INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

What's the Weakest Link in Your Supply Chain?

Institute for Homeland Security

Sam Houston State University

Justen R. Noakes

Author Biography

Mr. Justen R. Noakes is the President/CEO of KTLO Solutions, a professional consulting firm that provides enterprise risk management solutions focused on business and industry. Mr. Noakes has over thirty years of retail experience in engineering, project management, information technology, and emergency management. Mr. Noakes developed and led the Emergency Preparedness Department for H-E-B from 2004 to 2024. In those twenty years, Mr. Noakes led H-E-B's response to over twenty presidential-declared disasters, most notably Hurricanes Rita, Ike, and Harvey, as well as the COVID-19 Pandemic and Winter Storm Uri in 2021. Mr. Noakes serves on the Board of Directors for Texas Search and Rescue, an all-volunteer first responder organization, and is a Bexar County ESD2 Fire Department Commissioner. Mr. Noakes currently serves on the Private Sector Advisory Council and the Texas Emergency Management Advisory Council at the request of the Governor.

Disclosure statement: The author of this technical report, pertaining to the granted project, hereby discloses that there exist no conflicts of interest or competing interests to declare in relation to the research, authorship, and publication of this work.

Abstract / Introduction

Do you know the weakest link in your supply chain and how it could impact your business if it fails? In a digital economy driven by generative AI and same-day delivery, business owners today face an overly complex network of service providers, distributors, and suppliers. The weakest link is likely outside the business's four walls, and the business owner doesn't even know it exists.

This paper will discuss a tool business owners, business continuity practitioners, and senior security executives can use to identify supply chain business continuity and disaster recovery (BCDR) deficiencies in their critical supplier network.

To achieve true resilience across your supplier network, you must first understand the strengths and vulnerabilities of your supplier portfolio. This will require business owners to extend risk assessments outside their operations and into each supplier, especially those who provide critical components or services.

Implementing a practical process and tool that allows business owners to gain visibility into their suppliers' BCDR capability is the first step to ensuring that suppliers can continue operating during times of crisis. This tool will provide businesses with an initial, high-level assessment of the suppliers' BCDR capabilities, enabling them to either feel confident in the supplier's resilience or cause them to investigate further. This initial assessment will result in the Critical Supplier Resilience Index (CSRI).

The CSRI is designed for ease of use and understanding and fosters collaboration. It empowers business owners and suppliers to work together to identify strengths and opportunities in a supplier’s BCDR capability. It also gives business owners and suppliers a shared understanding of business continuity expectations, instilling confidence in the supplier's effectiveness and the value of the supplier's contribution.

Key Terms: Supply Chain – Resilience – Business Continuity – Capability Assessment – BCDR– Index – Critical Infrastructure – Survey – Supplier – Disaster Recovery – BCP – Extended Enterprise Risk Management

Introduction

Without proper plans and capabilities in place before an incident occurs, disasters and crises can affect a business's ability to provide products or services to its customers, including critical infrastructure. Supply chain disruptions can happen anywhere worldwide and involve manufacturers, distributors, and retailers. The ripple effect of supply chain disruptions can range from immediate impacts on the availability of raw materials for manufacturers to year-long consumer goods shortages for distributors and retailers.

Having resilient suppliers as part of your provider portfolio will not eliminate impacts from worldwide disasters. However, it will reduce disruptions to your and your customers' businesses, allowing normal operations to resume more quickly.

Business continuity planning (BCP) is the foundational process on which resilience programs worldwide are based. Disaster Recovery Journal defines BCP as "the process of developing prior arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions can continue within planned levels of disruption." Without these continuity plans, companies and their employees are at a disadvantage when an emergency occurs, often starting at ground zero, trying to figure out how to respond and recover from whatever disaster may have just happened. It is a well-documented fact that, according to FEMA, following a significant disaster, nearly 43% of small businesses do not reopen, and another 29% that do reopen fail within a year. Over half of small businesses are forced to close their doors following a disaster.

We often hear that these disasters only impact those on the coast affected by hurricanes or that "it will never happen to me." Based on research by FedSmallBusiness.org, in 2021, 1 in 10 small employer businesses suffered losses from a natural disaster during the prior 12-month period. These losses weren't from just hurricanes but included many types of billion-dollar disasters, including catastrophic flooding in New York, New Jersey, and Pennsylvania; historic cold weather and power outages from Texas to Nebraska; and wildfires in California and other western states scorching more than 7,000,000 acres of land and amounting to $10.6 billion in damages.

According to findings from the 2021 Small Business Credit Survey, over half of small businesses are not returning to open their doors because of these catastrophic natural disasters, and nearly 70% reported that they were in fair to poor financial condition due to the impacts of these disasters. Small businesses are ill-equipped to prepare for and respond to natural disasters. They often do not have the resources, know-how, and, more importantly, the time to worry about something that may never happen.

"Small businesses are a huge contributor to our economy, so if they're unable to rebound and provide goods and services on which we rely as a community, then obviously our recovery

efforts are going to be curtailed," said Jim Redick, Director of Emergency Preparedness and Response for Norfolk, Va.

Disaster Recovery (DR) and digital resilience have become top of mind for business continuity professionals as emerging threats from bad actors across the globe threaten our critical digital systems with cyber attacks and ransomware. The Disaster Recovery Journal defines DR as "The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage. The strategies and plans for recovering and restoring the organization's technological infrastructure and capabilities after a serious interruption."

FBI Director Christopher Wray, in 2024, stated that "China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities." This statement only reinforces the need for businesses nationwide to ensure that DR plans are in place to ensure business continuity and national security.

To that point, conversations around BCDR must involve security executives to ensure that if bad actors are involved in business disruption incidents, proper security protocols can be engaged and applied accordingly. In the past, BCDR has historically been the responsibility of risk management and emergency preparedness, but with the ever-growing number of physical attacks and cyber-attacks, security professionals are a fundamental part of the BCDR team and should be involved in all planning and execution activities.

Problem Statement

Small business owners who find the time and resources to build a BCDR plan tend to focus on their internal operations. They also tend to focus on a single aspect of the business, such as a specific building, process, or department, typically the most critical component or the highest production volume product. Rightfully so, these items tend to keep businesses afloat day to day and are critical to their success. However, looking holistically at the entire supply chain and understanding the interdependencies within the business process is essential.

Besides critical lines of work, businesses should particularly include processes that deal with employees, such as human resources, payroll, and benefits. Employees are the heartbeat of any organization, but for small businesses, they are critical to its success. Other important ancillary processes to include in planning efforts are marketing, public affairs, communications, advertising, and accounting. Departments such as public affairs and communications are critical to ensuring that customers hear about incidents directly from the source and not on social media; this is particularly true for a cyber incident or active assailant attack.

As with any business, the supply chain can only be as strong as its weakest link. When this weakest link is within the four walls, visible, and part of a business owner's process, the remedy

is within the owner's control. It can be fixed or, at the very least, shored up or worked around until resolved. However, vulnerabilities often live outside the control and even the visibility of a business owner. This is especially true as it relates to today's supply chains.

As businesses struggle to cut costs, increase productivity, maintain quality, and provide a satisfactory work environment for employees, business owners are outsourcing more and more components of their portfolio. As the competitive landscape continues to grow exponentially and globally, thanks to the internet and companies like Amazon, small businesses are turning to foreign companies that can provide services, components, parts, and supplies at a much lower cost.

From a business perspective, outsourcing allows the owner to produce products or provide services at a lower cost, allowing the business to grow, offer better pay, or even provide healthcare benefits for employees. However, outsourcing also introduces external companies' bad habits and deficiencies into the business owner's risk landscape. Therefore, those deficiencies and vulnerabilities have become the business owner's risks. Depending on the external company's BCDR capabilities, this could also mean that the business owner may have the opportunity to share or avoid some of the risks.

As with any business continuity and risk management conversation, the question is, "What should I be worried about?" and "What can I do about it now?" Fortunately, there are tried-and-true frameworks that help provide guidance and direction on how to assess risk and understand the business impacts. Then, taking those outputs, we build a set of guidelines and plans that help facilitate the response and recovery from business disruption incidents, both natural and human-made.

Problem Discussion

The US Small Business Administration, FEMA, and insurance companies such as Texas Mutual all provide great resources and templates to help businesses prepare for and respond to disasters. These resources are focused on ensuring that companies have a plan in place to support their ability to resume operations, take care of their employees, and have the right business insurance coverage. There are even geographic-specific resources available, such as coastal areas and seismic zones, that require enhanced insurance coverage, such as flood and earthquake insurance. However, because of the ever-expanding complexity of supply chains, the resources available to support an extended enterprise risk management model are limited.

Since September 11, 2001, in the United States, both the public sector and private businesses have focused on being more prepared for unexpected and unimaginable situations that could affect their ability to do their jobs and the safety of their employees. For business and industry, the focus for the past two decades has been on making individual companies more resilient to withstand business disruption incidents that could compromise the ability to deliver products,

services, or information to customers. Many systems and standards provide guidance, such as ISO 22301(The international standard for Business Continuity Management Systems), for business owners to reference, but these standards focus heavily on the organization alone. This has undoubtedly led to increased resilience for businesses worldwide; therefore, we are a more resilient society because of these standards and best practices.

During this period, there has also been a significant advancement in technology, specifically the ability to communicate and share information globally. This advancement has enabled businesses to leverage capabilities, technologies, and productivity tools worldwide. The access to the global economic market and capability has resulted in greater efficiencies and capabilities for companies to build better products at a lower cost and quicker turnaround times. As the demand for products and services has grown worldwide, the demand for lower costs and faster delivery has forced businesses to leverage external resources more than ever. Doing so has led to less visibility and control of critical networks outside the company.

Business and industry networks have grown substantially for decades, allowing companies to expand and develop new and improved products to meet the ever-increasing consumer demand. Never before have consumers had access to products and services at such low prices and short turnaround times…" Same-day delivery" is a standard part of our vocabulary. Today, up to 80% of operating costs may originate outside the organization.

However, as these business and industry networks expand, so does the complexity in which they operate. Any business continuity practitioner knows that complexity is the Achilles heel of resilience, making planning for business disruptions exponentially more difficult. Inherently, because of the high degree of complexity and multiple tiers of external factors in a business process, there is a higher possibility for deficiencies within these external processes. And because of the increased number of systems and processes, which ultimately lead to an increased number of deficiencies, the complexity of the network then leads to increased fragility.

Because of these global and complex networks, today's businesses are more susceptible to international disasters and crises than ever before, especially multiple events that may occur within a short period of each other, not only increasing the number of incidents to contend with but on a more frequent basis. Extended global networks allow businesses to operate more efficiently and effectively than ever, allowing companies to provide products that their customers demand at an inexpensive price with "same-day delivery." However, this efficiency and productivity come with the cost of drastically reduced resilience and the inability to weather the storm and return to normalcy when disruptions occur.

There are many examples of businesses going under because of poor planning or lack of business continuity capabilities, especially over the past decades with the globalization of the supply chain and the economy. In addition to the challenges brought forth by the COVID-19 pandemic, those failures seemed to multiply, with small to medium-sized businesses being the hardest hit. Many people are familiar with and were affected by the COVID-19 toilet paper shortage or the

microchip shortage that left thousands of new vehicles stranded in holding lots across the United States. But in the United States, very few things are more personal and emotional than one's favorite food, especially hot sauce!

One business continuity failure that hit home and affected millions was the shortage of Huy Fong's famous sriracha sauce. The 2009 bon appetit "Ingredient of the Year" has a cult-like following with its fiery red color, green cap, and crowing rooster on the label. Unlike the product itself, there is no shortage of Huy Fong Sriracha merchandise, songs, memes, and candy, not to mention a considerable internet following for the famous hot sauce. The popular sauce gets its red color from the red jalapeno, which is the same pepper as a green jalapeno, just with more time spent roasting in the fields of sunny California in this case.

For years, Huy Fong has exclusively used red jalapenos from neighboring Underwood Ranches in Southern California, conveniently located next to the Huy Fong Sriracha processing plant. The relationship was mutually beneficial as Underwood produced the perfect jalapeno that gave Huy Fong Sriracha its distinctive fire engine red color and spicey flavor that millions of customers had become accustomed to. However, in 2016, that all changed as Huy Fong decided to end the long-standing practice of pre-paying for the yearly jalapeno crop from Underwood Ranches. As a result, Huy Fong ended the relationship with Underwood Ranches and began the search for an alternative supplier for the red jalapenos. The result has been a backlash from customers as the new supply of peppers did not match customer expectations. "The classic garlicky, vinegary taste is still there, but the classic heat seems to have dropped off," Luke Gralia wrote in The Takeout. Although Huy Fong and Underwood have suffered financially from the relationship's demise, the real loser in this contract dispute is ultimately the customer. (Forbes, "What A Sriracha Shortage Teaches Us About Supply Chains"/May 09, 2024)

Multiple business continuity lessons can be learned from this story, but the fundamental aspect of having a valid contract in place with key suppliers is paramount. This story also exhibits the need to identify, establish a relationship with, and utilize alternative or secondary suppliers as part of your daily business plan. Utilizing secondary suppliers, even if for a small portion of the daily business, ensures that all the business underpinnings, such as the purchase order process, accounts payable, supply chain requirements, quality assurance specifications, and product quality standards, are in place, active, and achievable when needed. Reducing or eliminating single points of failure in your critical supply chain, whether for hot sauce or joint strike fighters, results in a more resilient supplier, consumer, and, ultimately, society.

Way Forward

We live in a world of extended complex networks, not only in the business environment but also in our personal lives. With the staggering speed of technological advancement, especially with artificial intelligence, we must not just expand our thinking to include extended networks, but we

should also put the same rigor and focus on those vulnerabilities as we do within our business. We must leverage and execute extended enterprise risk management strategies and planning theories as we did with business continuity planning after 09/11.

Extended enterprise risk management (EERM) is more than a program, set of guidelines, or plan; it's a mindset. The enterprise must be willing and able to look beyond the four walls of its business and consider the entire extended network its "responsibility." Simply declaring a supplier issue as "not my problem" is no longer an acceptable mindset, as the customer is ultimately affected by whatever disaster occurs halfway around the globe. In this ever-shrinking global economy, this hands-off approach will eventually result in lost revenue, decreased customer loyalty, and, ultimately, the company's demise. This extended enterprise mindset must live and breathe with the senior leadership of any company, including C-suite roles such as the CEO, COO, CFO, and Senior Security Leader. Undoubtedly, an extended enterprise mentality and the associated programs to address internal and external shortcomings will cost the company resources, time, and money, but as a result, will ensure the company remains open for business and relevant to its customers.

As companies begin to look outside of their span of control and into the operating models of suppliers and vendors, it is more important than ever that senior leadership takes on the role of relationship-building and collaborator. Unlike internal processes that can be changed based on directives, implementing successful changes outside of the organization within other business models will heavily depend on the relationship and influence between the two organizations. Not only is a more collaborative approach likely to result in a better outcome as it relates to business continuity deficiencies, but it will also pave the way for ongoing collaboration between the two entities that will foster continuing growth and improvement for years to come. And as "partnerships" form and grow, opportunities for advancement and improvement happen inherently.

After the onboarding and engagement of senior executive leadership, the first step to establishing an extended enterprise risk management mentality is a complete understanding of the networks your business operates within. This can be overwhelming, especially for a company with many capabilities or divisions. For example, a retailer must not only evaluate the customer-facing "storefront" but also the transportation, warehousing, and distribution network, the manufacturing plants, the external supply chain network, and a myriad of administration functions that work behind the scenes to keep everything functioning, including information technology, payroll and accounts payable for example. This can seem impossible as many companies do not have a detailed understanding of each of the internal processes, much less how they interact with each other and certainly not how they interact collectively with external networks.

EERM planning must be considered a long-term core capability and assigned to a department's responsibilities to ensure ongoing success. These plans often live in the Risk Management or

Emergency Preparedness Departments, with full-time staff and dedicated resources assigned to managing and continuously improving plans and capabilities. They have budgets and key performance indicators (KPIs) assigned to ensure continuous advancement and achieving desired and documented goals and objectives. As hazards and threats evolve and the emergence of "bad actors" continues to grow in the risk landscape, traditional physical security and cyber security should be included as part of the core EERM planning process and team.

EERM uses the best practices and planning components from the past two decades and applies them to businesses and processes outside the parent company's control. EERM programs are complex to design and manage due to the numerous moving parts that must be identified, understood, mapped, evaluated, and planned for. Establishing long-term goals and objectives is critical for success and must be supported, if not established, by senior leadership, preferably the C-Suite. These goals should be comprehensive and complete and provide clear direction for practitioners to work towards. Ambiguous or conflicting guidance will only delay plan development and will likely cause undue duress within the organization during plan development. This duress commonly manifests while identifying priorities, especially in multi-operational, multi-division companies. Deciding which plan gets developed first or which department is the "most critical" often leads to heated debates in the boardroom as everyone deems their function as "most critical."

Organizations should consider implementing a tiering system that will allow them to categorize their departments, systems, and capabilities based on a definable and measurable set of criteria, helping to remove the emotional debate from the decision matrix. This also allows "everyone" to have a place at the table and be included in the planning, even if at a lower-tier designation. This establishment of criticality, or tiering, is a critical success factor. It will serve as your Northern Star throughout plan development and as you decide where resources are placed and money spent. You can also use this "ranking system" as you develop and integrate your digital disaster recovery program into your EERM program.

Once the dust settles and priorities, goals, and objectives have been identified, determining a short-interval programmatic approach to project planning and implementation is a critical next step. Often, organizations embark on a business continuity project with a definable endgame in mind. However, as you start identifying interdependencies and defining processes, organizations quickly realize the intertangled complexities of their networks and business relationships. At the enterprise or extended enterprise level, business continuity is an ongoing process of discovery, analysis, planning, exercising, and maintenance; this process is circular with no endpoint.

Once a company has established C-Suite support, clear priorities, and a business continuity program, the next step is understanding how your company's processes and systems interact with the external world. Because of the complexity of the multi-tiered layers of external partnerships, senior leadership must help establish boundaries for the extended enterprise. These boundaries should be based on priorities established in the program's development, including criticality and

perceived risk. These boundaries should be flexible and allowed to expand and contract depending on the evaluated system or as external competencies are assessed.

Mapping how business processes interact and flow with external resources will provide a visual guide to identifying risk points that should be evaluated. The flows can be based on product flows, information flows, or financial flows; for this paper, we will focus on product flows. Businesses should also understand and plan for the mapping of digital systems to identify integration and information flows. Once business processes are established, overlaying digital system maps will provide a complete view of the complex processes.

Many commercially available tools help business continuity practitioners map complex business and digital system processes. Readily available applications such as Microsoft Excel and Microsoft Word have flow chart capabilities that provide low-cost options to begin the mapping process. The mapping process will require interaction between subject matter experts from the mapped departments and site visits to help fill any information gaps and confirm processes. The mapping process should be a living document with no "final version." It should be revisited annually when an incident occurs or when there is a change to the process.

As noted above, this paper will focus on the product flow processes of an extended enterprise risk management plan. Once mapping is complete, the business continuity practitioner can identify areas for analysis and planning. Often, problems occur at the interface points where a physical handoff, communication exchange, or data integration occurs between two or more parties. This paper will focus on evaluating critical suppliers, contractors, and service providers identified as crucial in the product flow mapping process.

The overall evaluation of critical suppliers, contractors, and vendors in the business sector should begin with the contractor's ability to fulfill the requested product or service order based on business needs alone. The success of the capitalistic business model depends on the ability to deliver what the customer wants better, faster, and cheaper than the competition. As previously discussed, the extended enterprise business model enables businesses to accomplish this more readily while also protecting the interests of the business, the contractor, and the customer.

Because of this, including resilience criteria is more important than ever before. Including resilience questions in the vendor evaluation process will ensure they are part of standard operating business procedures. Business continuity or risk analysis is often an "add-on" or ancillary process that is not necessarily required and is sometimes omitted in order to move the process along quickly. Making critical resilience questions part of the vendor evaluation process ensures compliance and the opportunity to evaluate a vendor before the award determination. Also, as vendors are assessed throughout the relationship with a business, resilience criteria can be included in that ongoing evaluation to ensure compliance. A key success factor for business continuity and resilience is integration into daily business operations, no different than vendor financial or insurance requirements today, which are standard practices and non-negotiable in most cases.

The business capability evaluation process of vendors, contractors, and suppliers can be arduous and time-consuming, often requiring significant time and effort from the company performing the evaluation. This evaluation is typically performed when companies review potential business partners for services or products, and vendors and suppliers are prepared to answer and address business-related questions. The challenge with adding business continuity and resilience questions to the evaluation process is that vendors must be more technically well-versed in these areas or rely on other company employees to respond. This adds time and complexity to an already time-consuming and complicated process.

The challenge is how to discern a measurable response from vendors that will provide a substantiative view into a company's business continuity practices without dramatically impacting the new vendor evaluation process. The Critical Supplier Resilience Index (CSRI) aims to provide insight into a company's BCDR capability, not an in-depth analysis. The questions and their responses are meant to give the interviewing company 1) a cursory, high-level understanding of the company's capabilities and 2) an indication of where more investigation will be required.

Three recommended categories of questions comprise the CSRI and will provide a framework for companies to focus on and work within. These categories can be modified as necessary to meet a company's needs. They should be reviewed frequently as the company and interviewer mature in the BCDR practice and the business model evolves. The three recommended categories are 1) Business Information, 2) Business Continuity Planning, and 3) Disaster Recovery Planning.

Business Information (BI) consists of basic information that should be part of the standard vendor evaluation process and is typically gathered as part of the new vendor information packet. BI is foundational information about a company's locations, points of contact, insurance specifics, and supplier relations. For some companies, this information may be included in their business continuity plans or part of their core vendor information; however, it is a critical component of business resilience.

Business Continuity Planning (BCP) questions refer to a company's ability to respond to natural and human-made disasters in its operations and extended network. BCPs focus on preparation and response plans for business processes.

Disaster Recovery (DR) questions will refer to a company's ability to respond to digital outages, such as cyber-attacks or ransomware attacks. They will also consider a company's core resilience related to everyday disaster recovery capabilities, such as data backup capabilities.

Again, the purpose of the questions in each category is to provide insight and guidance on where more research is needed, not an in-depth review of capabilities. By limiting the questions to a "Yes" or "No" response, companies are more likely to participate. Also, it should be fully expected that some degree of follow-up will be required, but the purpose will initially be to

provide insight. If it is determined that a more in-depth review is needed before a decision is made regarding the vendor, the interviewing company will have the opportunity to do so if they choose.

The following questions are based on experience and recommendations from business continuity industry professionals. They can be modified based on each company's needs and experiences. As companies become more familiar and comfortable with the process, they can be updated to meet the practitioner's experience level.

Business Information (BI) Questions:

- Does your company have primary, secondary, and tertiary points of contact, including email, office phone, and mobile phone, available 24x7x365 for all work locations?
- Does your company have up-to-date and complete addresses for all work locations?
- Does your company have up-to-date and executed contracts with all current vendors, suppliers, and contractors?
- Does your company have catastrophic (CAT) property insurance?

Business Continuity Planning (BCP) Questions:

- Does your company have personnel dedicated to business continuity planning?
- Does your company have documented business continuity plans for all critical operations?
- Does your company have a written business continuity plan for the product or service this questionnaire evaluates?
- Does your company have emergency plans for natural and human-made disasters?
- Does your company perform a business impact analysis yearly?
- Does your company have plans for loss of utilities, such as power, water, sewage, or data network/communications?
- Does your company have a 24-hour emergency operations center or watch desk?
- Does your company have a mass notification system implemented and used regularly?
- Do you exercise or test your business continuity plans at least yearly?

Disaster Recovery (DR) Questions

- Does your company have personnel dedicated to disaster recovery planning?
- Does your company have documented disaster recovery plans, scripts, recovery time objectives, and recovery point objectives for all critical systems?
- Does your company have secondary or fallback data center capabilities?
- Does your company have DR drills or exercises at least once a year?
- Has your company outsourced any information technology components, personnel, or capabilities?
- Does your company have a ransomware and cyber security breach recovery plan?

- Does your company have any outsourced programs, componentry, technology, or personnel based in China or Russia?

Each question above will carry a score of 5 points. The vendor performance will be graded on a scale of one to one hundred points, with letter grades being assigned based on the traditional school grading system of 100-90 being an A, 89 to 80 being a B, 79 to 70 being a C, 69-60 being a D and anything below 60 resulting in a failing grade. The resulting score will serve as the Critical Supplier Resilience Index (CSRI), providing the business owner with a measurement to assess each vendor and to serve as a measurement to evaluate further growth and development.

The questionnaire answers should be reviewed line by line, not just the overall grade, to identify risk points and vulnerabilities. However, any vendor scoring a D or less should be reviewed in detail, and a follow-up meeting should be scheduled to determine how and if risks can be mitigated before entering into a contractual agreement. Also, follow-up should be required if all questions that received a “No” response are in a specific category.

The CSRI weighting of each question and the grading system are all subjective to the requirements and needs of the company administering the assessment. If a company is technology-based, more weight could be applied to questions related to DR. Also, if a company is a government or military contractor, any “No” response could trigger a review or rejection. The weight given to each question and the grading system can and should be reviewed and agreed upon by all those evaluating the vendor and senior leadership before administering the assessment process.

Once the questionnaire is administered, results are returned, and the CSRI is established, a quick review of the answers will provide insight into whether additional follow-up is warranted and what type of follow-up is warranted. If you do not see any issues or concerns after quickly reviewing the responses, you should make a note and share your findings with the procurement or administrative personnel reviewing the contractor. Regardless of findings and grades, results and recommendations should be documented and shared with leadership and the department reviewing the specific contractor. If there is a failing grade or a particular area of concern based on the product or service being provided by the contractor, the assessment administrator should reach out and schedule time to review and discuss with the procurement or administrative personnel reviewing the contractor to ensure the risk is understood and there is no misinterpretation of the assessment results, this should be followed up by written correspondence between the two parties documenting the conversation.

As a part of the vendor evaluation process, there is also a set of questions that you should consider internally as you evaluate vendors for value-added outsourcing. Like the questions above used to assess external candidates for contracted work or products, these questions ensure that you have plans to recover quickly if a contractor or supplier fails to deliver on their contracted commitments.

Some questions to consider as you are evaluating external resources that will complement the outsourcing process are as follows:

- Have you identified and contracted backup suppliers if you lose the supplier being evaluated?
- Do you know the engagement process and lead times for contracted products or services if you need to engage the backup supplier emergently?
- Is your backup supplier aware that they are serving in that capacity and have the resources and supplies to support your contract?
- Do you have a good list of subcontractors, suppliers, and outsourced services that your supplier uses to produce your contracted product or service?
- Have you identified conditions or hazards that might affect your backup suppliers and their suppliers?
- Have you utilized your backup supplier in the past year?

By utilizing the CSRI, you should have a good understanding of your supplier's business continuity and disaster recovery capabilities and the extent to which you can recover if the supplier being evaluated has an issue. As mentioned above, this process will provide a cursory glance into the supplier's capabilities and will serve as a good indicator as to whether further investigation is required.

If a business wanted or required a more in-depth initial review, you could use a scored survey. Scored surveys allow for multiple-choice responses for each survey question, allowing you to assign weights to each response and provide a more granular scoring evaluation for each question.

As the CSRI is intended to be an initial assessment, caution should be taken not to make the questions on the scored survey too complex, as that may result in additional time needed to complete the evaluation or false answers.

An example of a business continuity-centric scored survey question could be as follows:

- How often does your company review business continuity plans?
    - Yearly
    - Every two years
    - Three to five years
    - Only when an incident occurs
    - No scheduled reviews

With a scored survey, each one of the responses would be assigned a value based on what you, as the assessor, deem essential to your company or project. If it is critical that your suppliers evaluate their business continuity plans yearly, a score of 5 can be assigned to option number one, "Yearly." The other options could be assigned values based on a company's or project's risk

tolerance. Performing a scored survey provides a more in-depth view of the supplier's plans and planning process and provides a good mechanism to provide suppliers feedback on their plans and planning as it relates to a company's needs. This feedback loop is valuable as it builds more resilient primary suppliers and suppliers that may be needed to serve as a secondary source.

Establishing the CSRI for each vendor, whether a simple survey or a scored survey, will give business owners some visibility into each supplier's resilience capabilities. The CSRI score will quickly and easily guide business owners on how to proceed with vendors and whether more evaluation is needed. Business owners can make critical supplier decisions based on criteria including business continuity, disaster recovery, and essential business operations by providing an easy-to-administer and easy-to-understand index.

Conclusion

Developing an extended enterprise risk management (EERM) program is time-consuming and arduous but will inevitably result in a more resilient, productive, and successful business overall. By evaluating and establishing CSRIs for each of your critical suppliers, you are taking the first step in building strong BCDR processes for your company. EERM is a journey and should be considered a vital business process, given the proper resources, attention, and funding as any other critical business component. As the EERM matures and BCDR components are integrated into everyday business practices, companies will become more capable of weathering storms and disruptions that will inevitably come their way, resulting in increased customer satisfaction, better business results, and a culture of resilience.

References

Disaster Recovery Journal Glossary of Terms. (10/31/2023). Self-report. In Disaster Recovery Journal Glossary of Terms. https://drj.com/resources/drj-glossary-of-terms/

Fed Small Business. (11/2022). The Impact of Natural Disasters on Small Businesses. https://www.fedsmallbusiness.org/analysis/2022/impact-of-natural-disasters-on-small-businesses

Federal Bureau of Investigation. (04/18/2024). Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says. https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says

Federal Emergency Management Association. (2023). *Effects of Disasters on Small Businesses.* https://emilms.fema.gov/is_0111a/groups/23.html

Gross, M. (03/03/2014). What We Talk About When We Talk About Sriracha. bon appetit. https://www.bonappetit.com/entertaining-style/trends-news/article/what-we-talk-about-sriracha

International Organization for Standardization. (10/2019). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. https://www.iso.org/standard/75106.html

McKay, J. (07/27/2018). Small Businesses Are a Vital Part of Community Resiliency but Often Overlook Vulnerabilities. *Government Technology*. https://www.govtech.com/em/preparedness/small-businesses-are-a-vital-part-of-community-resiliency-but-often-overlook-vulnerabilities.html

Miller, A., Hopper, A., Lee, F., Campbell, J., Serrano, O., & Abrahams, S. (2021). Thought leadership insights into the future of collaborative working. *Institute for Collaborative Working*. https://instituteforcollaborativeworking.com/Research-and-Knowledge/Resource-Library/Thought-Leadership-Insights

Vitasek, K. (05/09/2024). What A Sriracha Shortage Teaches Us About Supply Chains. *Forbes*. https://www.forbes.com/sites/katevitasek/2024/05/09/future-sriracha-shortage-shows-need-for-trust-with-supply-chain-partners/

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

© 2024 The Sam Houston State University Institute for Homeland Security

Noakes, J. R. (2024). What's the Weakest Link in Your Supply Chain? (Report No. IHS/CR-2024-1027). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/84YJC