CASE STUDY

The Belden Brick Sales Company

How The Belden Brick Sales Company Secured Its Data, Achieved PCI Compliance, and Eliminated the IT Headaches Holding the Business Back

Presented by

Cyber Protect LLC

No Geek Speak. No Hassles. Just Real Protection.

(586) 500-9300 | (888) 531-5099 | info@cyberprotectllc.com | cyberprotectllc.com

Executive Summary

The Belden Brick Sales Company, a Metro Detroit building-products firm, was running its business on an IT foundation held together with workarounds. Staff dealt with unreliable Wi-Fi, an aging network that regularly went down, computers that had never been properly secured, and no clear plan for what would happen if a cyberattack or data breach hit. The company also needed to stay compliant with Payment Card Industry (PCI) compliance standards to protect customer payment data.

Cyber Protect LLC stepped in, assessed every layer of the business's technology environment, and delivered a comprehensive modernization. The result: a secure, compliant, and stable IT infrastructure that lets the team focus on selling, not troubleshooting. Most tickets are resolved the same day. The network is dependable. Staff know what good cyber hygiene looks like. And the business is no longer one preventable incident away from a costly breach.

PCI Compliance Note

Any business that accepts, processes, or stores credit card payments is subject to Payment Card Industry Data Security Standards (PCI DSS). Failing to comply exposes a company to fines, increased transaction fees, loss of the ability to accept card payments, and significant liability if customer data is compromised.

The Challenge

When the management team at The Belden Brick Sales Company sat down to think honestly about their technology, the list of concerns was long.

Day-to-day operations were hampered by a Wi-Fi network that dropped regularly, slowing down staff and frustrating everyone who relied on it. The company operates across two locations, but the connection between those sites was inconsistent, creating delays and communication gaps that should not exist in a modern business.

On the security side, the picture was worse. Workstations had not been properly hardened. Systems were running outdated software. There was no zero-trust security model in place, meaning that if one device or account was compromised, the damage could spread quickly. Drive encryption, email backups, and secure remote access were either missing or inadequate.

Password discipline was inconsistent across the team, and staff had received little formal guidance on how to recognize and respond to phishing attempts or other common threats. The company also had no web filtering in place to prevent employees from inadvertently visiting malicious sites.

Layered on top of all of that was the compliance question. Accepting credit card payments was a top priority for an upgraded infrastructure, and it could not be just a regulatory gap; it is a legal and financial liability they take seriously. The company needed a partner who could address everything at once.

Why This Matters for Sales Companies

Businesses in distribution, wholesale, and retail sales regularly handle customer payment data and maintain records tied to contracts, pricing agreements, and client accounts. A breach does not just

cost money to remediate; it can permanently damage the supplier and customer relationships a sales business depends on to operate.

Why They Called Cyber Protect LLC

The management team knew they needed help but had been hesitant to engage. Like many small and mid-sized businesses, they had questions about cost, disruption, and whether a vendor would actually follow through or just sell them something and disappear.

What prompted the decision to move forward was a combination of growing concern about cybersecurity threats in their industry, the operational drag caused by persistent connectivity problems, and an upcoming need to demonstrate PCI compliance. Continuing to delay was no longer a viable option.

They chose Cyber Protect LLC because of the firm's track record with Michigan businesses and a straightforward approach: assess everything first, recommend only what is needed, and stay accountable for results. No jargon, no overselling, no vanishing after the invoice is paid.

The Cyber Protect Solution

Cyber Protect conducted a thorough assessment of the company's entire technology environment before recommending a single change. The goal was to understand not just what was broken, but what was missing and what was at risk. The resulting engagement covered every major layer of the business's IT infrastructure.

Network and Connectivity

- Upgraded the company's Wi-Fi network, replacing unreliable hardware with enterprise-grade equipment and a properly configured wireless environment
- Migrated the company to a more reliable internet service provider, eliminating the chronic outages that had been disrupting operations
- Repaired and stabilized intra-office connectivity between the company's two locations, ensuring both sites operate on a dependable network.

Endpoint and Device Security

- Deployed enterprise-grade firewalls to control traffic in and out of the network
- Implemented zero-trust endpoint security, meaning every device must verify its identity and health before accessing company resources
- Patched all systems to current security standards, closing known vulnerabilities that attackers routinely exploit
- Upgraded all workstations to Windows 11, ensuring the company operates on a supported, actively maintained operating system
- Enabled full drive encryption on workstations, protecting data stored on devices in the event of loss or theft
- Deployed workstation backup solutions to ensure business data is recoverable

Identity, Access, and Email

- Deployed Microsoft Entra ID (formerly Azure Active Directory) to centralize identity management and enforce consistent access controls across all users and devices
- Locked down user accounts and enforced the principle of least privilege, limiting what each user can access to only what they need
- Migrated the company to hosted Microsoft 365 email, providing enterprise-grade reliability, security, and email backup protection
- Implemented web filtering to block access to malicious and inappropriate sites, reducing the risk of drive-by malware downloads and phishing page visits
- Raised the company's Microsoft Secure Score, a measurable indicator of how well the Microsoft environment is configured and protected

Staff Training and Cybersecurity Awareness

- Trained the entire staff on password management best practices, including the use of strong, unique passwords and how to avoid common mistakes
- Delivered company-wide cybersecurity awareness education covering phishing recognition, social engineering tactics, and safe computing habits

The Results

The engagement delivered measurable, immediate improvements across every area of the business's IT environment. Here is a summary of outcomes:

Area Addressed	Outcome for The Belden Brick Sales Company
Network Reliability	Wi-Fi upgraded and stabilized; chronic outages eliminated with a new internet provider
Multi-Site Connectivity	Intra-office link between both locations repaired and operating reliably
PCI Compliance Readiness	Infrastructure hardened and aligned with PCI DSS requirements to protect payment data
Endpoint Security	Zero-trust model deployed across all workstations; systems patched and encrypted
Operating System Currency	All workstations upgraded to Windows 11 and fully supported
Identity Management	Entra ID deployed; access controls locked down and consistently enforced
Email Security and Backup	Migrated to hosted M365 with email backup and advanced security enabled
Data Protection	Workstation backups and drive encryption in place for full data recoverability

IT Support Responsiveness	Help desk tickets resolved same-day, virtually eliminating unresolved IT backlogs
Staff Security Awareness	Full team trained on passwords, phishing, and cybersecurity best practices
Microsoft Secure Score	Score raised to reflect a well-configured and properly protected Microsoft environment

Beyond the metrics, the change in day-to-day experience has been significant. Staff are not dealing with the frustration of a network that goes out or waiting days for IT problems to be addressed. Management has confidence that customer payment data is protected and that the business meets its compliance obligations.

What This Means for Your Business

If your business looks anything like this one, you may recognize some of the same gaps. Most small and mid-sized companies in the sales, distribution, and wholesale space did not build their IT infrastructure from the ground up with security in mind. It grew organically, piece by piece, and the vulnerabilities accumulated along the way.

Here are the questions worth asking honestly:

- If your Wi-Fi or internet connection went down today, how long would it take to recover, and what would that cost you?
- Do you know whether every computer on your network is encrypted, patched, and running a supported operating system?
- Are your employees able to recognize a phishing email or a social engineering attempt?
- If a cyberattack compromised your systems tonight, do you have backups that could restore your data quickly?
- Are you confident your business meets PCI DSS standards for the way you handle customer payments?

Answering 'no' or 'I am not sure' to any of those questions is a risk. It is also a problem that is entirely solvable. Cyber Protect LLC works with businesses of all sizes to close exactly these kinds of gaps, without disrupting operations or requiring a full-time internal IT department.

> **PCI DSS at a Glance**
> *PCI DSS compliance requires businesses to maintain a secure network, protect stored cardholder data, control access to systems that touch payment data, regularly monitor and test those systems, and maintain a formal information security policy. Non-compliance penalties range from monthly fines to loss of card processing privileges.*

About Cyber Protect LLC

Cyber Protect LLC is a Michigan-based managed IT and cybersecurity firm serving small and mid-sized businesses in regulated industries. With over 20 years of experience, Cyber Protect delivers enterprise-grade protection without the enterprise price tag. Our approach is simple: No Geek Speak. No Hassles. Just Real Protection.

To schedule a free risk assessment, call (586) 500-9300 or toll-free at (888) 531-5099, or email info@cyberprotectllc.com. Learn more at cyberprotectllc.com.

Is Your Business Protected?

Find out with a free, no-obligation cybersecurity risk assessment from Cyber Protect LLC. We will show you exactly where you stand and what it would take to fix it.

Call (586) 500-9300 | Toll-Free (888) 531-5099 | info@cyberprotectllc.com

cyberprotectllc.com