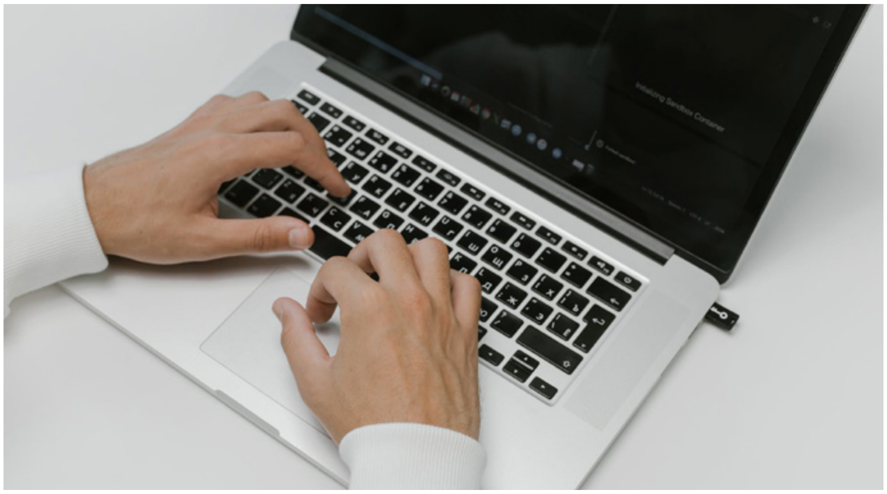
UHY LLP
Certified Public Accountants

STAFFING INSIDER

VOLUME 1 :: ISSUE 3

In This Issue:



CYBERSECURITY READINESS

As the leader of your staffing organization, the future wellbeing of the company rests on your shoulders, which includes the security of your network, data, and proprietary customer information. Every week in the news, there are reports of companies that have experienced cyber-attacks. While you think it will never happen to you, there is a good chance it could.

Since most likely you are not an information technology (IT) expert, here are six key questions you can use to have a discussion with your IT team about your current cybersecurity readiness.

1. Do we have a robust incident response capability in place?

What you want to hear
Yes, we have software that provides alerts and possibly a third-party provider to help monitor our system around the clock and responds through quarantine or other isolation capabilities.

Warning sign
No, we do NOT have anything in place to monitor anomalous or known bad activity on servers, workstations and laptops at all hours.

What can be done immediately
At a minimum, IT should consider deploying a next generation, endpoint detection, and response security tools. This type of software is quick to deploy and provides visibility and alerts to help quarantine the infected machine(s) and minimize the extent of the disruption. Better solution options, include active response on your behalf by the trusted monitoring companies.

2. Do we have a program to scan our network and applications for vulnerabilities?

What you want to hear
Yes, our company has a regular program to scan our network, applications, web services, and networked devices inside and from the internet in place.

Warning sign
No, we do NOT regularly scan our network, software applications and device configurations.

What can be done immediately
Cunning cyber attackers are ready to take advantage of vulnerabilities. Ask IT to conduct a vulnerability scan as soon as they can to begin to identify

Continued on Page 2...

Continued from Page 1...

and patch or remediate any high risk and critical vulnerabilities. At a minimum this should be done quarterly on internal assets and from an internet perspective. For the first few months request the results of the scan.

3. Do we have good backups of critical systems, data, and configurations?

What you want to hear
Yes, in case of a cyber event, our company has good backups of critical systems, data and configurations and we have tested them. The back-ups are stored offsite or in the cloud so they won't get damaged or deleted.

Warning sign
No, we do NOT have the ability to successfully restore operations from a backup and/or back-up files are onsite.

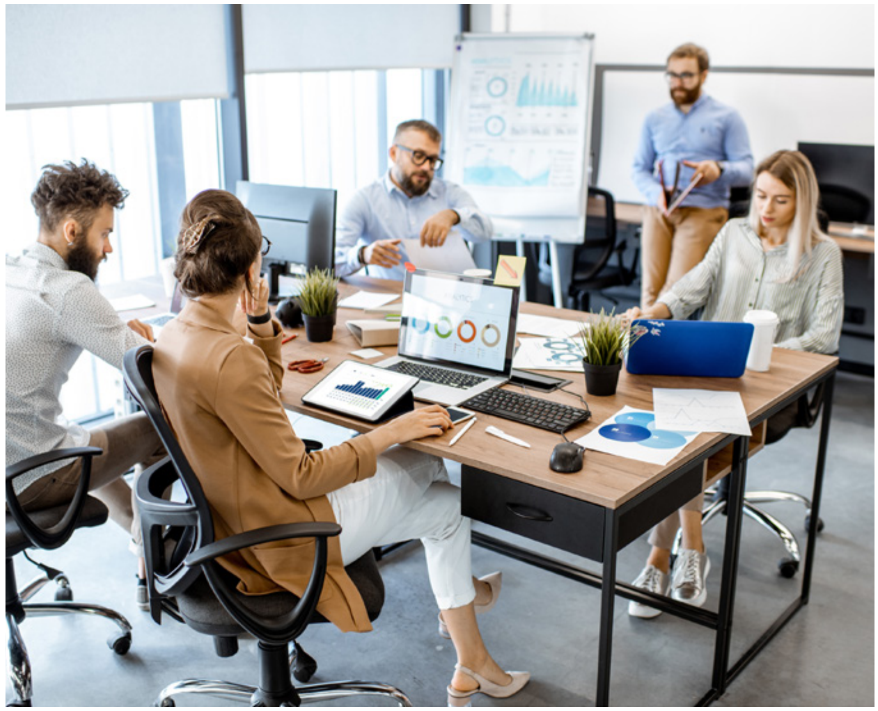
What can be done immediately
Work to minimize business continuity risk with your important systems. Confirm that all IT systems are included within the backup solution and ensure that they are tested periodically to work when needed. Treat backup files as critical data and ensure the backups are segmented and isolated from the rest of the network. Also, ensure a full copy of the backups is stored offsite and is inaccessible to any ransomware or malware that might break loose in your environment.

4. Do we have an incident response plan for a cyber-attack?

What you want to hear
Yes, our company has a solid plan in place that has been regularly tested and our employees understand their roles and actions depending on the situation.

Warning sign
No, there is NO cyber-attack or overall incident response plan.

What can be done immediately
You can't wait for a cyber-attack to occur to build an incident response plan. At a minimum, identify who your



employees need to contact if a cyber incident is happening. Document the expected actions to be performed in the event of an incident and perform some tabletop tests of the plan before a real event occurs. You may want to consider a cyber 911 call service that will quickly focus the incident response activities to stabilize the environment and begin the recovery process.

5. Do we have an employee security awareness program?

What you want to hear
Yes, our employees are our best source of defense and we have a continuous testing program in place, so our staff stays alert and vigilant.

Warning sign
No, our employees do NOT understand the extreme threat that phishing emails can pose to our company.

What can be done immediately
Phishing emails remain the easiest and most likely way to get into your business to steal data, access your internal network or begin the staging of malicious software. IT or an outside vendor can build an internal program to train and educate them about suspicious emails in their inboxes, instant messages, texts and calls.

6. Do we have cyber insurance?

What you want to hear
Yes, we have a cyber insurance policy that clearly outlines what the policy does and does not cover and we understand the carrier's role versus your role. For operational risks not covered by insurance, our company has taken the proper steps.

Warning sign
No, we do NOT have a cyber-attack or overall incident response plan.

What can be done immediately
Don't put your company's brand, your clients' trust and your future are at risk. An insurance broker can provide guidance on a policy and help you manage your risk appetite for a cyber loss. Ask specific questions on what losses are covered, including such things as public relations, ransomware payments, incident responders, and digital forensics.

WHAT TO EXPECT FROM A BIDEN ADMINISTRATION AND HOW TO MINIMIZE YOUR TAX LIABILITY

In the past year, US government spending has exploded due to the COVID-19 pandemic and economic recession. Relief packages total upwards of $6 trillion to date, and the new Biden administration has plans to continue spending in various packages investing in the future of the United States. We expect the Biden administration to offset these programs and stimulus spending by raising taxes. We've already seen changes in the American Rescue Plan Act (ARPA) and have an idea of what tax legislation the new administration plans to propose moving forward.

Based on campaign promises, new spending proposals, and the current split in Congress, tax professionals can gauge what to expect and how to prepare for changes affecting the IT and engineering staffing industry.

Passed legislation

Joe Biden passed the ARPA early on in his term. The bill includes the following:

- Unemployment compensation
- Stimulus checks
- Expanded child tax credit with advanced payments
- Excess business loss limitation – extended through 2026
- Employee Retention Credit
- Paid sick and family leave tax credits
- Payroll Protection Program

The two significant aspects that affect the IT and engineering staffing industry are the Employee Retention Credit and PPP.

Employee Retention Credit

The Employee Retention Credit has been extended to the end of 2021. Qualifying businesses are provided with the tax credit if they were fully or partially shut down or have incurred a decrease in revenue of more than 20% compared to 2019.

The requirements are different for 2020 and 2021, so be sure to do your due diligence in determining if your business qualifies. For 2020, companies receive a credit for 50% of qualified wages and healthcare costs, capped at 5k per employee for the year. Qualifying businesses will receive a credit of 70% of qualified wages and healthcare costs, and the maximum credit for each employee is $7k for 2021.

According to Alison Dunleavy, many businesses mistakenly presume they are eligible for ERC but fail to meet the requirements. It is essential to fully understand the qualifications for each year.

Proposed legislation

The Biden administration has already proposed two huge packages in the American Jobs Plan and the American Families Plan. Each package is currently structured to cost about $2 trillion. While we haven't seen a counterproposal from the Republicans, Tom Sena from UHY Advisors expects to see a compromise if the new packages are passed.

Paying for these packages will fall on America's top earners; the IT and engineering staffing industry needs to prepare for a corporate, individual, and estate tax increase.

Tax increases

Biden plans to raise the corporate tax rate from 21% to 28%. Tom Sena believes increasing this rate will make the US much less competitive on a global scale. The new administration is also expected to crack down on companies that offshore their business. One means of acquiring unpaid taxes from American companies is placing a 15% minimum tax on book income. There are also efforts to create a global minimum tax; however, this would need the support of many nations looking to attract American businesses looking for lower tax rates.

The Biden administration hasn't formalized their tax plan but consistently references the $400k income level. It is unclear if this amount is the amount for households or individuals, but Tom Sena feels earners making over this amount can expect a tax increase and prepare.

Significant changes in capital gains taxes are expected. Sena recommends that owners of highly appreciating assets seriously consider gifting, transferring, or selling before new tax legislation is passed.

Alison Dunleavy warns business owners who are planning to pass along their assets or cash will face a higher tax rate. The gift tax exemption is expected to decrease from $11 million per individual to somewhere between $3.5 and $5 million. Couples with combined assets above that threshold are potentially exposed to a 40% estate tax rate. She suggests considering reviewing your current estate plan and discussing different vehicles to preserve and transfer wealth sooner rather than later.

Minimize your future tax burden

While the tax structure hasn't changed to date, and to pass significant legislation such as a tax increase takes 60 votes in the Senate, it is essential to be prepared for notable changes in 2021. Business owners and employees in the IT and engineering staffing industry need to be proactive in receiving tax credits from the ARPA and preparing for future tax increases from the Biden administration

COST OF PERFORMANCE VS. MARKET APPROACH TO SOURCING REVENUE

Calculating how to source gross receipts is a key element in determining a staffing company's state income tax liability. Staffing companies operating in multiple states should be aware of the growing trend in which states are migrating from a cost of performance based sourcing method toward a market-based approach when determining where to properly source gross receipts derived from sales of services.

Under cost of performance (COP), receipts earned from performance of services are apportioned to the state based on the location where the taxpayer incurs expenses associated with providing those services. For example, assume Company ABC has all its property and employees in State A. State A uses the cost of performance for sourcing receipts from services. Company ABC clients are located in states B and C. Since State A had adopted the cost of performance rules, all of ABC Company's revenue would be sourced to State A as the COP is incurred entirely in State A.

However, if state A had opted for market-based sourcing rules, Company ABC could potentially be sourced to State B and C. Under the market-based approach, the taxpayer assigns sales of services to the state in which the services is received or where the benefit of the services is received. The market approach attempts to better match the receipts to the source of the corresponding revenue stream. The market approach also collects more tax from out of state businesses with significant economic activity, but have little in the way of payroll or property.

States differ in applying the market-based sourcing rules. In general, market can be defined in the following ways:

- Where the benefit is received
- Where the service is received
- Where the service is delivered
- Where the customer is located

Most states using market-based sourcing use a single factor sales apportionment instead of a traditional three-factor apportionment (this involves using a percentage based on property, payroll, and sales located in a state). It is possible for a taxpayer to pay no tax on a portion of their service revenue in states that have a single sales factor apportionment. For example, Company ABC has offices and employees located in State A. ABC Company has clients that are located in State D. The clients receive the benefits of ABC Services in State D. State D uses a COP based receipts for sourcing revenue whereas state A uses a market approach to sourcing revenue.

Both State A and D use a single factor sales apportionment. Under State D's COP based rule, the revenue would not be sourced to State D because the expenses associated with providing the services are incurred in State A. Therefore, in this example, income is not allocated to either State A or D.

It is also possible for taxpayers to have "double taxation". If in the above example, State D utilized a market approach and State A utilized a COP based sourcing, State A would allocate all of ABC's revenue to State A (where the services are performed, and the cost of services are incurred) and State D would allocate the revenue to State D (where the benefits of the services are received). In this example, the same revenue would be attributed to both states and subject to tax in both states.

Staffing companies need to review their current operations to identify and if possible to reduce the risk of double taxation. Tax planning should be examined to avoid under or over allocating income to states.

> "Calculating how to source gross receipts is a key element in determining a staffing company's state income tax liability."

EMPLOYING CONSULTANTS IN MULTIPLE STATES – A PRACTICAL APPROACH TO BALANCE TAX COMPLIANCE AND RISKS

The IT and engineering staffing industry has historically worked with consultants from various states. Many firms operate without complying with state and local tax obligations subjecting themselves to unnecessary risk. Balancing the costs and the risks for staffing in multiple states can be done by taking a pragmatic and thorough approach.

State and local tax basics

Navigating state and local tax law is a process that requires firms to be aware of definitions and facts outlined by individual states. The staffing industry is especially complicated because states approach different services we provide in unique ways.

Staffing firms need to be cautious when filing taxes with consultants in other states and not be too broad. Doing the research and understanding how each service is defined is imperative in avoiding tax penalties.

Taxability of services

In preparation for filing taxes, staffing firms need to be aware of how each state defines services. Services are subject to sales tax in some states, making attention to detail even more important.

Apportionment

The goal of apportionment is to compute the percentage of total profits that would be attributable to a particular state to pay income tax for that state. States have used a three-factor formula that includes payroll, property, and sales. More states are moving away from a three-factor formula to a sales factor in order to collect additional taxes. States use a cost of performance approach or a market approach in apportioning sales.

Staffing firms should track relevant data and manage state tax risk.

Working with multiple tax jurisdictions can be complicated, but if your tax department is clear on the state laws and is sourcing receipts, there shouldn't be any surprises come tax season.

Voluntary disclosure agreements

A voluntary disclosure agreement (VDA) is a binding legal contract between an entity and the state to provide full transparency and pay its tax obligations in exchange for reduced penalties. During an audit, states can collect over a decade of unpaid back taxes; if a VDA is agreed upon, the state can limit the look back period to 3-4 years. Another advantage of a VDA is that negotiation is often done anonymously.

Coming clean with your taxes also has disadvantages, especially if unpaid taxes are owed. It is essential to be prepared before applying for a VDA. Any missing details can void the agreement, and states have varying requirements. Do not voluntarily expose yourself or your organization if you haven't thoroughly examined your financials.

Facts and definitions matter

Our tax professionals stress that staffing firms should thoroughly examine where their consultants are working, especially as we have experienced more remote work. Understanding the source of services and individual state tax laws is crucial in avoiding penalties.

STAFFING INDUSTRY INSIGHT

Today's staffing organization is growing at a rapid pace and needs to have a team of financial services professionals that responds quickly to change. The average staffing company has outgrown the typical accountant and developed the need for a CPA firm with a deep industry focus. Our firm's National Staffing Practice has the skill set to anticipate and respond to the needs of your business by providing solutions that give you a competitive advantage.

OUR LOCATIONS

We have ample locations across the country with a heavy regional presence in the Great Lakes, Mid-Atlantic, Midwest and Northeast. Visit uhy-us.com to find an office near you.