Dermody, Burke & Brown, CPAs, LLC

Dimensions

A CPA's Report for the Construction Industry Summer 2022

Cybersecurity for Contractors

Guard Your Firm Against Devastating Cyberattacks

Hardly a week goes by without news of another cyberattack or data breach at a large U.S. corporation. These are happening across all different industries, from retailers and healthcare systems to internet and social media firms.

Contractors and construction firms aren't immune from the danger of cyberattacks. In fact, construction is the number one industry for ransomware attacks. Cybersecurity experts attribute this to some of the core processes that steer the industry, such as the proliferation of mobile devices and predictable schedules, as well as the growing use of technology to replace paper documents like project drawings, field directives, and purchase orders.

Ransomware attacks on Bouygues Construction and Bird Construction are just two high-profile cyberattacks in the construction industry. Now is the time to take proactive steps to help prevent your company from being victimized.

Ransomware and Other Attacks

Ransomware attacks occur when cyberthieves break into corporate systems and encrypt the company's data so you can't access it without an encryption key, which the attackers hold. They demand money (or a ransom) to release the key, effectively holding the company hostage. Businesses often have little choice but to pay the ransom if they want to access their systems and data.

But ransomware isn't the only cybersecurity threat construction firms face. Malware, business email compromise, and siegeware—which specifically targets smart building technology—are other major threats to contractors and construction firms. Successful cyberattacks can lead to costly downtime, workforce injuries, breaches of intellectual property (think sensitive blueprints and schematics) and bid data, and property damage due to compromised equipment.

Some small and mid-sized contractors believe they are at less risk from cyberattacks like ransomware than large contractors because they have less revenue. The opposite may actually be true: large contractors have greater resources to devote to cybersecurity defense, so hackers often concentrate on small and mid-sized firms they believe will be easier to penetrate.

Cybersecurity experts warn that siegeware could be the next big

Continued on page 3

Opportunity Zones

How to Realize Triple Tax Breaks

Everyone benefits when economically distressed communities are revitalized. This includes investors who have realized capital gains via the sale of real estate, closely held businesses, and other appreciated assets.

The Investing and Opportunity Act created Opportunity Zones that benefit both communities and investors. These are tax-based economic development tools designed to spur investment and create jobs in distressed communities. If you have realized capital gains on a prior investment, you can reinvest them in land, buildings, equipment, and other assets located within Opportunity Zones and defer the tax on the gain, as well as possibly realize other tax benefits.

How Opportunity Zones Work

Qualified Opportunity Funds (QOFs) are the vehicle used to invest in Opportunity Zones. A QOF must hold at least 90 percent of its assets in an Opportunity Zone. To qualify, an area must have a poverty rate of at least 20 percent or a median household income that's less than 80 percent of surrounding areas. There are currently more than 8,700 Opportunity Zones in the U.S. and five U.S. territories.

To realize the tax benefits of Opportunity Zones, you must reinvest capital gains in a QOF within 180 days of the asset's sale (or when capital gains would have been taxable). You can make QOF investments directly in tangible property (e.g., land, buildings, and equipment) located in the Opportunity Zone or indirectly through ownership of corporate stock or partnership shares by the QOF in a business that's located within the Opportunity Zone.

You must elect to defer capital gains by filing IRS Form 8949 with your tax return for the year when the gain occurred.

Paying the Deferred Tax

When you reinvest proceeds from the sale of an asset in a QOF, capital gains will be deferred until the sale of the QOF or December 31, 2026, whichever comes first. If you hold the investment in the QOF until December 31, 2026, you will pay the deferred tax using other liquid funds or by selling a portion of the QOF.

There are two other tax benefits to Opportunity Zones in addition to tax deferral:

- **Exclusion of capital gains –** If you hold your investment in the QOF for more than five years, you can exclude 10 percent of the deferred gains from income tax. And if you hold your QOF investment for more than seven years, you can defer 15 percent of the deferred gains from income tax. In other words, only 90 percent or 85 percent of the capital gain would be taxable.
- **Step up in tax basis –** If you hold your investment in the QOF for more than 10 years, its tax basis will increase to the fair market value on the day you sell it. In other words, your QOF investment will appreciate tax free, just like a Roth investment.

Note: If you sell your QOF investment in fewer than 10 years, you can roll the proceeds over into another QOF and still retain this tax-free benefit.

A Unique Opportunity

Opportunity Zones present a truly unique tax-saving opportunity for anyone holding appreciated assets. Not only can you defer capital gains on the appreciation, but you can also possibly eliminate a large portion of the deferred gain while eliminating all capital gains on the qualified Opportunity Zone investment.

Also, you don't have to reinvest all the proceeds from the asset's sale—you can reinvest just the capital gain portion of the proceeds if you prefer. This isn't the case with 1031 (or like kind) exchanges.

Be sure to consult with your tax advisor about whether investing in an Opportunity Zone makes sense for your situation.

We would be happy to talk to you about the benefits of Opportunity Zones. Call us to schedule an appointment.

Opportunity Zones: Who's Eligible?

A wide range of entities are eligible to invest in Opportunity Zones, including:

- Individuals
- Partnerships
- S corporations
- C corporations
- Multi-member LLCs treated as partnerships or corporations
- Trusts and estates

Guard Your Firm...

Continued from page 1

cyberthreat to construction firms given how much technology is built into facilities today. They report that cybercriminals are trying to highjack the automation systems of smart buildings. When successful, hackers gain access not only to the target building, but to other buildings it is connected to virtually.

IoT (Internet of Things) devices like worksite security and machine control present particular challenges to smart building owners. Cyberthieves can hack into IP cameras to observe worksite behaviors and examine materials to help plan an attack. They can also use drones to exfiltrate sensitive data from construction sites and interfere with work.

Causes of Data Breaches

According to the 2021 Verizon Data Breach Investigations Report, more than two-thirds (67 percent) of all confirmed data breaches were caused by leaked user credentials, misconfigured cloud assets and web applications, and social media attacks like phishing and spear phishing. Therefore, the first step to preventing cyberattacks is implementing a series of controls focused on these areas.

Start with employee education. Eighty-five percent of all data breaches involved a human element, according to the Verizon report, so you should provide comprehensive cybersecurity training to all employees—especially those with access to sensitive corporate information. All it takes is for one employee to open an attachment with malware or click a fraudulent link to open the cyber floodgates to criminals.

For example, teach employees how to recognize fraudulent emails and instruct them to never open attachments from unfamiliar sources or click suspicious links. Make sure employees understand the importance of setting strong passwords and keeping them secure. And instruct your accounting employees to confirm all wire transfers over the phone before initiating them.

Here are five more cybersecurity steps to consider:

1. Test your cyber defenses. One way to do this is to conduct penetration, or "white hat," tests periodically. In these tests, an outside entity (preferably a security consultant) will probe your IT system for weaknesses and try to hack in. Experts suggest conducting tests at least annually to uncover weaknesses in your cyber defenses so you can patch them.

2. Back up your systems regularly. This is the best defense against a ransomware attack because if your data is backed up the hacker has no leverage. Also keep your software and operating systems updated with the latest security patches. The best way to do this is to enable automatic updates.

3. Focus on remote security protocols. This has always been critical for contractors given how much work takes place in the field, but it has taken on added importance due to the growing number of employees who are now working remotely. Make sure remote employees' home Wi-Fi networks are secure and that antivirus software is loaded onto their digital devices. Also consider installing a virtual private network (VPN) for remote workers to use.

4. Ask your vendors about their cyber defenses. Given the interconnectedness of today's world, your firm's cyber defenses are only as strong as those of your vendors and partners. Find out about their cybersecurity practices by having vendors complete a Service Organization Controls, or SOC 2, report. This will detail which types of controls vendors have in place to guard against cyberattacks.

5. Create a cyberattack incident response plan. No matter how robust your cyber defenses, there's still a chance you might suffer an attack. You need a detailed plan of action to minimize damage. The plan should explain in detail the procedures you will follow in the aftermath of an attack, including which employees are responsible for which specific duties.

Make It a Priority

Cybersecurity threats aren't likely to diminish anytime soon. In fact, they'll likely increase going forward. That's why cybersecurity should be a top priority for construction firms.

Think about how you can implement strategies like these to protect your business from a devastating cyberattack.

Contact us to talk about cybersecurity in more detail.

New Lease Accounting Standard is Now Effective

After several delays, the new lease accounting standard has finally taken effect. The effective date for ASC 842 is January 1, 2022 for calendar year-end private companies.

ASC 842 requires all lease obligations to appear on the balance sheet as a right-of-use (ROU) asset and lease liability. Previously, payment obligations of operating leases were not reflected on the balance sheet. As a result, future debts, which could reflect significant financial liabilities, were practically invisible on the financial statements. Lease payments were mentioned in the financial statement footnotes, but not prominently with other liabilities.

Here are three important things to keep in mind as you prepare to implement the new lease accounting standard:

1. Lease definition – ASC 842 includes a new lease definition: "A contract, or part of a contract, that conveys the right to control the use of identified property, plant, or equipment (an identified asset) for a period of time in exchange for consideration." This definition specifies four main lease characteristics: an identified asset, the right to control the use of that asset, a set period, and consideration.

2. Embedded leases – Under ASC 842, all leases create a lease liability and ROU asset on the balance sheet. Look carefully at all service agreements and contracts to determine if they contain an embedded lease. If they do, you'll need to account for the lease according to the new standard.

3. Lease term – The lease term is defined as the noncancellable period during which a lessee has the right to use an underlying asset. This term should be based on the period during which the contract is enforceable. ASC 842 takes a position of "form over substance" regarding lease agreements—this emphasizes the contractually enforceable terms and conditions of the lease.

Give us a call if you have more questions about ASC 842.