CRITICAL VENDORS: THE MHA GUIDE TO SECURING YOUR SUPPLY CHAIN

MICHAEL HERRERA & RICHARD LONG

MHA CONSULTING
WHEN SUCCESS MATTERS

Table of Contents

INTRODUCTION....3
The Weakest Link....3
Overview of the Ebook....3
Who You Are....4
Who We Are....4
MHA Consulting Services and BCMMETRICS Products....4

CHAPTER 1: THE SUPPLY CHAIN THREAT AND BUSINESS CONTINUITY....5
A Growing Risk....5
Hanging by a Thread....5
Background of the Supply Chain Threat....5
Rise in the Use of Third-Party Providers....5
Increased Use of Collaboration Services....5
Rise in Cyberattacks....6
Dependence on China....6
Increase in Extreme Weather....6
Stabilizing Influences....6
Business's Response to Supply Chain Insecurity....7
Common Supply Chain Mistakes....7
How to Achieve Supply Chain Security....7
Takeaways....8

CHAPTER 2: SETTING UP A SUPPLY CHAIN RISK GOVERNANCE STRUCTURE....9
When Companies Lack a Supply Chain Risk Governance Structure....9
The Benefits of Sound Governance....9
Setting Up the Oversight Team....9
Work of the Oversight Team....10
Writing the Policies and Standards....10
Takeaways....10

CHAPTER 3: IDENTIFYING YOUR CRITICAL VENDORS....11
What Is a Critical Vendor....11
A Common Misunderstanding....11
Prioritizing the Business Processes....11
Conducting a BIA....11
Rating Vendors for Criticality....12
Consult Your BIA Results....12
Use Institutional Knowledge....12
Rank Vendors by Company Spending Level....12
Back-of-the-Envelope Assessment....12
Preparing a Detailed Master Vendor List....13
Takeaways....13

CHAPTER 4: ASSESSING THE THREATS TO YOUR CRITICAL VENDORS....14
Importance of the Vendor Threat Assessment....14
What to Look for in Assessing Vendor Threats and Resilience....14
Understanding a Vendor's Threat Profile....14
Assessing a Vendor's Resilience....14

How to Obtain the Needed Information 15
Remote Assessment 15
Documentation Review 15
Site Visit 16
Vendor Response 16
Cooperative Vendors 16
Unresponsive Vendors 16
Analyzing the Available Data 16
Identifying the Organization's Greatest Vulnerabilities 17
Takeaways 17

CHAPTER 5: IMPLEMENTING VENDOR THREAT MITIGATION STRATEGIES 18
Available Mitigation Strategies 18
Requesting Improvements 18
Fostering a Good Relationship 18
Identifying an Alternate Provider 18
Adding an Alternate Provider 18
Switching to an Alternate Provider 18
Diversifying Geographically 19
Devising Workarounds 19
Adding BCM Requirements to Vendor Contracts 19
What to Include in a Vendor Agreement 19
Unwilling Vendors 19
Implementing Mitigation Strategies 20
Takeaways 20

CHAPTER 6: CONCLUSION 21
The Future of Supply Chain Security 21
Takeaways 21

Critical Vendors: The MHA Guide to Securing Your Supply Chain

INTRODUCTION

The problems of the global supply chain have become front-page news. In recent months, images of container ships waiting outside ports and empty shelves in stores have become staples of the news media. A perfect storm of developments started by the COVID-19 pandemic has led to serious bottlenecks and shortages, thrusting supply chain security to the top of the national agenda.

However, concern about the global supply chain is nothing new for business continuity management (BCM) professionals. BCM professionals have long been trained about the need to protect their organizations against the loss of critical vendors (along with losses of facilities, human resources, and technology).

We at MHA Consulting and BCMMETRICS have been advising our clients for years about the importance of safeguarding themselves against possible disruptions in their supplies of critical goods and services. Before the current crisis, we published articles warning that third-party vendors could become companies' Achilles' heel and describing the corporate supply chain as a ticking time bomb.

This ebook arose from our conclusion that the supply chain has become the greatest source of vulnerability for most organizations. We estimate that among our clients, seven out of every 10 are vulnerable to being disrupted by the loss of a critical third-party product or service.

The Weakest Link

The supply chain has become the weakest link for most organizations in terms of their ability to carry out their mission-critical functions. These vulnerabilities preceded the current supply chain crunch and will persist after it. Indeed, several global trends suggest the problem will grow worse in the years to come.

This ebook does not propose a solution to the current global supply chain crisis. We are not logistics experts and do not have such a solution. This ebook offers a series of steps that organizations can take to manage down the risk in their supply chains over time, thus reducing their vulnerability to disruption, enhancing their resilience, and protecting their operations and stakeholders.

If the current crisis becomes a learning moment for organizations about the need to implement long-term protections against supply chain disruption, that would be a significant silver lining.

Overview of the Ebook

The ebook describes how supply chain insecurity poses a threat to organizations and sets out a four-step process they can implement to protect themselves. It will lead you to an understanding of the following topics:

- The severity of business's vulnerability to supply chain interruptions, the background of the threat, and common mistakes organizations make in managing supply chain risk (Chapter 1: "The Supply Chain Threat and Business Continuity")
- Why it is important to set up a supply chain risk governance structure and how to do it (Chapter 2: "Setting Up a Supply Chain Risk Governance Structure")
- What a critical vendor is and how to identify which of your suppliers are your critical vendors (Chapter 3: "Identifying Your Critical Vendors")

- The importance of assessing the threats to your critical vendors and their readiness to deal with them, and how to go about doing this (Chapter 4: "Assessing the Threats to Your Critical Vendors")
- The main vendor threat mitigation strategies, the importance of including business continuity requirements in supplier agreements, and how to implement these measures (Chapter 5: "Implementing Vendor Threat Mitigation Strategies")

Each chapter concludes with a list of takeaways summing up the points you really need to know.

Who You Are

This book is intended for frontline business continuity management (BCM) professionals who wish to gain a deeper understanding of the issues of the contemporary supply chain from a BC perspective and improve the supply chain security of their organizations. The information applies to organizations of all types: corporations, privately held companies, nonprofit organizations, educational institutions, and local, state, and federal agencies.

Who We Are

We are the CEO and founder of MHA Consulting (Michael Herrera) and a senior advisory consultant at MHA (Richard Long). We previously coauthored the ebooks Crisis Management: A Handbook for BCM Professionals and Your BIA Action Guide: A Handbook for BIA Professionals, and Michael is the author of the ebook 10 Keys to a Peak-Performing BCM Program.

As CEO of MHA Consulting, Michael has led MHA to a position as a leading provider of Business Continuity and Disaster Recovery services to organizations of all sizes in a wide range of industries in the United States and abroad, including many Fortune 500 companies. He is also the founder of BCMMETRICS, a cloud-based suite of continuity tools designed to help BCM professionals build comprehensive programs. Prior to founding MHA, he was a regional VP for Bank of America, where he was responsible for business continuity across the southwest region.

Richard is one of MHA's practice team leaders for technology and disaster recovery related engagements. He has been responsible for the successful execution of MHA business continuity and disaster recovery engagements in industries such as energy and utilities, government services, healthcare, insurance, risk management, travel and entertainment, consumer products, and education. Prior to joining MHA, Richard held senior IT director positions at PetSmart (NASDAQ: PETM) and Avnet, Inc. (NYSE: AVT).

MHA Consulting Services and BCMMETRICS Products

MHA Consulting offers a variety of services to help organizations improve the security of their supply chains, from supply chain security assessments to critical vendor identification to vendor risk mitigation plans. Our affiliated company BCMMETRICS offers the Compliance Confidence (C2) assessment tool as part of its BCMMetrics™ suite of online business continuity software. C2 makes it easy to evaluate the resilience of your third-party vendors and work with them on improving their BCM programs.

Don't hesitate to get in touch to discuss how our services and products can help organizations improve their supply chain security and become more resilient overall.

Michael Herrera, CEO (herrera@mha-it.com) and
Richard Long, Senior Advisory Consultant (long@mha-it.com)
MHA Consulting

CHAPTER 1: THE SUPPLY CHAIN THREAT AND BUSINESS CONTINUITY

The current crisis has brought the problems of the global supply chain to the forefront for consumers and businesses. But the problem of the supply chain from the business continuity perspective developed before the current crunch and will continue beyond it.

In this chapter, we will give an overview of the supply-chain issue from the BCM perspective, discuss a few of the major themes of the contemporary supply chain as they relate to resiliency, and look at business's response to its supply chain risk. We will also introduce the steps organizations should take to secure their supply chains and which will be spelled out in the rest of the ebook.

A Growing Risk

From the point of view of an organization, the chief concern about the global supply chain is that the organization might be prevented from carrying out its mission-critical activities due to the unavailability of a product or service that it normally obtains through a third-party vendor.

This risk is strong and growing for most organizations. The threat has typically been ignored and discounted, though fortunately that might be changing as a result of the current crunch. We wish to call attention to and explain this threat and help organizations get it under control.

Hanging by a Thread

Many businesses are dependent on third-party vendors and yet have minimal awareness about these dependencies, little visibility into individual vendors' resilience, and little to no influence over them. In most cases they also lack a Plan B for what they would do if a critical resource became unavailable.

This situation can leave the organization hanging by a thread. When their vendors have a problem, organizations have to scramble to come up with backup providers or workarounds. Sometimes their operations are brought to a standstill.

This happened often before the current supply chain crunch. It's happening more now. Several global trends suggest the problem will get worse in the future, even after the present crisis is alleviated.

Background of the Supply Chain Threat

The trend of organizations becoming more vulnerable to the loss of critical vendors is taking place against a background made up of the following elements:

Rise in the Use of Third-Party Providers

A central driver of the increase in risk in the corporate supply chain is the rise in the use of third-party service providers. Today organizations routinely hire third-party vendors to provide services and tools to perform functions that would formerly have been handled in-house. Examples of commonly outsourced services include application development, call center operations, manufacturing, logistics, and IT services. Third-party software tools that support payroll, enterprise resource planning, sales and marketing, and meetings also fall into this category.

From the BC perspective, there is nothing inherently wrong with an organization turning to outside vendors to meet their needs. But safeguards must be implemented because dependence on services and tools controlled by others diminishes visibility and increases risk.

Increased Use of Collaboration Services

When the COVID-19 pandemic began, the use of third-party collaboration platforms such as Zoom and GoToMeeting increased. Such tools are of great benefit from the business continuity perspective. They enable employees to maintain social distancing during pandemic conditions and allow workers to remain connected while working from home in the event of a loss of a central facility.

How prevalent the use of such tools will be moving forward is unknown. Organizations should keep up the ability to use collaboration services even once COVID-19 recedes. However, these services do experience periodic slowdowns and outages. In the past, such outages have affected platforms run by even the largest companies, such as Google and Microsoft. To the extent that organizations depend on these tools to perform critical functions, they are bringing significant new risk into their supply chains.

Rise in Cyberattacks

The rise in the frequency of cyberattacks poses a growing threat to the corporate supply chain. Organizations' vulnerability to such attacks varies with their circumstances and dependencies. For any organization, a cyberattack on one of its key vendors has the potential to deprive it of a critical product or service.

A cyberattack on a vendor can also harm an organization directly. The attacker can steal critical organizational data in the vendor's possession. Attackers who breach the computing systems of a vendor providing IT services to the organization might be able to gain backdoor access to the organization's computers, allowing the hackers to spy on its activities and cripple its operations.

The risk of back-door attacks through IT services providers is an overlooked problem and one likely to increase in the coming years.

Dependence on China

One of the most striking features of the corporate supply chain is its outsized reliance on a single country, China. The fact that China is on the other side of the Pacific Ocean from the United States is a massive liability. So is the fact that China is a one-party state that exercises tight control over its people and is in a state of chronic tension with the U.S.

The U.S. has come to depend on Chinese vendors because doing so has been easy and cheap. But this part of the supply network is not secure. The dangers of relying on China include the length and vulnerability of the shipping routes, the suppliers' lack of resilience, and the threat of trade and geopolitics conflicts.

This is an especially big issue with pharmaceutical companies.

Increase in Extreme Weather

The rise in extreme weather brought about by climate change is another threat to the contemporary corporate supply chain. The smooth functioning of the global supply network depends on the prevalence of moderate and predictable weather patterns. Extreme weather events have the power to disrupt the physical transportation of goods by ship, road, rail, and plane. They also threaten the infrastructure needed to provide services electronically.

As climate change disrupts familiar weather patterns—and increases the frequency of extreme weather events such as hurricanes, wildfires, and heat waves—the threats to the supply chain increase and with them the threats to the ability of organizations to carry out their mission-critical operations.

Stabilizing Influences

Fortunately, there are a few stabilizing influences in the background of the vendors problem.

One is the existence of regulations such as those of the Federal Financial Institutions Examination Council (FFIEC). Institutions operating under the FFIEC or similar regimes are required to assess and verify the security of their supply chains.

A second stabilizing influence is that, as awareness of supply chain vulnerabilities grows, more organizations are requiring their suppliers to demonstrate their resilience.

A third is that forward-thinking vendors are coming to realize that they can gain a competitive advantage by being able to show potential customers that they have sound business continuity programs. In the future, this will probably become a requirement.

Business's Response to Supply Chain Insecurity

Organizations have responded in a variety of ways to the problem of supply chain insecurity.

A small minority have implemented rigorous programs to vet vendors, insist on high standards in vendors' continuity planning, and identify alternate sources of supply for critical goods and services. Some organizations have taken things to the next level by vetting their fourth-party vendors, their suppliers' suppliers.

However, the vast majority of organizations today have been half-hearted in their efforts, leaving their supply networks riddled with risk. Some unprepared organizations have already suffered supply-related impacts. All remain vulnerable to such disruptions moving forward.

Common Supply Chain Mistakes

Unprepared organizations tend to make the same types of mistakes in trying to make their supply chains more resilient. The most common are:

- Bringing a casual, check-the-box attitude to the job of identifying threats and vetting suppliers.
- Failing to regularly look at and assess risks of all types across their supply chain.
- Failing to adequately vet their suppliers' recovery plans.
- Being overly willing to believe their vendors' claims that they are resilient.
- Not pressing their suppliers about their continuity plans for fear of antagonizing them.
- Not following a standardized approach in evaluating suppliers' resiliency.
- Not ensuring that the people performing vendor BC assessments are properly trained.
- Not verifying the resiliency of their fourth-party vendors (their suppliers' suppliers).
- Overestimating the reliability and motivation of Software as a Service (SaaS) providers.

How to Achieve Supply Chain Security

Few organizations today enjoy true supply chain security; however, the process for achieving such security is straightforward and within the reach of every organization. The process comes down to adopting one particular overarching attitude and implementing four relatively simple steps.

First, the attitude. During the 1980s, American negotiators in nuclear disarmament talks with the Soviet Union described their approach as "trust but verify." The phrase describes the need to treat the other party's claims with cordiality but also insist on evidence to validate them. This is the attitude organizations need to take in vetting their critical third-party suppliers.

The four steps that should be implemented are as follows:

1. Establish a governance program for managing supply chain risk.
2. Identify your critical vendors.
3. Assess the threats to your critical vendors and their readiness to deal with them.
4. Take steps to mitigate the most likely and potentially impactful threats.

The rest of this book will demonstrate this attitude and explain the steps. By adopting and implementing them, every organization can improve the security of its supply chain, thus ensuring its ability to carry out its mission, boosting its overall resilience and protecting its stakeholders.

TAKEAWAYS

- Supply chain insecurity is a large and growing threat.
- Many organizations would be unable to carry on their mission-critical activities if they suffered the loss of a vendor providing them with a critical product or service.
- The background of this issue includes the rise in the use of third-party providers and collaboration services and an increase in cyberattacks, extreme weather, and dependence on China.
- Most organizations have done little or nothing to protect themselves against supply chain insecurity, leaving them highly vulnerable.
- The rest of this book shows how organizations can reduce the risk in their supply chains, increasing their resilience and protecting their stakeholders.

CHAPTER 2: SETTING UP A SUPPLY CHAIN RISK GOVERNANCE STRUCTURE

The first step in protecting your organization against impacts caused by the loss of critical goods and services is to establish a governance structure for overseeing your supply chain. A good supply chain risk management (SCRM) governance structure consists of two things: an oversight team and a set of policies and standards setting forth how the organization will manage the areas that influence supply chain risk.

When Companies Lack a Supply Chain Risk Governance Structure

Organizations that lack a solid SCRM governance structure are handicapped in their efforts to reduce the risk in their supply chains. The employees at such organizations, rather than pulling together, typically work to different standards or no standards at all, sending mixed messages to vendors and allowing them to evade responsibility.

Organizations in this situation have little hope of gaining a clear understanding of the risk in their supply chains, much less bringing it under control. The procurement people at such an organization are unlikely to evaluate the vendors on a business continuity basis. They have no way of knowing which vendors provide excellent service, which should be replaced, and where refunds should be sought.

Without an SCRM governance structure, confusion reigns and supply chain risk spreads like wildfire.

The Benefits of Sound Governance

Having a sound supply chain risk management governance structure brings many benefits in the effort to reduce supply chain risk.

It makes it clear who is in charge of SCRM, creating a center of authority and accountability. It also creates rules of the road defining how the organization will evaluate vendors and the continuity standards vendors are expected to meet.

Developing a solid SCRM governance structure is the first step toward understanding and reducing the risks that are transmitted to the organization through its third-party vendors.

Setting Up the Oversight Team

The first step in establishing a sound SCRM governance structure is to set up an oversight team. The contours of the team will vary depending on the size of your organization, its culture, and the level of support your effort enjoys from senior management. Ultimately, the most important thing is not the composition of the team but that certain key functions typically performed by the team be carried out by someone.

The SCRM team is usually set up as an independent risk management office though sometimes it is located in the business continuity office.

In the ideal case, the SCRM oversight team will have as a sponsor and overall leader a senior executive who champions the effort and has the primary responsibility for its success. This person allocates resources and helps the team get through roadblocks.

The SCRM group's membership should be a cross-functional group of senior leaders drawn from across the organization and include representatives of the procurement, legal, IT, and enterprise risk departments, as well as people from business areas across the organization that are heavy users of goods and services provided by third-party vendors.

The responsibilities of the individual SCRM group roles should be documented, reviewed with the members, and formally approved.

Work of the Oversight Team

The responsibilities of the SCRM oversight team are the same regardless of its size or level of formality. The team's main duties are:

- Identify the organization's critical vendors.
- Assess the threats and risks facing the critical vendors.
- Assess the robustness of critical vendors' business continuity planning.
- Develop mitigation strategies to protect the organization against the loss of its critical vendors.
- Work to obtain approval of mitigation strategies by senior management.
- Implement the approved mitigation strategies.
- Develop the policies and standards that govern supply chain risk management.

The oversight team also establishes the strategic direction of the SCRM program; performs continuous, proactive monitoring of the supply chain; meets regularly to review the state of the supply chain; and pushes to make evaluating suppliers from the BC perspective a regular part of the company's way of doing business.

These activities will be explained in subsequent chapters.

Writing the Policies and Standards

The supply chain risk management group is responsible for writing the policies and standards that govern the organization's approach to managing its third-party vendors. These rules and policies are typically developed in consultation with the supply chain stakeholders and senior management and might require management approval.

The goals of the SCRM policies and standards are to bring about consistency and uniformity, heighten efficiency, increase visibility into suppliers' risk profiles, and bring down supply chain risk.

The SCRM policies and standards typically address issues affecting the following: critical suppliers, activities, functions, services, materials, goods, partnerships, supply chains, relationships with interested parties, and the potential impacts related to a disruptive incident.

The SCRM policies and standards codify and standardize the approach the company will take in managing its relations with its third-party suppliers. They are commonly incorporated in purchasing agreements and contracts as a way of obliging suppliers to meet certain standards.

Subsequent chapters will look in detail at the topics that form the main themes of the SCRM policies and standards.

Takeaways

- Developing a governance structure to manage supply chain risk is the first step toward reducing the threats to the organization from its third-party vendors.
- The main elements of a supply chain risk management governance structure are the oversight team, the team sponsor, and the policies and standards that govern the organization's relationships with its suppliers.
- The main tasks of the oversight team are writing the policies and standards, identifying critical vendors, assessing vendor threats and resilience, and developing and implementing mitigation strategies.
- The remaining chapters of this book will describe those activities in detail.

CHAPTER 3: IDENTIFYING YOUR CRITICAL VENDORS

As your organization tries to reduce the risk in its supply chain, a key early task is developing a solid understanding of your vendor network. You need to know what goods or services the different vendors provide and how losing each vendor would impact the organization's operations.

Furthermore, you need to identify your organization's **critical vendors**, the suppliers it depends on to carry out its core mission. These are the vendors you will focus on in the later stages of the supply chain risk management process.

What Is a Critical Vendor

A critical vendor is a third-party supplier that provides the organization with a product or service that is essential to its ability to carry out its core functions.

A critical vendor can be defined as:

- Any vendor that, by missing its commitments, would cause the organization to be unable to achieve a stakeholder's core mission.
- Vendors who are the only available provider of an important resource.
- Any vendor that supplies a product or service crucial to helping the organization recover from a crisis.

Third-party products or services can be critical to a process if a high volume of the item or service is required or if the lack of it would quickly bring the process to a halt.

A Common Misunderstanding

A common misunderstanding is thinking that the organization must provide comprehensive protection against the loss of all of its vendors. This often leads to discouragement since many organizations have hundreds, if not thousands, of suppliers.

Your organization only needs to protect itself against the loss of vendors providing goods and services critical to its ability to carry out its core operations. This is usually a much smaller, more manageable number.

Suppose your organization purchases goods and services from 500 vendors. Your SCRM team might realize after conducting its analysis that only a dozen of these provide mission-critical resources. Those 12 vendors would receive the full package of mitigations described in this book. Your other suppliers would receive limited or no protection since the resources they provide are less important and/or are easily available from other sources.

Prioritizing the Business Processes

Before your organization can identify its critical suppliers, it must know which of its business processes are most important. The products and services needed to perform the most important and time-sensitive business processes are in most cases the critical products and services. The suppliers that provide those products and services will in most cases be your organization's critical vendors.

As a business continuity professional, you will already be familiar with the best method of prioritizing your organization's business processes: the Business Impact Analysis (BIA). As a first step in identifying your critical vendors, your SCRM team should consult the organization's most recent BIA or arrange for a new one to be performed if no current BIA exists.

Conducting a BIA

In doing a BIA, a team of in-house business continuity professionals (or outside consultants) conducts a department-by-department survey of the organization. Key members of each department are asked to fill in a questionnaire and sit for an interview about their department's business processes. These experts list, describe, and prioritize their department's business processes, ranking them based on the severity of the impact to the organization if they could not be performed for various periods of time. The department-level results are synthesized in discussions with higher-level managers, arriving at a prioritized listing of the organization's business processes overall.

The BIA enables the organization to determine its critical external dependencies. The suppliers that provide the goods and services needed to perform the highest-priority and most time-sensitive processes are those that might be worthy of designating as critical, depending on additional factors.

Rating Vendors for Criticality

Once your organization's business processes have been prioritized, your SCRM team can begin identifying the company's critical vendors. There are many possible approaches to use in rating vendors for criticality. Which is best for your organization will depend on its size, complexity, and culture.

The following methods are good ways of identifying which vendors the organization truly depends on. They can be used singly or in combination.

Consult Your BIA Results

Consulting your BIA results is an excellent place to begin in identifying which vendors are critical to your organization. Note which business processes are the most critically time sensitive, determine which products and services they depend on, and identify the third-party suppliers that provide those products and services. This will give you a good understanding of what vendors you should focus on in your threat assessment and mitigation efforts.

Use Institutional Knowledge

Many companies have employees who have deep first-hand experience of the organization's supply chain as a result of having worked for many years in a related department, such as material control or procurement. Such people are typically highly knowledgeable about the organization's vendors and their relative importance to its operations. They might even have put together lists with the suppliers ranked by priority. The institutional knowledge of these employees can be an excellent resource in helping the supply chain risk management group rank suppliers for business continuity purposes.

Rank Vendors by Company Spending Level

Ranking your suppliers by how much your organization spends with them is another good way of getting a handle on which vendors you depend on most. Looking at company spending figures can reveal critical dependencies that might otherwise get overlooked.

Discretion should be used in applying this metric since the organization might spend a lot with one vendor on a commodity that could easily be obtained from another supplier. In such a case, spend level is not a true measure of vendor criticality.

The opposite situation can also occur, as when a company only rarely buys something from a supplier, but the item purchased is one that the organization cannot operate without (e.g., a specialty machine part).

Back-of-the-Envelope Assessment

Similar to using institutional knowledge is a method that might be called a back-of-the-envelope assessment. In this informal technique, a few well-informed people put their heads together and jot their thoughts on vendor criticality down on the proverbial envelope.

The participants should evaluate the relative importance of each supplier by asking themselves questions such as: How important is the vendor's product or service to the processes of the company? Does the vendor supply a commodity that can easily be found elsewhere or a specialized product with few or no other potential suppliers? How critical is the vendor's part or service to the business?

In the absence of resources to conduct a more thorough study, a back-of-the-envelope assessment is a reasonable place to begin in identifying which suppliers merit mitigation.

Preparing a Detailed Master Vendor List

If your organization's SCRM effort is backed by sufficient resources, you should consider compiling a Detailed Master Vendor (DMV) list. Such a list states how each product or service maps to the business processes, how critical the product or service is to each process, and what should be done if the product or service becomes unavailable.

A good DMV list includes the following information for each vendor:

- The product or service the vendor provides.
- The business process(es) in which the product or service is used.
- An indication of which processes would be impacted and what the impacts would be (primary and secondary) if the product or service were to become unavailable.
- A rating of the importance of the product or service to each process in which it is used. (Rate the product Critical if the process cannot proceed without it, Moderate if the product's absence would quickly but not immediately stop the process, and Low if the product or service is "nice to have" rather than essential or if it can easily be replaced.)
- Whether the vendor is the sole available provider of a resource.

The DMV list, which should be updated at least once a year, can be consulted to obtain sublists of critical products and services that are tailored for each recovery plan (keep the sublists with the plans).

Assembling a DMV list is an activity for which the saying "Don't let the perfect be the enemy of the good" applies. Your team should put together the best list it can without spending too much time on it. The list will mature over time.

As a final step, the DMV list should be reviewed and approved by management, if possible.

Takeaways

- The organization's critical vendors are those that provide it with a product or service essential to its ability to carry out its core functions.
- To identify its critical vendors, an organization must first develop a prioritized list of its business processes.
- Good methods of ranking vendors for criticality include consulting a current BIA, using institutional knowledge, and ranking vendors by company spending level.
- A Detailed Master Vendor list states how each product or service maps to the business processes, how critical the resource is to each process, the impact on the company if the resource were lost, and what should be done if the resource becomes unavailable.

CHAPTER 4: ASSESSING THE THREATS TO YOUR CRITICAL VENDORS

Once your organization has identified its critical vendors, it should conduct a threat assessment of each one, looking at the threats and risks it faces and how prepared it is to respond to them.

The best attitude to take when vetting vendors is "trust but verify."

Importance of the Vendor Threat Assessment

The reason your organization should inform itself about the threats facing your critical vendors is because their exposure carries over to your organization owing to your dependence on them for one or more critical products or services. This relationship means their risk is your risk.

To reduce the risk in your supply chain, your organization must understand exactly where the risk resides. It can then take steps to mitigate it.

Taking these steps requires gaining insight into the threats facing each critical vendor as well as their preparedness to deal with them.

For suppliers that provide your organization with critical technology services, do not assume they are secure because they are large, well-known, or based in the cloud.

What to Look for in Assessing Vendor Threats and Resilience

In assessing the threats facing your critical vendors, your organization should seek two types of information: the threats facing the vendor and their readiness to deal with each one.

Understanding a Vendor's Threat Profile

The threats facing each vendor will vary depending on their location and industry, among other factors.

The following are examples of the sort of threats and risks that should be considered:

- Exposure to natural disasters such as hurricanes, tornadoes, earthquakes, and wildfires.
- Exposure to industrial hazards such as nearby chemical plants and oil refineries.
- Exposure to loss of electrical power.
- Likelihood of being targeted by a cyberattack.
- Likelihood of being affected by incidents of civil unrest.
- Tendency toward high workforce turnover.
- Tendency toward financial weakness or disarray.
- Vulnerability to mismanagement.
- Vulnerability of company and industry to negative macroeconomic trends.
- Likelihood of experiencing reputational damage.

For each potential threat, consider the chances of it occurring and the likely impact if it did occur.

Assessing a Vendor's Resilience

As you gain insight into the threats facing each critical vendor, you should also assess their readiness to deal with each threat. Essentially, you will be appraising the soundness of their business continuity management (BCM) program.

In terms of the risk carried over to your organization, there is a significant difference between a vendor exposed to a threat for which it is unprepared and another supplier facing the same threat but from a position of high readiness and resiliency.

The following is a list of some of the elements you should consider in appraising a vendor's business continuity program:

- Level of security of their physical facilities and computer systems.
- Level of their access to backup power supplies.
- For technology vendors, determine whether their security protocols are sufficient.
- Whether their annual BCM budget is sufficient to fund the execution of their BCM program on a daily basis.
- Status of their BCM program oversight, governance, and management team.
- Level of competence of their BCM program leadership, staff, and recovery teams.
- Status of their internal threat and risk assessment (documenting their threats and mitigation).
- Status of their crisis management planning, team, training, exercises, and maintenance.
- Status of their BIAs in terms of comprehensiveness, regularity, and recency.
- Degree to which BIA results are leveraged in recovery planning.
- Existence of and appropriateness of their recovery strategies.
- Status of their business continuity planning, training, exercises, validation, maintenance, and degree of alignment with industry standards.
- Status of their IT disaster recovery (IT/DR) teams, strategies, plans, training, exercises, validation, and maintenance.

By acquiring the above information, you gain the ability to gauge how vulnerable your critical vendors are to the threats they face. This helps you form a true picture of their exposure and hence your exposure, since your organization is dependent on them to carry out its mission-critical operations.

How to Obtain the Needed Information

There are three main methods for obtaining information about the threats facing your critical vendors and their readiness to deal with them.

Remote Assessment

A remote assessment is an informal appraisal of the vendor's threats and preparedness based on publicly available information and past experience. The team conducting the assessment considers the vendor's geographic location and industry, relevant information from the news, information available through internet searches, and everything it knows about the vendor and its BCM program based on past experience and conversations. This provides a preliminary sketch of the threats facing the vendor and its readiness to manage them.

Documentation Review

The organization requests and scrutinizes documents pertaining to the vendor's continuity planning. The reviewers might prepare and submit a questionnaire for the vendor to fill out, asking probing questions and giving a deadline of two to three weeks for the questionnaire to be completed. Such documents can reveal a lot about the threats facing the vendor, the quality of its recovery planning, and its attitude toward resiliency.

The documentation requested from each vendor should vary depending on their criticality. Suppliers deemed "Critical" should provide their current BIA, recovery plan, and annual live disaster recovery exercise results that prove the ability to meet or exceed Recovery Time Objective (RTO) requirements. Vendors classified as "Important" should provide their current BIA, recovery plan, and live disaster recovery exercise results every other year. Suppliers categorized as "Other" should provide their current BIA and recovery plan and results of annual desktop disaster recovery exercise.

By reviewing the documentation, knowledgeable reviewers can learn where the vendor falls on the spectrum of very lax to highly responsible in its business continuity planning. Some suppliers might send solid, comprehensive BCM plans and others only a two-page summary full of boilerplate. The reviewers' job is to evaluate the material submitted, identifying any gaps in the vendor's program and assessing how much risk they pose to their own organization.

A documentation review also allows the organization to understand such matters as to what extent vendors will be able or willing to increase support during a crisis event and the remediation for missed service-level agreements (SLAs) or commitments (often only a refund, with no consideration of other costs).

Site Visit

In a site visit, a person or team from the organization travels to the vendor's location, is taken on a tour, asks questions, reviews recovery documentation, and possibly observes a recovery exercise. A site visit is the most involved and expensive way of assessing vendor risks and readiness but also the most thorough.

Site visits allow the organization to test claims made in the recovery documentation. They allow the reviewers to assess the level of physical security with their own eyes or see whether the vendor's backup generator is really capable of supporting their whole operation, as claimed.

Visits that include an exercise allow the reviewers to see the vendor's recovery plans and team in action, giving them first-hand knowledge of their resiliency.

Vendor Response

Organizations seeking to gain information from their critical suppliers about their risks and resilience can meet with a wide range of responses from the vendors.

Cooperative Vendors

Many suppliers are happy to answer their customer's questions about their threats and continuity planning, provide the requested documentation, and host them for a visit. Such vendors tend to be ones that take business continuity seriously and have sound recovery plans. Their maturity and transparency amount to a risk mitigating factor over and above those contained in their recovery plans.

Unresponsive Vendors

Unfortunately, some vendors routinely ignore or deflect their customers' requests for information about their risks and preparedness. This can take various forms.

The unresponsive vendor might be too large relative to the customer to make it worth its while to field their inquiries. Such suppliers sometimes make a standard package of information on their recovery planning available. The reviewers will have to make do with this in assessing the vendor's threats and readiness.

Alternately, the vendor might know itself to be unprepared and stonewall out of a desire to avoid being exposed or embarrassed.

Some vendors are inconsistent, agreeing to a site visit, for example, and then betraying nervousness or annoyance at the reviewers' presence and questions.

Analyzing the Available Data

The reviewers' task is the same regardless of how much or little information the vendor provides: to analyze the available data and make an assessment of the threats facing the vendor and its readiness to deal with them.

Making such an assessment requires a degree of street smarts. A vendor's unresponsiveness or impatience can itself be a revealing data point about their readiness.

Identifying the Organization's Greatest Vulnerabilities

The ultimate goal is to identify your organization's greatest supply chain vulnerabilities. This is done by determining which of your critical vendors are the most likely to be hit by an outage and also the least prepared to deal with one. These are the suppliers you will prioritize in implementing the mitigation strategies described in the next chapter.

Takeaways

- The organization should assess the threats facing each of its critical vendors and also the vendor's readiness to deal with them.
- The needed information can be obtained by remote assessment, documentation review, and site visits.
- The best attitude to take in evaluating vendors' BCM programs is "trust but verify."
- Vendors differ in how responsive they are to requests for information about their threat profiles and BCM programs.
- The reviewers' job is to analyze the available data and make an assessment of the threats facing the vendor and the solidity of its business continuity program.
- The ultimate goal is to identify which of your critical suppliers pose the greatest threats to your organization.

CHAPTER 5: IMPLEMENTING VENDOR THREAT MITIGATION STRATEGIES

Once you have identified which of your critical vendors pose the biggest security threats to your organization, you are ready to begin developing and implementing strategies to reduce those risks.

Available Mitigation Strategies

There are several strategies available to help your organization mitigate the risk it incurs from its critical vendors. The strategies can potentially be implemented at any point in the history of your organization's relationship with the vendor.

Some strategies are implemented in partnership with the vendor; others can be put in place independently by your company. The strategies can be used singly or in combination.

Requesting Improvements

Your organization can ask the vendor to it strengthen its BCM program. In pursuing this strategy, your organization would explain its concerns about the vendor's resilience and propose changes to close the gaps you have identified. Their response is likely to depend on how much they value your business.

Ideally, your organization and the vendor will agree on the vendor's vulnerabilities and jointly devise a plan and timeline for addressing them. Your organization would then need to follow up to ensure that the outstanding issues were resolved in the allotted timeframe. If the vendor does not keep its end of the agreement, you would be well-advised to move on to one or more of the other strategies.

The important subject of including business continuity requirements in vendor contracts is discussed below.

Fostering a Good Relationship

Your organization can and should strive to build a good working relationship with its critical suppliers. The name and contact information for the liaison at each critical vendor should be easily accessible and up to date.

Keep abreast of any developments that might impact the supplier, such as hurricanes or wildfires. If the vendor is facing a challenge, get in touch and ask if they foresee any impact on their ability to provide the product or service you obtain from them. Diplomatically remind them that you are depending on them and ask what they are going to do to prevent or fix the disruption.

Identifying an Alternate Provider

Your organization can pre-identify a provider that is ready, willing, and able to provide the needed good or service in a timely fashion if the primary supplier were to go down. Doing this legwork ahead of time can speed recovery in the event of a vendor outage.

Adding an Alternate Provider

Your organization can maintain its relationship with the primary supplier but add an alternate provider of the critical product or service. If the primary vendor were to go down, your company could pivot to the alternate provider. Note that there might be issues of capacity in suddenly ramping up your orders from the alternate supplier. These should be explored and addressed ahead of time.

Switching to an Alternate Provider

If your primary supplier of a critical good or service is simply too vulnerable—and too unwilling to close the gaps you have identified—your best option might be ending your relationship with them and transferring your business to one or more vendors that are more responsible and resilient.

Diversifying Geographically

Try to source each critical good or service you use from vendors in different geographical locations. This eliminates the chance that a single region-wide problem will take out all of the vendors that provide you with a particular product or service.

In practice, this means do not source critical goods or services exclusively from providers in China, or the hurricane-prone Gulf Coast, or wildfire-prone areas of the West.

Devising Workarounds

Your organization can devise workarounds that can be used if your primary supplier of a critical product or service becomes unable to provide it. Such a workaround might involve turning to an alternate supplier, making a change in-house (such as performing a process manually) that enables your organization to continue its mission-critical operations without the critical component, at least for a period of time, or increasing your safety stock of critical products, supplies, or materials. Such workarounds can be noted in the Detailed Master Vendor List described in Chapter 2.

Adding BCM Requirements to Vendor Contracts

One of the most important supply chain risk mitigation tools is including business continuity requirements in vendor contracts and purchasing agreements. This practice is on the rise and likely to increase in the coming years.

Every organization should make it a goal to spell out in their supply contracts the BCM measures the vendor is obliged to implement and the resilience-related information and access it must provide. Once such agreements are in place, the failure of the vendor to honor them would constitute breach of contract.

A good agreement will say that the vendor must have a business continuity plan and that you have a right to inspect the plan, review the vendor's IT/DR tests, and conduct on-site visits. The agreement should also set forth the consequences to the vendor for any disruption of theirs that impacts your organization.

What to Include in a Vendor Agreement

Ideally, the following business continuity–related provisions should be included in the agreements you make with your critical vendors:

- Critical suppliers should be legally bound to ensure continuity of their supply chain and the delivery of services and materials to the organization.
- Agreements should contain specific wording defining BCM requirements, service-level expectations, and penalties for interruptions and incidents.
- The agreement should say that the vendor must have a business continuity plan and that your organization has a right to inspect the plan, audit the vendor's IT/DR tests, and perform on-site visits.
- The agreement should describe how the parties will communicate.

Unwilling Vendors

How willing vendors are to include business continuity language in your joint agreements can depend on how critical you are to them (rather than how critical they are to you). Some vendors might be uninterested in addressing your concerns.

It might help to explain that the provisions you are seeking will benefit the vendor as well (by improving their resilience and making them more attractive to other customers). If a critical vendor declines to address your supply chain security needs, implement one or more alternate mitigation strategies.

Implementing Mitigation Strategies

Reducing the risk in your organization's supply chain requires an overall effort made up of separate initiatives tailored for each critical vendor.

Each initiative requires looking at the threats facing a given critical vendor, their readiness, and the impact on your organization if they were to go offline. The next step is implementing one or more mitigation strategies for that vendor.

The steps for implementing mitigation strategies for a given critical vendor are as follows:

1. List the possible mitigation strategies for use with the vendor.
2. Evaluate the suitability of each strategy for this vendor.
3. Select one or more strategies that you think are feasible and likely to be effective with this vendor.
4. Document your proposed course of action for implementing the chosen strategies (with timeline).
5. Present your proposal to management, explaining your reasoning and soliciting their feedback.
6. Incorporate management's feedback and obtain their approval for the final plan.
7. Implement the approved plan.
8. Conduct regular reviews of the mitigation strategies, updating them as needed.

By following these steps, your organization can systematically manage down its supply chain risk, increasing its resiliency and protecting its ability to carry out its mission-critical operations.

Takeaways

- Multiple strategies are available to help an organization mitigate the threat posed by its critical vendors.
- Available mitigation strategies include working with the supplier to improve their BCM program, adding a new supplier, switching to a new supplier, diversifying geographically, and devising workarounds to deal with the loss of the product or service.
- Organizations should seek to include strong business continuity language in their vendor contracts and purchasing agreements.
- A good vendor agreement requires the supplier to have a solid business continuity plan and gives the organization the right inspect the plan and conduct on-site visits.
- The process for implementing vendor threat mitigation strategies is: evaluate potential strategies, select one or more strategies, draft a proposed action plan, obtain management approval, implement the approved plan, and conduct periodic reviews and updates.

CHAPTER 6: CONCLUSION

The COVID-19 pandemic led to a crisis in the global supply chain that made headlines. The problem of business's extreme vulnerability to supply chain outages preceded the current crisis and will persist after it is resolved.

Over the past several years, multiple factors have worsened the problem of supply chain insecurity, including the rise in the use of third-party providers and collaboration services and the increase in cyberattacks, extreme weather, and dependence on China.

A relatively small number of organizations have responded to the situation with prudence and energy. A larger number have done little or nothing, leaving themselves open to having their operations brought to a sudden standstill by the unexpected loss of a key resource from a third-party vendor.

Every organization should assess the risk in its supply chain and take steps to reduce it, if necessary.

Reducing supply chain risk can be accomplished by following a straightforward four-step process:

1. Establish a governance program for managing supply chain risk, including setting up an oversight team, finding a sponsor, and writing the policies and standards to govern the organization's relations with its suppliers.
2. Identify your critical vendors and determine what the impact on your organization would be if you were to lose the key products and services they provide.
3. Assess the threats to your critical vendors and their readiness to deal with them.
4. Identify the most likely and potentially impactful threats to your organization and implement strategies to mitigate them.

To increase the chances of success, those trying to rein in supply chain risk are advised to adopt the attitude of "trust but verify."

The Future of Supply Chain Security

The following are some of the main developments we anticipate seeing in the area of supply chain security over the next five years or so:

- Organizations will grow increasingly serious about assessing their suppliers' business continuity programs.
- Vendor contracts will see increased use of business continuity language.
- There will eventually be business continuity certification programs for vendors.
- There will be a strong movement toward evaluating fourth-party vendors (your suppliers' suppliers).
- Vendor assessment will grow more standardized.
- A stronger legal and contractual framework establishing requirements for vendors' continuity planning will emerge.
- More companies will hire third-party business continuity consultants to conduct assessments of their vendors' resiliency.
- Use of third-party vendor resiliency assessment tools will increase.

Takeaways

To conclude, here is a list of five takeaways covering the entire book:

- Many organizations would be unable to carry on their mission-critical activities if they suffered the loss of a vendor providing them with a critical product or service (Chapter 1).
- The first step in reducing an organization's vulnerability to a vendor outage is developing a supply chain risk management governance structure, including setting up an oversight team, finding a sponsor, and writing the policies and standards governing the organization's relationships with its suppliers (Chapter 2).
- The organization must identify its critical vendors and determine what the impact would be if each critical supplier went down (Chapter 3).
- The organization needs to assess the threats facing each of its critical vendors as well as the vendor's readiness to deal with those threats (Chapter 4).
- The organization needs to implement one or more of the available mitigation strategies to bring down the risk from each of its critical vendors, thus increasing its supply chain security and better protecting its stakeholders (Chapter 5).

The threat that supply-chain insecurity poses to organizations' ability to carry out their mission-critical activities is real and growing. However, it is within the power of every organization to reduce the risk in its supply chain. The steps to do so are well-known. All any individual organization needs to do begin securing its supply network is to make a commitment to prioritize this area and begin taking the steps.

We have enjoyed this opportunity to share our thoughts with you.

Please do not hesitate to contact us if you would like information on how consulting services from MHA Consulting and software products from BCMMETRICS can help you in assessing and improving the security of your organization's supply chain.

Michael Herrera, CEO and
Richard Long, Senior Advisory Consultant
MHA Consulting