THE PRACTICAL ASPECT

Small Business Interruptions

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2HU81oq

According to the Allianz Risk Barometer 2019, for the seventh year in a row, executives and insurance experts worldwide are most concerned about business interruption risk scenarios.[1] Business interruptions, caused by humans or nature, are common and, perhaps, more frequent today. The early 2019 US government shutdown, which lasted for more than a month, caught several thousand independent contractors off guard. As for natural calamities, we hear more about frequent—and more impactful—hurricanes, tornadoes, floods and fires; much of this is attributed to climate change, although there are naysayers to this assertion. A more recent addition to this growing list of external risk scenarios is the polar vortex that dipped down into the Northern Hemisphere from the North Pole, causing temperatures to plummet to unprecedented below-zero levels. Almost everything in the affected area, the upper Midwest, USA, came to a standstill for at least one day.

Size matters when we talk about business interruptions. Large businesses are probably more prepared for such discontinuities than small businesses. Large businesses put more thought into risk management, are better prepared with contingencies, have more resources on hand, and are likely to have many locations, which may reduce the impact on any local area of operation where a disaster strikes. And yet, even big businesses go into liquidation following a disaster, for example, Pacific Gas & Electric Company (PG&E) filed for bankruptcy following catastrophic wildfires in California, USA.[2] Overall, small businesses bear much greater risk for a complete meltdown in the event of a major calamity. Research by the US Federal Emergency Management Agency (FEMA) found that 40 percent of small businesses will not reopen after a natural disaster. Unfortunately, of those that initially survive the catastrophe, 20 percent will still close within the year. Rationalizations such as "it will not happen to me" are common. In a *Journal of Accountancy* survey report, 21 percent of small business respondents said, "I've never had an issue before; disasters are rare in my area;" another 30 percent admitted, "I haven't really thought about it;" an additional 27 percent did not believe it is important to their businesses; and 20 percent said that they have not had time to develop and institute a plan.[3]

When a survival issue is denied or its existence is weakly acknowledged, the outcomes downstream are, at best, left to the destiny. Preparedness is missing. According to one report, 62 percent of small US businesses have not established a formal plan for responding to a natural disaster or any other emergency.[4] Another finding emerging from a survey by Nationwide Insurance points to the alarming conclusion that 75 percent of small businesses do not have a business continuity plan.[5] Perhaps this was a fortuitous approach in the past, but when 100-year flood areas become five-year flood areas, there is more at stake than this level of disregard would suggest.

Vasant Raval, DBA, CISA, ACMA
Is professor emeritus of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and corporate governance. He can be reached at vraval@creighton.edu.

Rajesh Sharma, Ph.D., ITIL Foundation, Six Sigma Black Belt
Is a quality management office (QMO) chair at Software Engineering Services. He has more than 19 years of experience in establishing and managing project management offices (PMO), QMOs, metrics programs, and as a lead for independent verification and validation (IV&V) projects. As a QMO and IV&V lead, he has performed quality audits, process improvement and IV&V assessments. He can be reached at rajsharmane@gmail.com.

Risk Assessment

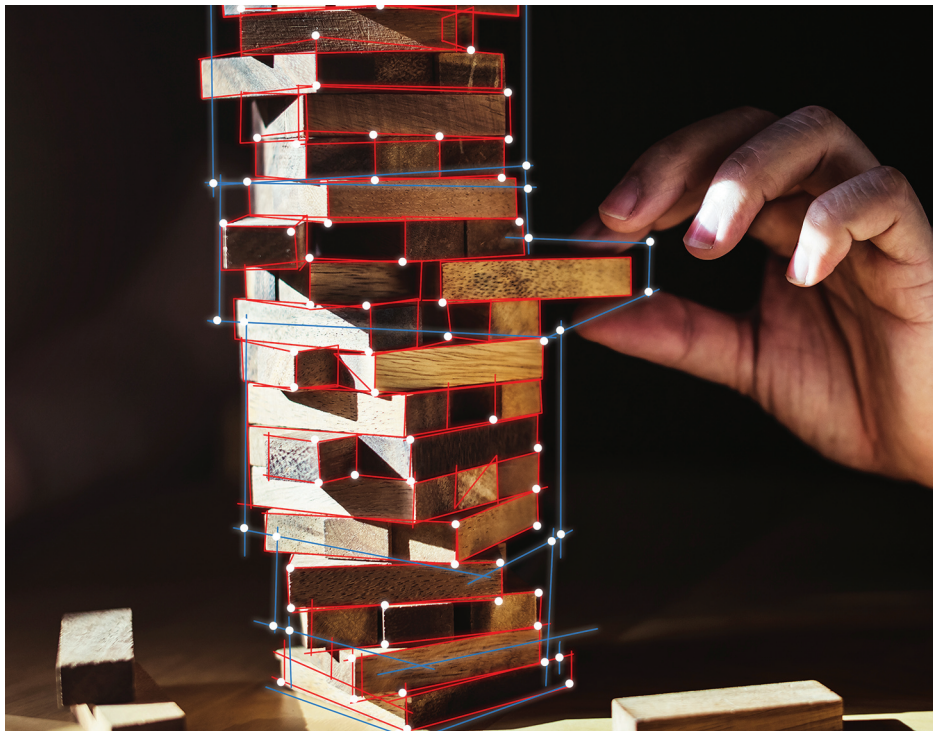
Without a risk assessment, preparation is like shooting in the dark, perhaps causing an organization to spend more resources than it needs to and still not managing the risk on hand. Any risk assessment is an acknowledgment of threat and, thus, a serious undertaking in protecting the organization from threats. Small businesses are likely lacking risk assessment expertise since many cannot afford a full-time risk professional on staff. However, small businesses can learn from organizations such as chambers of commerce or the Small Business Administration (SBA) in the US.

Experts suggest that the first imperative in creating an effective risk management system is to understand qualitative distinctions between three types of risk organizations, including small businesses, face:[6]

- **Preventable risk**—Internal to the organization and controllable
- **Strategy risk**—Risk emerging from the organization's strategy
- **External risk**—Risk scenarios that arise out of events outside the enterprise and beyond its control. A common and unpredictable source of business interruptions, external risk can only be mitigated by focusing on "identifying them, assessing their potential impact, and figuring out how best to mitigate their effects should they occur."[7]

> "ANY RISK ASSESSMENT IS AN ACKNOWLEDGMENT OF THREAT AND, THUS, A SERIOUS UNDERTAKING IN PROTECTING THE ORGANIZATION FROM THREATS."

For organizations that deal with larger corporations as suppliers, for example, it is likely that the



customer (large corporation) would want assurance that the organization would be able to sustain disasters, including natural calamities, and man-made threats such as hacking, malware infection to its systems and data theft. For complex corporations, third-party risk management (TPRM) has become a priority as the risk of third parties affect the organization doing business with them. In meeting the business continuity and resiliency requirements of such customers, it is likely that the small third-party enterprise will get more guidance and, perhaps, a nod of approval on the plans it has made. Whereas such imposed requirements might seem onerous, the long-term benefits of any actions emerging from the sourcing organization undoubtedly exist. Perhaps the cost of such compliance may be passed on to the customer through proper pricing of products or services.

Risk Mitigation

One major obstacle to risk mitigation steps in small businesses is that the resources are limited. Immediate needs overpower long-term goals. What can be done frugally is likely to be entertained without much hesitation. While large enterprises can justify spending significant resources to this

Enjoying this article?

- Read *Getting Started with Risk Management*. *www.isaca.org/Getting-Started-With-Risk*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

end, even those large entities may find it challenging to allocate significant amounts to business continuity. Doing more with less in a creative manner is likely the answer. Redundant resources are a typical risk mitigation response for recovery from disasters; however, small enterprises cannot afford to duplicate resources. As a result, they might look for collaborative efforts where each enterprise can depend on another compatible business, preferably in another location. While this sounds ambitious, colocation has not been a popular risk mitigation approach among small organizations because of the difficulty of staging collaborative arrangements across organizations.

Risk mitigation should respond to risk assessment results. Whereas this may not be perfectly achieved with standardized templates and plans, these types of resources, if available from chamber of commerce or the SBA, should prove helpful as a starting point. Again, the will to support such initiatives has a better chance of succeeding if standardized plans address frugal measures that small enterprises can afford. It is not so much that smallness implies unwillingness, but, rather, lack of affordability, especially of something that has unforeseen benefits. Combined with awareness of the problem, it is necessary to next address the cost feasibility. Without benefits exceeding costs, enterprises are unlikely to take the steps to implement what is necessary. According to one report, 96 percent of businesses with a disaster recovery solution in place fully recover operations.[8] So, the value proposition of a disaster recovery plan (DRP) is convincing enough to act.

Sustaining for Tomorrow

Sustainability of small businesses begins with accepting the reality that disasters will happen, especially with climate change. No place on earth can be considered completely safe from natural calamities. For small business owners, recognition of this reality is a first necessary step. Without coming out of the denial mode, not much can happen in the risk management space. It is comforting that the SBA has an online course on disaster recovery; however, it is geared to post-disaster corrective measures such as how to access Economic Injury Disaster Loans.[9] While important, this does not serve the purpose of preventing disaster-related losses or improving chances of business continuity. An online course designed to achieve these objectives should prove helpful to small business owners. Importantly, such a course needs to be customized to the critical aim of getting the entrepreneur out of the denial mode.

Beyond building awareness of such crises, proactive measures to help avoid or minimize the impact of a calamity are important. For example, small enterprises should be aware of web-based early warning mechanisms to react quickly to impending storms, floods or hurricanes. The US National Weather Service focuses on providing timely and precise information, for example, regarding approaching hurricanes and what businesses should do proactively to minimize or avoid the impact of the disaster.

Most corporate DRPs resort to duplication of data and redundant resources, such as hot sites and cold sites. These measures could be appropriate and effective, however, the affordability threshold for small organizations is low and significant redundancies may not be an option. A creative approach to building similar but affordable redundancies is required. In this regard, the chamber of commerce or an association of the industry to which the business belongs could help. For example, such industry associations can help identify in advance a compatible factory, a potential colocation site outside of the area where the disaster strikes. The affected enterprise in this situation can resort to help from the colocation firm to recover and, ultimately, normalize its operations.

Seeking experts to help a small enterprise can be facilitated in two ways. First, if the enterprise is a supplier to a large enterprise, it is likely that in the process of managing third-party risk, the large corporation would lend its expertise to educate, guide and support the small enterprise in taking appropriate risk mitigation steps. Although limited and, to some degree, focused on one customer, such help could be valuable to small organizations lacking professional expertise. Second, powerful professional organizations such as the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA) (perhaps in collaboration with the SBA) and ISACA® could help develop a resource of volunteers willing to assist small enterprises in their area to achieve some measure of insulation from disaster impact.

Finally, disaster-related insurance should prove helpful. Insurance is a corrective step; however, in the event of a calamity, it provides resources to rebuild what is lost and recover from the damaged condition. Even a high-deductible plan may work for

some organizations that cannot afford full coverage. It should be recognized that insurance is not a panacea, but it will, at least, provide funds for the business to get back on its feet.

If the value of disaster recovery was greater than its cost in the past, the future is likely to bring exponentially higher benefits. What has changed is the threat level, especially that of natural disasters due to climate change. And, even cybersecurity threats have escalated due to the connected world in which businesses are operating. The payoffs are potentially great, and the time is now to act in protecting the future.

Endnotes

1 Ryan, V.; "The Most Pressing Business Risk This Year," *CFO*, 22 January 2019, *www.cfo.com/risk-management/2019/01/the-most-pressing-business-risk-this-year/*

2 Lazo, A.; "PG&E Has Few Allies in Sacramento," *The Wall Street Journal*, 31 January 2019, *www.wsj.com*

3 Drew, J.; "Most U.S. Small Businesses Lack Disaster Recovery Plans," *Journal of Accountancy*, 2 August 2012, *https://www.journalofaccountancy.com/news/2012/aug/20126135.html*

4 *Ibid*.

5 Insurance News Net, "Most Small Business Owners at Risk for a Disaster," 31 August 2015, *https://www.nationwide.com/personal/about-us/newsroom/press-release?title=083115-small-biz-survey*

6 Kaplan, R. S.; A. Mikes; *Managing Risks: A New Framework*, Harvard Business Review, USA, 2012, p. 49-60

7 *Ibid*., p. 56

8 Rock, T.; "2017 Disaster Recovery Statistics That Businesses Must Take Seriously," Invenio IT, 31 January 2018, *http://invenioit.com/continuity/2017-disaster-recovery-statistics/*

9 US Small Business Administration, Disaster Recovery: A Guide to SBA's Disaster Assistance Programs, USA, *https://www.sba.gov/course/disaster-recovery-guide-sbas-disaster-assistance-programs/*