How to Defend Your Construction Firm: 8 IT Safeguards Anyone Can Implement

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This guide will get you started in protecting everything you've worked so hard to build.

Provided By: XSolutions
Author: Mike Layland, CXO
20 Squadron Blvd STE 320, New City, NY, 10956
www.xsolutions.com

Are You A Target?

As a small or medium construction executive, you're on the front lines of a growing battle. Right now, hackers from regions like China, Russia, and Ukraine are launching relentless attacks on businesses like yours. What's their goal? To steal your client data, case records, and sometimes even your hard-earned money. Shockingly, some of these operations are even backed by government resources.

Think your business is too small to be a target? Think again. Every day, **82,000 new malware threats** emerge, and **half of all cyberattacks** are directed at businesses like yours. And the reported breach count isn't the total – not even close! Many breaches go unreported to avoid bad PR, fines, or legal complications.

According to the National Cyber Security Alliance, **1 in 5 small businesses** suffered a cyberattack last year, and that number continues to rise as companies embrace cloud technology and mobile devices. With regulations tightening and data breaches becoming headline news, implementing these **seven critical security measures** is no longer optional - it's critical.

1. **The Biggest Security Risk to Your Business? *Your Team.***

   Believe it or not, most security breaches happen because an employee unknowingly opens the door for attackers. Whether it's clicking on a malicious link, downloading an infected file, or opening a phishing email - these actions can allow hackers to access your network. Once inside, they can spread malware across other devices.

   Phishing emails - designed to look like legitimate messages - are a significant threat. Even the best spam filters can't protect your business if someone on your team clicks on a malicious link. That's why training your employees to recognize phishing attempts and online scams is absolutely essential. Cybercriminals are incredibly sophisticated, and even tech-savvy employees can be tricked. A single mistake can lead to devastating consequences, so regular education is a must.

   To minimize risks, it's crucial to implement an **Acceptable Use Policy (AUP)**. This document sets clear guidelines for how employees can use company-owned device and accounts. A well-done AUP can restrict access to potentially harmful websites, unauthorized applications, or risky websites.

Enforcing this policy through content-filtering software on your firewalls can help regulate what employees do online during work hours. You can even customize access levels to grant specific permissions to certain team members while maintaining stricter controls for others.

2. **Strong Passwords Aren't Optional**

   When you set your password to "123456" - hackers are excited. Easy passwords like birth years, pet names, or similar are extremely vulnerable. That's why you must make it policy for passwords to have a minimum of eight characters, a combination of capital letters, symbols, and digits. Also, be sure to enforce passcodes on any mobile device lock screens. Employee carelessness can be solved for by automating and enforcing strong password standards via policy.

3. **Multifactor Authentication (MFA) Everywhere**

   MFA adds an additional layer of protection by requiring your users to verify their identity with something other than just a password. Examples you may be familiar with could be a code sent to their phone or an authentication app.

   Even if an employee's password is compromised, MFA makes it significantly harder for cybercriminals to gain access to your systems. This extra step is particularly important for accessing sensitive business data, cloud applications, or email accounts.

   While it may seem like an inconvenience, MFA can be a game-changer in preventing unauthorized access and is an essential component of a modern cybersecurity strategy.

4. **Patch and Update Frequently**

   Cybercriminals are drawn to outdated software like moths to a flame. Once found, they exploit vulnerabilities in the code and gain access to your systems. Stay ahead of this risk by ensuring all devices and applications are regularly patched and updated. Under a managed IT plan, this process can be automated, giving you peace of mind without the manual effort.

5. **Backup Like Your Business Depends On It (Because It Does)**

Whether it's a ransomware attack or accidental file deletion (accidental deletions happen more than you may think), a solid backup system can save your business. Ensure your backups are automated, monitored, and tested frequently to guarantee reliability when disaster strikes.

While there are many types of backups available on the market, we have found that the best backups offer hourly server backups and are **immutable** (meaning they cannot be changed, deleted or encrypted by a bad-actor)

6. **Don't allow employees to access your businesses data with personal devices that aren't monitored and secured by YOUR IT department.**

The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all it takes is a username and password. Employees are now even asking if they can bring their own personal devices to work (BYOD) and use their smartphone for just about everything.

But this trend has DRASTICALLY increased the complexity of keeping a network - and your business data - secure. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get breached (although that remains a possibility). Your biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected, thereby giving a hacker access to your data and cloud application.

So, if you ARE going to let employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a security professional. Further, do not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps.

But here's the rub: Most employees won't want you monitoring and policing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your business. Our suggestion is that you only allow employees to access work-related files, cloud applications and e-mail via business-owned and monitored devices, and never allow employees to access these items on personal devices or public Wi-Fi.

7. **Invest In A Good Firewall.**

   A firewall is your first line of defense against cyberattacks and a great way to enforce company wide internet policies. But it's not a set-it-and-forget-it tool - it needs regular monitoring and maintenance. A managed IT provider can keep your firewall running effectively to safeguard your network.

8. **Protect Your Bank Account.**

   Did you know your BUSINESS bank account doesn't enjoy the same protections as your personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your account!) Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, NOT fraud.

   So here are 3 things you can do to protect your bank account. First, set up e-mail alerts on your account so you are notified any time money is withdrawn. The FASTER you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the DAY it happens can be stopped. If you discover even 24 hours after it's happened, you may be out of luck. That's why it's critical that you monitor your account daily and contact the bank IMMEDIATELY if you see any suspicious activity.

   Second, if you do online banking, dedicate ONE computer to that activity and never access social media sites, free e-mail accounts (like Hotmail) and other online games, news sites, etc. with that PC. Be sure that machine is monitored and maintained behind a strong firewall. And finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account. All of these things will greatly improve the security of your accounts.

Want Help In Implementing These 8 Essentials?

If you're worried about the risks posed by cybercriminals and how your employees may inadvertently expose your network, give us a call to discuss how a managed security plan can safeguard your business.

At absolutely no cost or obligation, we'll send a security expert and a senior technician to your office to perform a **comprehensive Security and Backup Audit**. This evaluation will identify vulnerabilities in your network and assess potential data loss points and security gaps. Our audit will even touch on typically overlooked areas, such as mobile devices, laptops, tablets, and home PCs. After this audit, you'll have clear answers to critical questions:

- **Is your network truly protected from today's most advanced cybercriminals?** If not, what are the essential steps you need to take right now to shield your business?

- **Are your backups genuinely reliable?** We'll verify that all crucial files and data are backed up and give you an accurate estimate of how long it would take to restore them in case of an emergency (hint: it's often longer than expected).

- Are your employees misusing the internet on your time? Whether it's accessing inappropriate sites, job hunting, or wasting hours on personal emails and social media, do you really know the extent of these activities?

- Are you unknowingly breaking data compliance laws like PCI? With regulations constantly evolving, it's surprisingly easy to fall out of compliance without realizing it - but the consequences can include hefty fines and damaging publicity.

- Is your firewall and antivirus software optimized and up-to-date?

- Are employees storing sensitive business data on unsecured cloud apps like Dropbox that fall outside your backup solution?

We understand it's tempting to assume your current setup has everything under control. **But from experience, we're confident that we'll uncover at least one serious vulnerability putting your business at risk for cyberattacks, data loss, or prolonged downtime.** Unfortunately, we've seen it happen far too often in the businesses we've audited.

Even if you already have an IT team or provider managing your network, a second opinion can be invaluable. As a neutral third party, we'll give you a no-spin assessment with nothing concealed or sugar-coated. If you want the full picture of your network's security, we'll deliver it.

You Are Under No Obligation To Do Or Buy Anything

We understand that deciding on IT solutions takes trust. That's why our free audit comes with no strings attached. Whether or not you choose to work with us, we're committed to giving you clear insights into your networks posture.

You've worked hard to build your business - don't let a cyberattack undo it all. Call us at **877-807-1332** or email **michael@xsolutions.com** to schedule your free assessment today.

Dedicated to serving you,

Mike Layland
Web: www.xsolutions.com
E-mail: michael@xsolutions.com

See What Our Clients Are Saying:

PEACE OF MIND WITH TOP-NOTCH SECURITY

“Switching to XSolutions was primarily driven by our need to enhance security. Before XSolutions, we were vulnerable to hackers and ransomware, and we couldn't even qualify for cyber insurance due to our weak defenses. Since partnering with XSolutions, our security has significantly improved, and I can now sleep peacefully knowing we are well-protected against cyber threats. We also have robust backups in place, ensuring that our company would not be devastated in the event of an attack.

XSolutions stands out from other IT firms because they don't follow a 'one size fits all' approach. They understand the unique needs of our company and consistently offer solutions to make our systems more reliable, secure, and seamless. Unlike other IT firms that are reactive, XSolutions is proactive in helping us stay ahead with the latest IT advancements.

If you're considering XSolutions as your IT firm, know that they offer the expertise of a large IT consultancy while remaining small enough to provide personalized care for their clients. Whether you need better security, more efficient tools, or just want to stay current with IT developments, XSolutions is an excellent partner. I wholeheartedly recommend them to any business, big or small.”

-Adam Russin, Co-President of Russin Lumber