CYREN

10 Steps to Protect Your Construction Business from Cyberthreats

Solution Brief

Construction-related companies of all sizes have become targets for phishing, malware, and ransomware attacks.

In a world increasingly dependent on digital technology and with supply chains becoming more interconnected, the construction industry is being challenged by continued increases in the volume and sophistication of cyberattacks. This is particularly true for small- to mid-sized construction companies, who are frequently targeted in an effort to get at larger partners and customers. According to the 2018 Verizon Data Breach Report, small businesses are the target of cyberattacks more than 58% of the time.

Business Dynamics Influence Cyberthreats

Extensive partnerships create collective risk – The decentralized and interconnected nature of the construction industry makes email and web threats particularly dangerous. With complex groups of stakeholders, including prime contractors, subcontractors, partners, vendors, materials and services suppliers, and financial and investing entities, the construction and building trades "supply chain" offers myriad opportunities for cybercriminals to leverage a smaller, less protected business to breach a larger customer or financial entity.

New tools are bringing new risks – New technologies and business processes are having a dramatic impact on construction and building trades activity, with numerous applications and tools emerging that are changing how companies design, plan, and execute projects. The adoption of internet-based, collaborative systems for everything from email and financing to digital design, estimating, and quality control are driving improved costs and timelines, but at the same time these technologies open businesses to new paths for cyberattacks.

Outdated security posture creating security gaps – Companies relying on outdated security technology are at extreme risk. Endpoint and appliance-based security and online "free" security tools are typically not updated in real time, so new and evolving threats are slipping through before protection is in place.

Unprotected mobile workforce – With an increasingly mobile workforce, employees are no longer confined to a work environment protected by perimeter security devices. Bring-your-own-device (BYOD) policies mean that numerous different devices, each with a different operating system are accessing company resources—and potentially downloading harmful phishing, malware, and ransomware that, in turn, gets passed to others on the same corporate network. Today, mobile devices need to be protected regardless of location, device type, operating platform, or device ownership.

Target Credit Card Hack Started With Supplier Email

The infamous Target breach – in which 40 million credit and debit cards, and email and mailing addresses for 70 to 110 million people were hacked and compromised in 2013 – began with an employee at an HVAC company who opened an email attachment containing malware that captured stored passwords and sent them back to the hacker. Among the credentials stolen were the HVAC vendor's login information to some of their customers' systems, including Target.

Other high-profile hacks that began with a vendor in the supply chain include the massive 2014 Home Depot hack, which resulted in 56 million stolen credit and debit card details and 53 stolen email addresses, and the hacks into Amazon Web Services and Wendy's, as well as the so-called "Panama Papers" breach.

> "More than 60% of cyberattacks originate from the supply chain or from external parties exploiting security vulnerabilities within the supply chain."
>
> ACCENTURE, 2016

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

10 Steps to Protect Your Construction Business from Cyberthreats

Solution Brief

The Business Impacts of a Breach

Among the potential business risks that construction-related businesses need to factor into security decisions are:

Business interruption – Construction and building trades businesses are heavily reliant on project and production schedules to ensure profitability and customer satisfaction. It only takes one ransomware attack to have a detrimental effect on an entire construction project, including work shutdown and potentially significant delays in the delivery schedule, leading to financial consequences, including a reduction in fees or fines for delayed delivery. The French construction supply firm Saint-Gobain lost several days of business as victims of the infamous Petya ransomware attack in 2017.

Significant financial loss – Construction can be a lucrative and high-cash flow business, making significant financial loss as the result of cyberattack a strong reality. Patco Construction, a Maine-based construction firm lost $300K+ when hackers diverted money from their bank accounts using fake IP addresses to trick the financial institution.

Loss of sensitive corporate data – Phishing attacks, including spearphishing or business email compromise (BEC) attacks use spoofed email messages and copycat websites that look legitimate to trick victims into sharing valuable personal or business information, such as Social Security numbers, user names and passwords, or building blueprints, electrical schematics, financial data, or building access or security guard details. In 2013, blueprints for the new Australian Security Intelligence HQ building were stolen by hackers and leaked. And, in 2016, an employee at Turner Construction fell victim to a 'spear phishing' scam in which the entire database of employee information, including W-2s and social security numbers were sent to a spoofed email account created by cyber criminals.

Reputation and loss of business – Construction and building trades companies risk major reputation damage and loss of clients and business if their company is used as the point-of-entry for a larger cyberattack. As an industry that operates with a large number of stakeholders, cybercriminals will often use small stakeholder businesses, such as an HVAC vendor or general contractor to initiate a hack into a larger company. In the notorious Target Corporation breach, cybercriminals gained access to Target systems by hacking into Target's HVAC supplier's IT systems and stealing login credentials.

What you can do to protect your company, business partners, and customers

1. **Automate threat updates to the shortest possible time interval.** You need to make sure there isn't a time lag for protection from new threats.
2. **Deploy cloud-based email gateway protection from a security provider.** Cloud-based Secure Email Gateways add more advanced security like time-of-click URL analysis and protection from business email compromise. The default security provided by hosted email security services like Office 365 provides only a basic layer of protection.
3. **Deploy a web security gateway.** An effective web security gateway will stop new and zero-day malware downloads, attempts to access malicious URLs, and communications with botnet C&C servers.
4. **Protect against evasive threats with sandboxing.** Today's malware developers are incorporating many different tactics to evade detection by traditional technologies. A cloud sandbox array is a new capability that can sit in-line with an email security gateway to protect from today's evasive malware.
5. **Use a password management tool and multi-factor authentication.** Password re-use makes phishing attractive for criminals. A breach into one system containing user names and passwords will likely be exploited to access other systems.
6. **Deploy endpoint security with active/behavioral monitoring.** Malware and ransomware evolve quickly and you need to augment traditional AV with next-generation detection.
7. **Patch early, patch often.** Outdated operating systems, browsers, and plugins are major vectors for malware infections.
8. **Back up regularly and keep a copy off-site.** If your files are ever encrypted by ransomware, then you can simply restore them after removing the ransomware. You should test that your backups can be restored-don't wait till an emergency!
9. **Turn off network shares and unnecessary admin rights.** Current malware exploits sharing vulnerabilities and seeks out mapped network drives with large file repositories. Also, some malware leverages admin privileges.
10. **Train users.** Educate users about the social engineering tricks that are used.

Consult us about Cyren's security services:

Email Security   Cloud Sandboxing   DNS Security

www.Cyren.com   sales@cyren.com