Technologies, we help law firms modernize their technology, strengthen their cybersecurity, and reduce business risk through comprehensive Managed IT Services. The result is a secure, reliable IT environment that allows lawyers and staff to focus on serving their clients instead of worrying about technology.