CDN TECHNOLOGIES

Case Study:

When a Break-In Became an IT Security Wake-Up Call

Industry: Manufacturing

Services Provided: Network Assessment, Managed IT Services, Cybersecurity, Microsoft 365 Security Hardening, Network Infrastructure Upgrades, Immutable Back Ups & Business Continuity

The Challenge

For one Mississauga manufacturing company, the need to rethink its IT strategy became very real after an unexpected event: **their office was broken into and ransacked.**

Several computers were stolen, including the computer used by accounting peron. The thieves also took the company's NAS (Network Attached Storage) device. This device was being used to store their on-site backups.

At first, the stolen equipment appeared to be the biggest concern. **It wasn't.**

The company soon realized that their backups had disappeared along with the computers they were meant to protect. Even more concerning, employees had saved passwords directly in their web browsers on their stolen computers.

The Assessment

CDN Technologies performed a comprehensive network and cybersecurity assessment. The objective wasn't simply to replace what had been stolen. We needed to understand what the thieves potentially had access to, what the company could recover, and what other risks were hiding in the environment.

- **Stolen device exposure:** We considered what company information, applications, and credentials could potentially have been accessible from the stolen computers.
- **Password and credential security:** Browser-saved passwords and other credential practices were reviewed to identify accounts requiring additional protection.
- **Accounting and financial access:** Particular attention was given to the potential exposure created by the theft of the accounting computer.
- **User accounts and permissions:** Administrative access and unnecessary privileges were identified.
- **Email and cloud applications:** Account security and authentication practices were evaluated.

The Solution

The guiding principle was straightforward:

Losing a computer, server, or even the entire office should not mean losing control of the company's data, passwords, or ability to recover.

- **Move backups off-site:** Implement encrypted off-site backups so the same physical incident cannot take out both production systems and their backups.

- **Implement image-based disaster recovery:** Protect complete systems so critical devices and applications can be restored more quickly after a major incident.
- **Monitor and test backups:** Regularly verify that backups are successful and, more importantly, recoverable.
- **Improve password management:** Move away from relying on passwords saved locally in browsers and establish centrally managed password practices.
- **Strengthen protection for sensitive accounts:** Apply additional controls to accounting, administrative, and other high-value accounts.
- **Modernize network infrastructure:** Replace aging equipment and use virtualization to separate critical roles.
- **Standardize and secure workstations:** Move employees onto supported operating systems with consistent security configurations.
- **Modernize email and productivity tools:** Move toward a centrally managed Microsoft 365 environment with stronger identity controls.
- **Improve employee cybersecurity awareness:** Train employees on password security, phishing, account protection, and other common threats.
- **Establish proactive IT monitoring:** Continuously monitor the environment so risks can be addressed before they become business disruptions.

The Results

The break-in fundamentally changed the way management viewed IT security. Before the incident, a backup sitting on a NAS seemed like a backup. Passwords saved in a browser seemed convenient. Computers were viewed primarily as replaceable equipment.

After the robbery, the company understood how those individual decisions could combine into a much larger business risk.

The resulting IT strategy helped the company:

- ✓ Establish an off-site backup and disaster recovery strategy.
- ✓ Remove the risk of relying exclusively on a backup stored beside the systems it protects.
- ✓ Strengthen password and credential management.
- ✓ Add additional protection to sensitive company accounts.
- ✓ Improve security around accounting and financial systems.
- ✓ Reduce the potential impact of a stolen computer.
- ✓ Eliminate unnecessary administrative privileges.

- ✓ Improve protection against ransomware and account compromise.
- ✓ Modernize aging infrastructure.
- ✓ Standardize endpoint security and patch management.
- ✓ Improve the company's ability to recover from future disruptions.
- ✓ Move from reactive IT support toward proactive technology management.

Why This Matters for Manufacturing Businesses

For manufacturers in Mississauga, Oakville, Burlington, and across the GTA, an IT problem can quickly become an operations problem. Whether it's theft, ransomware, hardware failure, or another unexpected event, protecting your systems and having a reliable recovery plan helps prevent downtime and keeps your people and production moving. **The goal isn't just better IT—it's making sure a technology problem doesn't become a business interruption.**

CDN
TECHNOLOGIES

About CDN Technologies

CDN Technologies provides managed IT services and cybersecurity solutions for manufacturing businesses in Mississauga, Oakville, Burlington, and across the GTA. We help manufacturers **reduce downtime, protect against cyber threats, prevent data loss, and recover quickly when something goes wrong.** From unreliable technology and aging infrastructure to cybersecurity, backups, and day-to-day IT support, our proactive approach helps keep your systems secure, your employees productive, and your operations moving.