TOP TRENDS AND TOPICS FOR MANUFACTURERS

After a turbulent 2020, here's what to be aware of in 2021

By Cheryl Aschenbrener, CPA

From a life-altering global pandemic to the tumultuous 2020 election, manufacturers and distributors experienced a year unlike any other. It should be no surprise that planning for 2021 and beyond will be different than it has been in the past.

As a result of these changes, we've identified top-of-mind trends and topics manufacturers should pay attention to, including the following:

- Potential tax implications resulting from the recent election and what manufacturers can expect for the next four years
- The Cybersecurity Maturity Model Certification — a crucial topic that will affect manufacturers beginning in 2021
- Best practices to prevent against ransomware and phishing attacks at the company level, especially in a remote working world

Bracing for a new tax landscape

Throughout the 2020 presidential campaign, President Joe Biden proposed various tax law changes for individuals and businesses. While new tax reform would require support from the House and Senate, we can presume Biden will be eager to implement his proposed tax changes.

Biden's campaign proposed a tax increase to fund a clean energy program that combats climate change. Biden also advocated imposing higher Social Security taxes for individuals earning more than $400,000 and taxing capital gains as ordinary income for individuals with higher incomes. According to his campaign website, Biden will look to repeal aspects of the Tax Cuts and Jobs Act and enact higher individual income tax rates for taxpayers with incomes over $400,000. His plan will also increase the corporate tax rate to 28% from 21% and impose a 15% minimum tax on companies' book income.

These proposed changes would alter the current tax landscape, as Biden supersedes a Republican president mostly in favor of supporting Big Business. However, Biden has supported an implementation of manufacturing incentives that would induce demand for U.S. products, expand the R&D credit and strive to revitalize manufacturing facilities.

Preparing for the Cybersecurity Maturity Model Certification (CMMC)

Although this is a new area of compliance, manufacturers whose products are involved in any way in the supply chain of the Department of Defense (DOD) should become familiar with this important certification. The CMMC verifies that the confidential and personal material of companies that maintain contracts with the DOD are protected from misuse, thus meeting cybersecurity standards of protecting the companies. According to the Office of the Under

> *While the cyber protections on servers and computers in your corporate office or warehouse might be top-notch, remote employees may be lacking proper security at home, leaving your company vulnerable.*

Secretary of Defense for Acquisition & Sustainment, "The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks."

For those manufacturers providing contractual or vendor services to this branch of the U.S. government, this compliance requirement is expected to go into effect in early 2021. Certification assessments will be performed by a third-party organization and are mandatory.

Preventing ransomware and phishing attacks

While most manufacturing companies still have the majority of their employees on the floor, it's likely that at least some of their back office, accounting or human capital staff are working from home during this ongoing pandemic. We've seen an increase in phishing attacks — which is when hackers send your employees (sometimes convincing) emails that contain a malicious link or embedded attachment. Phishing attempts increased significantly in 2020 as many Americans began working from home, and email is the preferred and most utilized form of communication. While the cyber protections on servers and computers in your corporate office or warehouse might be top-notch, remote employees may be lacking proper security at home, leaving your company vulnerable.

You may not think a compromised remote employee's access is an issue for your company as a whole, but it is. If a hacker can access your organization's server by guessing or obtaining an employee's password, they are likely able to access the critical application servers that keep your manufacturing business running. With this comes the risk that your confidential employee, financial and customer information can be read, copied or deleted. In many scenarios, factories are forced to shut down temporarily to retroactively address a compromise.

Best practices to prevent against costly and dangerous cyber breaches include implementing a multi-factor authentication system, in which remote employees can access company files only after providing a password on two devices (a computer and phone, for instance). You can also hire a third party to simulate a phishing attack: The third party would send a mock phishing email to your company's employees and determine how many people click the link and fall victim to the artificial attack. This could assist in analyzing your current cybersecurity strategy and showing you where improvements may be necessary.

Conclusion

2020 has been a year we won't soon forget. As manufacturers dive full-steam ahead into 2021, they should develop thorough, strong cybersecurity practices, prepare for the CMMC requirements and carefully analyze their tax situations for opportunities and shortfalls.

Cheryl Aschenbrener, CPA, is a partner and the national leader of transaction advisory services at Sikich LLP in Brookfield. Contact her at 262-317-8514 or cheryl.aschenbrener@sikich.com.