The Top Four Risks Facing Your Company

One need only to scan the headlines to know what happens when risks aren't managed correctly. Data breaches. Vendor disruptions. Productivity and quality issues. You can't effectively reduce your company's exposures, however, if you don't know your areas of vulnerability.

A key step to managing your company's risk and identifying your vulnerabilities is by conducting a comprehensive, enterprise-wide risk assessment. Your assessment should consider your organization's objectives, operational and financial size and your risk tolerance. Your assessment would identify and evaluate the particular events and circumstances relevant to your organization's opportunities and risks. These risks may entail consideration of third party vendors, information technology (IT), staffing and succession planning and emerging markets.

Third Party Vendors

As with other areas of your operations, your approach to managing third party vendors should be based on the risk each vendor poses. A vendor that assists with your company's payroll and billing, for example, may have more risk than a vendor that performs another operational function because the first vendor handles sensitive, financial information.

The vendor's location is an important consideration with the vendor's risk. Some entities may have more regulatory risks because they're multinational. Others may be in areas commonly affected by disruptive events, such as natural disasters, fires or labor strikes.

Past performance is also key. Vendors that have had cybersecurity attacks or other disruptive events may present a higher risk. Consider what triggered the initial incident and what has been done to prevent a similar event from occurring.

Your company should conduct a thorough, annual vendor risk assessment and perform the necessary due diligence with its third-party relationships to reduce its vendor risks. Due diligence can help you identify what the vendor might require in terms of controls and monitoring.

Information Technology

Your organization needs to be vigilant about protecting sensitive data that involves addresses, phone numbers, Social Security numbers and credit card information. Cybercriminals have shown they can get into a range of systems to access personally identifiable information.

Sensitive information should have multiple layers of protection, including strict limits on who has access to the systems. You may also consider whether this sensitive information needs to be encrypted. The U.S. Office of Personnel Management was recently criticized for failing to encrypt Social Security numbers. Formalized policies and user training about intrusion detection, IT security and incident response can also lower your IT risks.

To mitigate security risks, storing data in the cloud may be appealing, but it requires careful monitoring. Oftentimes, companies do not have control over where their data in the cloud are stored, and depending on the type of data involved, you may run the risk of regulatory noncompliance. For example, human resources information cannot be housed on computers overseas. Other data may be subject to state requirements, and what those are will vary by region. Before moving any information to a cloud system, do your research about

what would be permissible and what should remain in data centers under your company's control.

Your IT risks should be continually monitored and your systems updated to keep pace with the ever-evolving cyber threat environment. For more information, please see Enhance Your Organization's Cybersecurity Strategy.

Staff Management and Succession Planning

In all the focus on improving your profit margins or your internal processes, you may have overlooked an essential element of your operations—your staff. Company leadership is essential to keeping your business running smoothly.

As your executives near retirement, you should be sure you have a process in place that can help you identify the right successors. You should evaluate which positions will need to be filled, from managers through chief executive officers and chief financial officers. As part of the evaluation, consider the position's responsibilities. You may find that an executive retiring provides an opportunity to shift around responsibilities or reshape the role being vacated to better suit the current needs of your organization. Having a clear idea of what you need will help you pinpoint the right candidates and the right process to take to identify those personnel.

Emerging Markets

Working internationally can bring numerous benefits to your operations, but anytime you enter new territory, you're also increasing your risks. Be sure you have an understanding of the rules and regulations you may face in the international market. A legitimate transaction in the United States might not be permitted in your new location.

Emerging markets may be particularly challenging, as fraud and corruption tend to be more prevalent. You'll need processes in place that make sure you are not in violation of the Foreign Corrupt Practices Act of 1977 (FCPA), among other anti-corruption provisions.

A Proactive Approach is Key

Consideration of all your risks should also be part of an ongoing risk management process. Your risk environment is always in a state of flux. Only by periodically reviewing your areas of exposure can you keep up with those changes.

CBIZ®

Our business is growing yours

Learn more about how our risk advisory services can support your business at www.cbiz.com/RAS