Risk Advisories

Staying alert to risk during COVID-19

D&O (Directors and Officers) Concerns

- This is an event-driven exposure that will likely result in D&O claims (similar to Cyber, #METOO).
- Two D&O Securities suits have already been filed, one against Norwegian cruise line alleging that the company was employing misleading sales tactics related to the outbreak and another against Inovio Pharmaceuticals alleging misleading statements relative to vaccine development.

What to do

- Communicate carefully, accurately, clearly and timely with employees, clients and other stakeholders
- Review your crisis management/business continuity plan to ensure it addresses COVID-19, including remote working capabilities and supply chain management
- Follow generally accepted guidelines provided by the CDC and other governmental entities
- Track and follow SEC guidance (Public Companies)
- Obtain professional advice on employee obligations relative to health and safety protocols, as well as employment practices
- Review your contractual obligations to customers and your financial arrangements to identify potential issues and mitigation strategies
- Engage early and proactively with other parties
- Monitor your disclosure obligations on a regular basis
- Monitor the situation and adjust prudently
- Add COVID-19 to the board meeting agenda

oswald®

Risk Advisories

EPL (Employment Practices Liability) Concerns

- Coronavirus could provide an easy tripwire to any disciplinary action taken against an employee who chose to work from home – especially when "work from home" is at the employee's "discretion".
- Employers discretion on can lead to retaliation allegations:
    - *You allowed me to work from home, I chose to do so and now you are promoting someone who chose to come to work.*
    - *You told me I could cancel business travel at my own judgement, I did and now I received a poor review, etc.*
    - *This is a good opportunity for poor performance employees to file a complaint alleging retaliation/ wrongful termination/failure to promote suits.*

It is still too early for this litigation to hit but the industry expects this to be fertile territory for claims.

What to do

- For controls it would be best to follow third party guidelines like those available from the CDC and other governmental entities.
- Ensure work from home and business travel policies are compliant with federal and state laws to avoid discrimination claims.
- Legal opinions on best practices from Employment practices attorneys may be helpful. (please consult with your legal counsel for guidance).

oswald®

Risk Advisories

Crime Concerns

- With less employees coming to the office, internal controls like dual-sign off of checks and separation of duties will suffer, resulting in an increased risk for crime.
- There may be more urgency around turning around wire transfers because of delayed payments due to skeletal crews at your organizations and your organization's clients.
- Anticipate stressed / anxious employees are more likely to skip standard protocols to get things done.

What to do

- Adjustments in accounting may be necessary to keep crime controls at an acceptable level.
- Reminders should be sent to keep everyone aware of your firm's commitment to internal controls, especially now.
- If anticipated, any delayed payments to vendors or employees should be anticipated and communicated to affected parties.
- Alert employees to have heightened awareness of cyber attackers preying on our distracted state and vulnerability.
- Remind every employee of their responsibility to think twice before opening emails and clicking on links, even if the email appears to be from a known and trusted party.
- Confirm wire-transfer orders with a confirmation call-back to authenticate the request.

oswald®

Risk Advisories

Cyber Concerns

It is unfortunate, but during any disaster, cybercriminals will attempt to exploit people and companies.

- **Phishing** scams targeted to Coronavirus cybercriminals are taking advantage of those looking for more information on the outbreak.
- **Malware** is being spread through lots of email communications geared at coronavirus information seekers.
- **Social engineering** of users to gain access to credentials or intercept payments. This could be a third party impersonating a Help Desk or impersonating a vendor or client to divert payment.
- IT teams are managing an increased population of remote and/or novice remote employees. They are also stretching the system's remote capabilities. With the team's capacity stretched, increased stress levels and exhaustion lead to mistakes or omissions of standard protocols

What to do

- Stay mindful of these vulnerabilities at a time when your employees and vendors are distracted.
- Keep your guard up and avoid opening attachments from unsolicited emails. Be cautious of apps as well.
- Alert all employees of these vulnerabilities and remind them of their responsibility to pay attention and do their part to manage these risks.
- Confirm your organization is using Dual Factor Authentication (DFA) across systems. Include e-mail, third party administrators, payroll processors, etc. If you do not use DFA, consider implementing.
- Create a triage system for "help desk" requests to help manage employees expectations. Communicate with employees what the triage is – i.e. system critical items versus non critical to manage frustration levels

Oswald's Cyber Strategic Leader, Lacy Rex, is available to advise you on your cyber needs and questions.

513.716.6002
lrex@oswaldcompanies.com

oswald®