FrankelZacharia LLC

Certified Public Accountants

Are You Up to Date on Cybersecurity for Your Manufacturing Company?

Frankel Zacharia shares some hidden areas that may present threats to your manufacturing company's cybersecurity.

Cyberthreats are increasing for manufacturers, especially because of the advanced level of technology that governs processes and activities. A notable example is the recent cybercrime uncovered at Tesla. An employee there was offered $1 million to insert malware into Tesla's network systems. Fortunately, the employee alerted the company and the FBI, and the threat was avoided.

High-profile companies are not the only targets of cyberattacks today—threats such as this example are unfortunately becoming more common among manufacturing companies of all sizes. Small to midsize companies are especially vulnerable in three key areas:

1) **Risks From Your Supply Chain**

Your business partners, suppliers and other members of your supply chain may pose a very real threat to your systems. Each day, they send your company emails, promotions and invoices. You may even share software programs that are critical to your manufacturing processes. Because the sender appears familiar, your employees may quickly and automatically respond to emails, pay electronic invoices or click on a link without following some simple due diligence steps. Cybercriminals trick employees by making small changes to email addresses or automated templates, and then using these false communications to insert malware into a company's IT systems. By developing and adhering to cybersecurity protocols, and providing employees with ongoing IT security training, you can instill a culture of vigilance against cyberthreats for email and internet use.

2) **Failing to Update Software and Hardware**

It's easy to fall behind on updating software and hardware when other, more pressing issues draw on your time, attention and funds. However, updating hardware and software may be one of the best ways to protect your company against potential cybercrimes. Because cybercriminals are continuously trying to break down barriers, IT companies are continuously updating software to patch holes in security. If you fail to update software and fall behind, or if you have not upgraded the hardware that holds your sensitive client and company information, you could be putting your company at risk. To remedy the situation, begin by checking for the latest versions of your hardware and software with system manufacturers to see if potential updates are available. It may require a small cash outlay to catch up, but this small investment will prevent larger, more expensive cybersecurity problems from occurring.

3) **Unexpected Points of Entry**

It may seem like something out of a science fiction movie, but cyberattacks can occur through “smart” appliances such as refrigerators, coffee makers and HVAC systems. These smart appliances and building systems are part of your company’s network and thus provide access points for malware to gain entry into your IT systems. Any common technology that is connected to your wireless internet poses potential security threats that give hackers the ability to see and control everything taking place on that particular network. By updating hardware and software with appropriate firewalls and cybersecurity features and exploring the potential risks with smart appliance manufacturers, you’ll be able to protect your company against this type of threat.

It’s important to stay alert to the changing nature of cyberthreats to keep your company’s sensitive customer and business data secure. Cyberattacks can happen to companies of all shapes and sizes, not just the Teslas of the world. The best defense is to remain vigilant and adaptable to protect your company’s sensitive information.

Questions on Cybersecurity? Please contact Brandon Nyffeler by phone at 402.963.4365 or by email at bnyffeler@fzacpa.com.