ISSUE 82 • WINTER 2020

BIZGROWTH STRATEGIES

IDEAS TO HELP GROW YOUR BUSINESS

3 Stories That Could Affect Your Accounting in 2020

6 Keys to an Effective Benefits Communication Strategy

Takeaways from 2019's Biggest Information Security Incidents

Recruiting in a Seller's Market

Top 2 Trends in Management Liability

CBIZ

Your Team.

In This Issue

CBIZ CBZ
CBIZServices BizTipsVideos

To view this newsletter and past issues of *BIZGrowth Strategies* online, visit **cbiz.com/news/newsletters**.

To subscribe to this newsletter or a variety of others, visit **cbiz.com/newsletter-subscribe**.

You can also call us at **1-800-ASK-CBIZ** (1-800-275-2249).

CBIZ in the News

The Wall Street Journal
Tiny tax moves can save you big on Medicare premiums
November 22, 2019

FoxBusiness.com
Taxing college athletes' scholarships? How it could work
October 30, 2019

Fast Company
Can you ever wear shorts to work?
September 4, 2019

For more articles, visit **cbiz.com/news/in-the-news**.

Tax & Accounting

3 Stories That Could Affect Your Accounting in 2020

BY **MARK WINIARSKI**

As your organization fine tunes its strategy in the New Year, you're likely monitoring different trends. From the global markets to issues closer to home, here are three major stories that may affect your accounting in 2020.

Global Economic Uncertainty

There is quite a bit of global economic uncertainty. With countries including China and India experiencing slower growth and the United Kingdom's "Brexit" from the European Union, the global economy could face a recession. A slowed transport of goods in and out of the United Kingdom, trade conflicts and worry about the long-term repercussions of a slow-down could lead to a difficult year.

Climate change presents another major risk factor for the economy in 2020. As many areas see record flooding, extreme temperatures and drought, companies may struggle to maintain their bottom line. There could also be long-term consequences; a 2019 study from the International Monetary Fund (IMF) projects a 7.22% decline in global GDP by 2100. The study suggests the dip could result from the effects that higher temperatures have on industries, including agriculture, manufacturing and tourism.

Global uncertainty may increase the challenges in evaluating accounting estimates such as impairment assessments and fair value. Public companies may need to consider and enhance risk disclosures made in their required SEC reports.

Tariffs

Tariffs are often understood as an additional cost imposed on the exporter of foreign goods, but they are actually levied against the importer of those goods. It is typically the country issuing the tariffs that is most affected by these taxes as importers decide whether to raise their prices or seek alternative measures to lower costs in order to offset tariffs.

As trade conflicts continue and tariffs are levied that make imports less desirable for consumers, this could quickly create challenges for American companies' cost accounting and accounting estimates. If your business has been directly affected by the tariffs, you may benefit from an adjustment to your accounting policies in order to effectively handle the impact on your business and prevent additional complications.

Cybersecurity

One of the biggest threats facing global security today is cyberattacks. And as regulations and best practices continue to evolve at the local, state, federal and global levels, companies will likely have their hands full maintaining compliance and improving their data protection efforts. Cyber risk assessments will continue to be important planning tools. Cybersecurity presents liability issues and requires management oversight. Public companies will also be responsible for cybersecurity disclosures.

Another movement to watch is activity around data protection laws. As the EU's General Data Protection Regulation (GDPR) wraps up its second year, the U.S. federal government is considering how national cybersecurity regulations may be used stateside. Preparing for increased cybersecurity regulations now could help your organization make a much smoother transition if or when new rules are introduced.

Companies that are mindful of these accounting trends are more likely to be prepared for a successful year. Working with an accounting advisor who understands the emerging developments and their potential impact on your business can help ensure a successful 2020.

MARK WINIARSKI
CBIZ MHM, LLC
mwinarski@cbiz.com | 816.945.5614

Employee Benefits

6 Keys to an Effective Benefits Communication Strategy

BY **ALEX LANNING**

A year-round benefits communication strategy is critical to your plan's success, your HR team's sanity, and your employees' engagement and satisfaction. These six tactics are key to ensuring that strategy is effective:

1. Set clear goals.

Start with being in tune with what drives your business strategy and your benefits strategy; this will help you identify goals for your communication strategy. For example, if you're focused on managing costs, your goals might include getting employees to the best providers or decreasing unnecessary health care spending. Further, sit down with your team to determine where things didn't go quite as well as planned last year and set goals to improve in each of those areas.

2. Segment your audience.

Segment your employee population – based on things like location, key demographics, tenure, job function, etc. – to ensure you reach them in the most efficient and effective ways possible. Consider the communication challenges with each group, for example:

- In-office, tech-savvy employees – emails often go unread
- Satellite office employees – less available hands-on help from HR
- Remote employees – low engagement; employees are mobile and can be distracted
- Employees with families – high responsibility with extensive coverage needs; spouse may make benefits decisions
- English as a Second Language (ESL) employees – may prefer communication in their native language
- Manual laborers – less online access

Once you identify these groups, you can determine what methods of communication will be best, which most likely will be a combination of channels.

3. Create a unique benefits brand.

A brand is not only the logo, color scheme and tone used in communications; it is also the feelings it evokes when seen. A brand helps create a consistent and predictable experience, which builds trust and comfort.

When developing a benefits brand, your goal should be to capture your employees' attention, which in turn will drive engagement and action. And, while your benefits brand should be unique and recognizable, it should also connect to your organization's overall brand.

4. Develop informative yet simple messaging.

One of the most common messaging mistakes made is including too much information and/or detail. When this happens, there's no way for employees to quickly and easily digest the information. As a result, they're more inclined to skip the communications altogether. Try these messaging best practices:

- Write the way you speak.
- When possible, address only one (ideally) or two benefits topics per communication.
- Break up complex topics into smaller, more manageable pieces.
- Use graphics to visually convey information and/or to break up text.
- Use easy-to-understand language; leave the industry jargon behind.

5. Utilize a multi-channel communication approach.

A multi-channel approach will help you address employees' different communication preferences and learning styles. Be sure to consider the full range of options when developing your plan, including:

Face-to-Face

- Benefits fairs & lunch-and-learns
- One-on-one
- Group communications

Online & Mobile

- Videos & webinars
- Social media
- Email
- Apps
- Text

Information Portal

- Benefits website/micro-page
- Company intranet
- Interactive benefit guide

Materials

- Benefits guide
- Direct-to-home mailers
- Posters & flyers
- Newsletters

6. Prepare a year-round communications calendar.

Communicating benefits year-round, not just during open enrollment, is crucial. For the majority of people, there is a huge learning curve when it comes to being able to confidently navigate the benefits world. A steady distribution of this information will make understanding the information much more manageable and less stressful. It will also increase engagement and make it simpler for them to make the best benefits decisions. Year-round communications will also decrease the quantity of employee emails, calls and other inquiries that HR must handle.

Know that your benefits communication plan will naturally evolve over time. However, to ensure it improves over time, you must measure its success to identify what's working and what's not. This will provide you with the information necessary for you to appropriately adjust your strategy moving forward.

ALEX LANNING
CBIZ Benefits & Insurance Services, Inc.
alanning@cbiz.com | 816.945.5594

Human Resources

Recruiting in a Seller's Market

BY **JAY MESCHKE** & **LESLIE SHAW**

Despite some early signs of economic slowness, the employment markets are by and large still hot – white hot. What does this mean? Simply said, it is a seller's market. Prospective candidates are being bombarded with new and exciting opportunities to consider. The opportunities are coming from executive search firms, proactive talent acquisition professionals and that thing called the internet – with portals and job boards a plenty – enticing talent to raise their hands or consider answering a call, text, LinkedIn inquiry and a host of other outreach techniques.

When a seller's market exists, there are several strategies and tactics an organization should employ to combat such an environment.

The first is to collectively recognize that the seller's market exists in the first place. Without such recognition, companies default to historical and time-tested processes when filling vacancies at all levels in their organizations. In a seller's market, a hiring entity must change its processes by shifting gears into hyper-drive or risk losing out on high-potential individuals who are being courted by a more nimble, creative and proactive competitor.

(Continued on page 7)

Takeaways from 2019's Biggest Information Security Incidents

BY **CBIZ RISK & ADVISORY SERVICES TEAM**

Sometimes looking to the past helps us understand the current risks to information security. Examining the information targeted and how unauthorized users tried (or did) access an organization's information can illuminate the cyber risks that may exist within your organization.

American Medical Collection Agency (AMCA) Breach

Third-party providers' risks are your risks. The AMCA breach, related to a six-month-long unauthorized intrusion, affected the patients of the companies who had been using the agency for bill collection. Combined, almost 20 million patients from LabCorp and Quest Diagnostics had their names, dates of birth and data on their medical services compromised. The size of the breach and the associated costs with fixing it resulted in the company operating the AMCA to file for Chapter 11 bankruptcy.

Key Takeaway: Consider Third-Party Controls

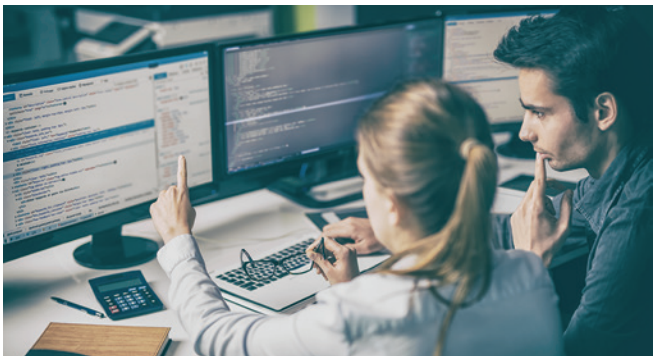
Your organization should have ongoing conversations with third-party service providers about their information security protocols. Failures in a third-party provider's system and organization controls can be catastrophic for everyone as those whose personally identifiable information is compromised will not be as concerned about *where* the failure in controls happened as much as about *why* it happened.

Baltimore's Ransomware Attack

No one is completely safe from information security risks. The City of Baltimore experienced a ransomware attack in May where outside attackers used a vulnerability in the city's computer operating systems to effectively take all servers offline. Hackers asked for 13 bitcoin (roughly $76,280) to restore access to the affected servers, but the City of Baltimore refused to pay. City officials estimate an $18.2 million recovery cost from the so-called RobinHood ransomware attack, which includes revenues lost during the nearly two-week-long lockout and the city's investments in system upgrades to help prevent future information security incidents.

Key Takeaway: Cybersecurity Takes an Investment

Improvements to information security systems will likely take a significant investment. The City of Baltimore reallocated $6 million to pay for critical information



technology infrastructure and is also looking to add cyber liability insurance coverage. It's important to note that evaluating additional protections or upgrades can mitigate risks, and creating a multi-year implementation plan may make information security a more manageable investment.

Capitol One Data Breach

In July, Capitol One learned that an unauthorized user had gained access into customers' Social Security numbers, bank account numbers and credit card application data. FBI investigators quickly identified the perpetrator as a former software engineer who had worked for Capital One's cloud hosting company. The perpetrator gained access through a firewall misconfiguration on a web application, but law enforcement stopped the perpetrator before credit card information was compromised. Capital One estimated that around 100 million individuals were affected in the U.S. and 6 million in Canada. It estimated that less than 1% of its customers' Social Security numbers had been captured.

Key Takeaway: Cybersecurity Policies Are Effective

Your organization should have a clearly defined process for notifying law enforcement of a cyber incident. Capital One's breach detection and notification processes appeared to work as designed. Its protocol helped make what could have been a devastating breach much less severe.

If you need assistance evaluating your cybersecurity strategy stands, you may want to enlist the help of an information security specialist.

CBIZ RISK & ADVISORY SERVICES TEAM
www.cbiz.com/ras

Second, set strict deadlines for each recruiting assignment. It is often the case that hiring entities inadvertently lengthen recruiting cycles by relying upon a multitude of one-on-one interview sessions. Instead, use group interview formats, presentations and/or auditions, and video interviews.

Third, develop a transparent and trusting relationship with a recruit to the point of learning, early in the process, details about other opportunities the candidate is entertaining – especially the timing of those competing situations. Further, do not get complacent when another potential employer sweeps in front you and your attractive job opening. You must stay in touch and top of mind with best-fit candidates; it's easy to do so with the multitude of automated solutions available. People generally like to be "courted and wanted." Use this knowledge to your advantage.

Fourth, effectively use your senior leadership team. Routinely ask your leaders to reach out to candidates. A simple voicemail, text or email over a weekend goes a long way to communicate interest and sell your opportunity in a subtle but effective manner.

Lastly, do not fade off when your offer has been verbally accepted. This is when you need to double your communication efforts. Counteroffers are being accepted more routinely today than in the past. Organizations will pull out all the stops to retain their top performers by offering more money, titles and a multitude of enticements, including hot boxing the at-risk employee with timely calls and platitudes from the CEO or other dignitaries.

At this stage in the process, a hiring enterprise should clearly articulate the dynamics of a candidate accepting a counteroffer to stay. Although there are a number of studies that speak to this topic, empirical evidence suggests that as many as 70 to 80% of people who accept counteroffers either leave or are let go within a year. Why? There were reasons a person was looking elsewhere in the first place. More money at a candidate's existing employer doesn't fix the problem nor does a new title. Equally as important, a boss will never forget that a person used leverage to improve his/her situation. Use these tidbits to your advantage by reminding your new hire the ramifications of succumbing to the allure of the counteroffer.

In all, it is incumbent for your organization to step up its game in this hot job market. Do so, and you will see positive results.

JAY MESCHKE
CBIZ Talent & Compensation Solutions
jmeschke@cbiz.com | 816.945.5401

LESLIE SHAW
CBIZ Talent & Compensation Solutions
lshaw@cbiz.com | 816.945.5416

Insurance Strategies

Top 2 Trends in Management Liability

BY **DAMIAN CARACCIOLO**

As exposures generated by everyday business operations increase, the need to protect a business and its management also rises. That's where management liability comes in; it can save companies the expense of litigation and claims settlement.

Management liability is typically a package of various insurance policies designed to protect a corporation and its directors and officers. The package could include directors & officers (D&O), cyber, employment practices liability, fiduciary liability, crime, kidnap and ransom, tax mitigation, and reps and warranties (R&W) coverage. In 2020 there are two key management liability trends to keep in mind:

Directors & Officers (D&O) Liability

The D&O market is continuing to firm, particularly for large private and public risks. Expectations for 2020 include increased underwriting restrictions, limitations in terms/conditions and invariably higher rates and retentions. We also expect reductions in primary capacity driven by the frequency in lawsuits, merger and acquisition (M&A) activity, shareholder activism, and higher attorney and settlement costs. The severity of suits are generally eroding primary aggregate limits, resulting in higher excess pricing.

We do not see the market hardening as severely for the middle-market private and non-profit D&O segments. While we anticipate some pricing adjustments, they will be driven more by the financial health of the entity, increases in rating metrics and industry rather than by an overall market correction. However, companies in emerging industries and start-ups will see increases in both pricing and retentions, as well as possible coverage restrictions as carriers look to remain a viable market for these risks while managing exposure.

(Continued on page 8)

CBIZ Your Team.

Insurance Strategies *(Continued from page 7)*

Claims against directors and officers are becoming increasingly common. The cost of defending a D&O claim can run well into the six figures, leaving a business financially crippled.

Cyber Liability

Cyber liability risk and exposures continue to evolve. Carriers are keeping pace by improving and extending coverage; however, a thorough review of current and proposed coverage is necessary to ensure changing threats are addressed.

As the statistics indicate, there is no slowing of breach frequency and the extent a criminal will go to expose your data:[1] [2]

- Ransomware attacks increased 350% in 2018.
- The average organization was accessible to hackers for 275 days.
- 57% of organizations had firewalls in place at time of compromise.
- 50% of organizations were breached through remote access.
- 33% of organizations were breached internally.

Those perpetrating these schemes do not discriminate based on company size or industry; they select targets of opportunity. While the large breaches are the ones in the headlines, there are more small- and mid-sized business breached each day. These businesses are subject to the same state laws and reporting requirements as Fortune 500 companies but perhaps are without the financial wherewithal to absorb the costs associated with breach notification compliance.

Despite the increase in claim activity there remains ample capacity, keeping pricing flat for those risks with solid security and IT policies and procedures. Rate increases, if any, would be commensurate with growth (revenue, records held) year over year.

All businesses, regardless of size or industry, have exposure. The key is making sure the coverage is tailored to your business and includes extensions addressing the evolving risk.

[1] CyberSecurityVentures.com "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics"
[2] IBM Security – "2018 Cost of a Data Breach"

DAMIAN CARACCIOLO
CBIZ Insurance Services, Inc.
dcaracciolo@cbiz.com | 443.472.8096