TOLMAN & WIKER
INSURANCE SERVICES, LLC
INNOVATIVE RISK ADVICE SINCE 1923™

VENTURA | LOS ANGELES | SALINAS | SANTA MARIA | BAKERSFIELD

Small Business and Risk

February, 2014
The Rough Notes Company, Inc.

A small business approach to enterprise risk management

Small businesses are subject to risks and uncertainties. In fact, they are typically more vulnerable to risks than large businesses because they may have less experience in dealing with them and/or lack access to capital in order to handle shocks to the business. In a world of super-charged risk, it behooves owners of small businesses to adopt some degree of formal enterprise risk management (ERM). For the purpose of this article, small business is being defined as a business with 50 or fewer employees unless otherwise noted.

Interestingly, according to The Hartford 2013 Small Business Pulse, “While the majority of small business owners generally feel successful with how their businesses are operating, they are becoming increasingly more conservative with the overall level of risk they are taking with their business.”

Taking a conservative position toward risk implies that both proactive risks and passive risks are being considered.

ERM is a process

Generally, small businesses neither want nor need to introduce some of the good but non-core processes or practices that might be found in large companies. On the other hand, there are processes that make sense or are essential for small businesses— because they add value. The trick is to adopt those that are actually essential and design them to scale with the business. Enterprise risk management, looking at risk holistically, starting with the strategy and goals of the organization, and taking steps to address the risks, is essential in today’s world and is scalable.

In adopting even the most basic approach to ERM, the strategic goals of the business will be in play. Thus, the categories of risk to be analyzed can include: financial, legal, regulatory, market, operational, reputational, liability, property, cyber, and human resource risks, among others. Some risks will be insurable; others will not.

A basic process approach would entail multiple steps: 1) identify risks, current or potential; 2) prioritize risks; and 3) accept, avoid, transfer or mitigate risks.

Step one involves the business owner and key staff periodically reviewing the goals and identifying the major risks that might interfere with meeting them. The resulting list of risks can be shared with the business’s insurance broker, accountant and attorney for additional input and feedback.

Step two involves some sort of ranking of the risks, so that only those that are very likely or have potentially significant impact are highlighted for action.

Finally, step three is to decide how these risks will be handled and enact a plan to address them. Will they be transferred (generally meaning insured), accepted, reduced or avoided? The specific mitigation action planned will be dependent on many factors such as feasibility and cost.

An illustration

To illustrate how the process may play out, one typical goal will be discussed and analyzed hypothetically. The hypothetical business, ABC Fencing, is a fence installation company that employs three full-time employees. The types of physical fences they install are made of wire, wood, plastic or concrete. They do not do electronic fencing. To complete the picture, they do initial installation as well as maintenance and repair of fences—whether or not they did

the installation—and they also erect prefabricated sheds. Assume that one medium-term goal of the business is to increase the number of customers from outside the existing customer base radius (a particular group of towns in the county). Next, assume that there are marketing and advertising tactics planned to meet that goal. For some businesses, the planning and analyzing might stop there. In other words, existing or potential risks associated with the goal and tactics would not be seriously examined.

However, if some level of ERM was in place, all of the goals would be looked at in terms of what risks might interfere with meeting the target. Based on keeping abreast of national and local news and drawing on past experience, assume that the owner and general manager identify the following as some of the more significant risks the business might face for this marketing goal:

• Neighboring counties and/or the homeowner associations of housing developments in those counties introduce regulations prohibiting all but electronic fencing.

• Direct competitors of the business decide to open up in neighboring counties (either start-ups or other contractors expanding their offerings).

• New housing construction in the expanded territory (recent homebuyers are a major source of new business for fencing contractors) dips below historical averages or dries up for a protracted time period.

Having identified the potential risks, assume that ABC Fencing further researches conditions to determine how realistic and imminent these risks are and what their impact might be. The business can then decide if there is a need to take mitigation action, which could involve anything from changing the goal to investing in the introduction of a new product line, e.g., electronic fencing, or even opening another location in a different territory beyond neighboring counties where new construction may be more vigorous.

• The value of analyzing the risks relative to such an important goal—a goal that would entail expense for the business—should be clear. Investigating the risks allows the business to take a more appropriate, efficient and effective path toward its goal.

A plethora of risks

There is no shortage of risks to challenge small business. Small businesses have been feeling the effects of the economic slowdown since roughly late 2007. This can be seen by looking at Dun & Bradstreet's Small Business Health Index which measures failures, payments, etc., found on their Web site, www.dnb.com. Below we look at just three categories of risk: weak economy, increased regulation, and cyber and systems.

Weak Economy. The economy, or more precisely a weak economy, can be a serious threat to small businesses. It can result in lower sales volume, slower payments or nonpayment, less credit availability, and compressed margins. A small business in such an economic environment may address the risk by reducing expenses, adding higher margin products and services, forging new partnerships, and so on. As with many external risks, a business owner cannot eliminate the risk itself but can mitigate the risk with actions designed to overcome its effects.

Increased Regulation. More costly or rigorous laws or regulations can pose a risk to small businesses. There are so many new and old laws, regulations and statutes that businesses must comply with at the federal, state, county, and city levels. There are also instances where requirements from different sources are inconsistent with one another, adding confusion on top of volume. It is true that employers of fewer than 50 full-time employees are exempt from some laws or regulations, but they must keep abreast of changes to the law, e.g., modifications to the exemption level or of the definition of full-time and part-time employees. Such exemptions have enabled many small businesses to get started and to prosper because they would not be able to afford the cost burden of the laws from which they were exempted. At the same time, small businesses with 50 or more employees have had to find ways to successfully cope with these laws. With new laws being passed, the burden gets heavier.

Risks relative to the laws and regulations for small businesses include:

1) uncertain cost of implementation,

2) non-compliance risk, i.e., fees, fines, closure from inadvertent failure to comply, and 3) reputational risk associated with non-compliance, if reported publically. Therefore, the business owner or manager needs to know the laws and abide by them or accept major risk.

Cyber and Systems. Cyber risk can no longer be considered the bane of big business alone. Cyber attacks are on the rise. The annual Symantec Internet Security Threat Report (ISTR) revealed that "Webbased attacks increased 30% in 2012. Surprisingly though, is that a majority of those attacks targeted small business with less than 2,500 employees, proving that no matter what size your business is, it's vulnerable to potential attacks." 1

Cyber attacks can take the form of attacks that overwhelm and cripple the site (denial of service attacks) or attacks that pilfer data or corrupt data and systems. These are serious risks to business.

But, it is not just actual cyber attacks that small business must be concerned about. In a networked world there are all sorts of threats to small businesses. These can vary from angry customer comments posted on social media sites; to system failures that shut down operations; to poorly scripted, hastily sent e-mails that inadvertently bind the company to something unintended. There is elevated risk associated with maintaining required privacy of information, especially when all manner of devices carry the data such as laptops, notepads, and smart phones. Then, there is a trend toward cloud computing with its unknowns. As the tip of the iceberg, this overview indicates the expanse of the underlying iceberg that cyber risk represents.

Conclusion

The purpose of the article was not to explore every type of risk category; there are too many. The main point being made is that ERM can help small businesses achieve their strategies and goals by dealing with the risks that may interfere along the way. The ERM process is made up of the steps: 1) identify, 2) prioritize, 3) take action. In the end, the benefits of practicing ERM will well outweigh the effort.

1. “Threat Landscape Evolves, Attacks More SMBs in 2012.” Swathi Turlapaty, May 13, 2013, www.symantec.com/connect/blogs/ threat-landscape-evolves-attacks-more-smbs-2012.

Return to Article Index

Forward this article to a colleague

Address To Recipient Name

Subject

Message

Send Reset