CONSTRUCTIONDIVE

SPONSORED

Who says you can't fight ransomware attacks?

Published Aug. 2, 2021

SPONSORED CONTENT BY EGNYTE

They go by cheeky, even beguiling names like SamSam, Locky, WannaCry, and Reveton. You know these names better for the untold pain, suffering, and loss they create through ransomware data theft and extortion.

What makes this scourge even more harrowing is the way criminals actively focus on construction companies. No wonder many industry leaders ask, "Why us? We're a construction company. What do we have worth stealing?" It turns out plenty.

First, a quick look at the new normal by the numbers:

- **1 in 6:** Construction companies reported a ransomware attack in the past year (it's believed most assaulted companies don't report it, fearing reputation damage)
- **74%:** Success rate for construction industry ransomware attacks (42.5% for other industries)
- **Every 11 seconds:** Cadence of ransomware assaults, costing business about $20 billion annually, according to Cybersecurity Ventures
- **$220,300:** Average construction industry ransomware payment

- **15**: Lost operational days in a typical construction company data breach

If you've experienced an attack, you understand the stakes. It goes beyond a catastrophic ransom demand. It's a terrorizing strike at the heart of your reputation and ability to maintain normal business operations. The viability of all current projects and bids is immediately jeopardized.

Existential Risk

Even if you're fortunate to have business insurance that helps recoup some or all of the financial loss, you're subject to increased premiums, reduced coverage, both, or summary cancellation. One way or the other, you pay.

"I've been with companies where a data breach is a life-ending event. They say, 'We can't pay. We can't recover from this. We're done,'" says Nick Espinosa.

Espinosa is a best-selling author, noted TED speaker, cybercrime consultant, and head of Security Fanatics, a global authority on cybersecurity and IT infrastructure defense. He understands why the bad guys prey on construction company data assets. Those crown jewels could include:

- Employee information
- Designs
- Bid data
- Profit/loss information
- Banking records
- Materials pricing
- Other confidential information

"First, let's be clear: Every vertical is under attack. No one is spared. Yet, construction is singled out because they tend to be cash rich and constantly under the gun to meet delivery targets. Construction companies are seen as more vulnerable and willing to pay," explains Espinosa.

Outpacing Security

There's another reason, too. Rapid growth in a booming economy is a double-edged sword. It's great for the bottom line, of course. But it can also mean cybersecurity gets left behind as companies accelerate their digital transformation. That leaves it to a typically overworked and understaffed IT department to battle a clever, relentless enemy.

"Construction companies don't invest enough in cybersecurity. They tend to be a bit behind. It's like hiring a specialty contractor. Do you want a drywall contractor to install your HVAC system? The skillset has to match highly talented and resourceful thieves. Cybersecurity is a specialty field that few companies have the internal know-how or time to keep up with," says Espinosa, noting the criminals' sky-high success rate in breaching construction company defenses.

New Paradigm?

Kevin Soohoo, Director, Construction and Engineering for Egnyte, a leading content management company, says the ransomware plague merits the same level of leadership commitment that worker safety commands.

"Construction projects are full of risk and uncertainty. Traditionally, project drivers were seen as a triad of labor, material, and equipment. For example, the industry has made great advances in safeguarding labor with highly tangible results," Soohoo says.

How tangible? Dodge Data & Analytics reports 72% of contractors say their safety program positively impacts their industry standing, with 66% asserting safety practices help lift business development.

Powerful Antidote

The risk posed by ransomware attacks begs the question, isn't it time to treat cybersecurity with fervor and focus as a safety management program? Lax attention to either one is a potential business crippler or killer.

The good news is the industry is starting to make this a regular topic, sharing best practices at the national level for notable trade associations like the MCAA and NECA, among others. In fact, the AGC IT Conference, one of the few construction events with a huge focus on Construction IT, is featuring three separate breakout sessions on Cybersecurity over the 2.5-day event.

Winning Strategy

Espinosa recommends companies insist on free and common-sense practices, like multi-step authentication on sign-in. This simple action often scares off a potential attacker—the hacker figures why bother defeating this obstacle when there are far more accessible targets available. Additionally, Espinosa advises a defensive strategy be formed around a third-party security assessment. "That's the right step to better sleep at night," he advises.

Another notable step is to partner with a content management company like Egnyte, top-ranked for data-centric security by G2, the independent go-to authority on business software. "Egnyte bakes in security much more stringently than most content management companies," Espinosa reports.

In a world marked by cyber thieves determined to upend your business, it makes sense to rethink long-held security assumptions. Consider implementing best practice cybersecurity measures that safeguard your data assets from the unthinkable.