STRATEGIC BCP®

The VRCM Professional's Playbook:

The Challenges of Managing Vendor Risk Contingency Plans

Use of third-party vendors for critical products and services is a common aspect of business. While business process outsourcing continues to flourish, organizations rely more on critical, "Tier 1" vendors for essential products and services. This reliance increases our exposure to various types of risk, including regulatory risk, reputational risk, information security risk, and financial risk.

Vendor Risk Management intersects with Business Continuity Management (BCM) and Operational Risk Management (ORM) where third-party vendors provide critical products, services, or have access to critical company information. Just as BCM encapsulates Risk Assessments, maps critical processes to people, assets, and conducts Business Impact Analyses, vendor risk management extends those concepts to third-party suppliers, partners, and contractors.

Using established risk management principles, Strategic BCP defines a practice to manage vendor risk while addressing contingency and recovery capabilities. Vendor Risk and Contingency Management (VRCM) ensures vendors are prepared with proven, demonstrable contingency and recovery plans to return to service levels you require to recover and operate your processes and critical systems.

Assessing the Impact: Measuring Vendor Risk

VRCM has gathered significant attention lately—considering that serious, newsworthy problems affecting national retailers and global consumer electronics leaders have involved third-party vendor breaches.

In this playbook, we address the following:

- ☑ Aligning vendor risk management and BCM to fill the gap with VRCM
- ☑ Effective Planning Tools
- ☑ Third-Party Hacks
- ☑ Reputation Management
- ☑ Effective Oversight

Many organizations do not understand the impact of vendor products and services on their own continuity and recovery efforts. We believe VRCM must include contingency plans to address gaps in critical products and services left by vendors. To date, many organizations manage vendor risk separately from BCM. More mature BCM program managers conduct a "Vendor Business Continuity Review" instead of a risk assessment as full assessments are not commonplace in BCM programs (and they should be). Connecting vendor products and services to your processes, products, and services while ensuring vendor assessments include contingency and recovery capabilities will demonstrate operational resiliency, address the role vendors play in mission-critical delivery, and show that appropriate contingency plans are essential.

The Grand Design: Aligning Vendor Risk Management and BCM Planning

Effectively managing risk requires a structured, integrated process that works as part of your overall BCM strategy. BCM must include provisions for your company's third-party vendors, suppliers, and contractors—many of which will no doubt be essential to your continuity of operations. The first questions you need to ask are: What access do vendors have to my own data and that of my customers? How critical are their products and services to my business continuity? Does the vendor have a mature program for information security and BCM to aid in my operational resiliency? Most importantly, what were the results of the vendor's last DR exercise? Were issues found that could impact their ability to fulfill their SLA to our critical processes, products, and services? If so, how are they remediating those issues?

When assessing risk, information security almost always comes to the forefront in most organizations. Take—for example—an IT service organization that relies on an external vendor for hosting or cloud services. They will always need a host that is available and online for critical applications. In this example, the cloud vendor would certainly take precedence as a critical or Tier 1 vendor for contingency planning and recovery. Depending on your circumstances, vendors will fall into tiers that indicate the criticality of their products and services and—most importantly—the part they play in your operational resiliency program.

Understanding the impact a vendor has on your ability to recover is essential. Using a point rating system ensures you have a clear metric by which to measure vendor relevance. For example, a point rating based upon the BIA that the business units have completed would reflect vendor products and services that are critical to recovery and enable the organization to rank vendors specific to the recovery of a process or asset. The rating should not be arbitrary. It should be formulaic, based on the link to the business function in question, the RTO, and critical component inventories.

In heavily regulated business segments such as healthcare, pharmaceuticals, banking, and financial services, your vendor risk program will be subject to regulatory requirements. For example, asset-management and wealth-management organizations are subject to unique oversight and sensitivities involving privacy, data storage, personnel, and due diligence. If your organization does business outside the U.S., you may be subject to country-specific legal and data privacy regulations. Other specialized industries carry similar demands. For example: In October 2013, the Office of the Comptroller of the Currency (OCC) issued a risk management guidance bulletin applicable to national banks and federal savings associations on Third-Party Relationships. It requires that entities "assess the third party's ability to respond to service disruptions or degradations resulting from natural disasters, human error, or intentional physical or cyber attacks." In addition, regulatory requirements can extend beyond you to your vendors and—in some cases—the "vendors' vendors," often called "fourth parties."

Game-plan checklist:

- ☑ Determine how vendor products and services align to company processes, products, and services and identify which are critical to your operations.
- ☑ Determine how risk exposure affects processes, products, services, and reputation.
- ☑ Determine the information security implications of working with vendors, and measure the effectiveness of their internal security policies.
- ☑ Develop, test, and maintain contingency/recovery plans and run books that address critical vendors.

Effective VRCM Planning: Finding the Right Tools

Effective VRCM need tools that will manage and identify vendor products and services aligned to your operations, align vendors to potential business impact, identify critical products and services, and document alternate vendor sources. The last area is particularly important. There may be only one vendor making a product important to your operation—but what if that vendor is unable to operate due to an incident? If a critical supplier—for example—was unable to deliver a key part required by your manufacturing process for four weeks instead of within an SLA of four days, what would be the financial and operational impact to your business? Has the vendor exercised this scenario, and what was the outcome? Are there alternative vendors that can provide the same product or service, or perhaps you can mitigate this risk by carrying a longer parts inventory? These questions are essential to planning and recovery.

Often, smaller organizations with few critical vendors perform assessments manually through SharePoint, spreadsheets, or e-mailed surveys. These tools require significant manual manipulation and data movement as non-integrated tools rely on human intervention to be useful. Detailed instruments such as the Standardized Information Gathering (SIG) questionnaire from *The Shared Assessments Program* can definitely help by providing a standard set of questions for vendor risk assessments. Developing the proper assessment mechanism such as collecting, weighting, and scoring results, identifying issues, and taking action will only be as effective as the tools and process you employ.

Without automation, however, planning efforts can become challenging when it is time to identify, document, and remediate issues. While many BCM tools enable a company to identify vendors and associate them with business functions, they lack the ability to measure vendor risk. Strategic BCP's ResilienceONE software addresses this important gap by measuring risk via a numerical score representing the criticality of the specific vendor product or service to the business process. This scoring is essential to the important step of prioritizing your vendor product and services based on criticality; the priority facilitates an immediate understanding of just how critical a vendor's products or services are to recovery.

In some firms, the BCM team operates in a silo detached from the vendor risk management team—even though they are required to identify vendors as part of their contingency planning. How can they best do this without replicating the work of the vendor risk management team?

Game-plan checklist:

- ☑ Identify how many critical or "tier-one" vendors your organization currently uses.
- ☑ Identify your most-critical vendors and align them to potential business impact.
- ☑ Identify potential alternate providers should any of your critical vendors go down.
- ☑ Determine capabilities, requirements, and limitations of current planning and recovery tools and seek software solutions that integrate vendor risk management with contingency planning and recovery.
- ☑ Incorporate scenarios for BC/DR exercises that include tier-one vendors.
- ☑ Participate in Tier 1 vendor BC/DR exercises annually, and actively assist in their improvement.

Third-Party Hacks Mean First-Person Problems

In December 2013 during the height of the holiday shopping season, Target Corporation suffered one of the largest and most widely reported data breaches in United States history. The attack compromised the personal information—including names, phone numbers, addresses, and e-mail contacts—of approximately 110 million in-store and online Target customers. The immediate financial cost was high as Target paid $10 million to affected consumers, $39 million to affected banks and credit unions, and an undisclosed amount in class-action attorney fees. The reputational impact was far greater than the financial impact. Sales plummeted as customers went to competitors.

When additional details emerged, we learned that hackers had accessed not only customer contact information, but also payment card numbers and encrypted PINs. Cybersecurity analysts focused on a single point of attack—Target's Point-of-Sale (POS) payment system. While the payment industry has set retailer standards intended to keep customer data secure, those standards mean very little once a hacker accesses the overall corporate system itself.

First, one of Target's HVAC contractors fell victim to a malware phishing attack using a trojan virus that captures keystrokes, takes screenshots, and copies login credentials. Using the contractor's credentials, hackers were then able to access Target's contractor, partner, and property-development portals. It seems that hackers then attacked the retailer's internal systems. At this point, analysts believe that the hackers compromised a Windows server, located the POS system, and installed a trojan virus that gathered and transmitted the stolen customer payment data.

The initial financial impact was significant: Q4 net profit fell over 46% and Q4 expenses shot up $61 million due to the breach.

Unfortunately, the entire incident began with a third-party vendor's reliance on a free anti-malware solution that did not offer real-time protection. Better-quality, professional-grade solutions could have identified and blocked the type of trojan virus hackers used and, with effective vendor risk assessments, Target may have identified this weakness at the contractor. This is a best practice mandated by prescriptive compliance contracts. Target could have required endpoint protection and regular audits of contractors and partners to keep enterprise resources secure.

Game-plan checklist:

- ☑ Clearly understand the systems each of your vendors can access through rigorous vendor risk assessment surveys and checklists, cross-checked to the internal "consumers" using the vendor's products and services.
- ☑ Determine what information security protections your vendors have in place.
- ☑ Conduct audits or reviews of data and information security tools and policies with vendors.
- ☑ Review incident detection, response, and escalation with each of your critical vendors.

Reputation Management: The "Wild Card" of Risk

The harm caused by damage to an organization's reputation can carry just as much weight as damage to systems, facilities, or processes. In fact, it may ultimately be harder to recover from this damage than from others, as it can have a larger financial impact from reduced revenue and falling stock value. Just a few short years ago, Apple found themselves thrust to the forefront of the discussion on reputation management—and learned first-hand how vital vendor risk really is.

In 2010, more than 10 employees at Foxconn—a Chinese company that assembles products for Apple and others—committed suicide. In response to the number of deaths—more than any other year—Foxconn promised to lower work hours and provide greater oversight. In early 2012, reports from both Huffington Post and Bloomberg noted "serious and pressing" violations of Chinese labor laws as reporters spotted a number of children between the ages of 12 and 14 entering the Foxconn factory that assembled Apple's iPhones. Later that same year, explosions destroyed two Foxconn factories and killed several workers.

According to labor-rights groups, employees who assembled Apple devices worked too quickly, labored under inconsistent health and safety policies, and found themselves exposed to dangerous chemicals. In response to this criticism, Apple joined the Washington-based Fair Labor Association (FLA) to address the workers' rights controversies that long-plagued their alliance with Foxconn. At the time, inspectors noted more than 50 violations of labor laws—including breaches of the FLA code of conduct. This troubled relationship shows the critical role that oversight of vendor practices play in reputation management.

Game-plan checklist:

- ☑ Identify the potential risk of vendor practices to your organization's reputation.
- ☑ Perform thorough due diligence on vendor labor, safety, and management practices and incorporate regulatory violations in your BC/DR planning.
- ☑ Make sure your vendors' labor, safety, and management practices align with your own.
- ☑ Maintain communication with vendors on regulatory and oversight requirements and conduct frequent, consistent assessments for Tier 1 vendors.

Oversight: The Key to Effective Governance

Ultimately, effective vendor risk and contingency management requires that you hold all of your third-party suppliers to the same high standards of accountability that you have established within your own organization. That is the only way to close the window of vulnerability and prevent dangerous—potentially catastrophic—scenarios that can cripple your business.

As Brad Keller—Senior VP of the Santa Fe Group—observes: "If a third party doesn't have the same controls in place or the level of controls you need from a risk management standpoint, you have a serious risk to address."

Game-plan checklist:

- ☑ Identify laws, regulations, frameworks, and standards that apply to your organization.
- ☑ Make sure vendors comply with the same laws, regulations, frameworks, and standards and seek evidence of their compliance.
- ☑ Recognize that both business continuity and risk management must work together to provide truly effective contingency and recovery planning.

Conclusion: "Not My Problem" is a Dangerously Obsolete Notion

Considering the potential harm to systems, processes, operations, and reputation that can affect your organization through a vendor, it becomes obvious that most organizations need to do much more than they are doing now. Keller summarized the issue succinctly: "If you're outsourcing to or relying on a third party, you can't just shut the door and say it's someone else's problem. You can outsource the function but you ultimately own the risk."

ABOUT THE AUTHOR

Terence Lee

Terence Lee is the Vice President of Governance, Risk & Compliance (GRC) Strategy for Strategic BCP. He has over 25 years of expertise in IT Risk, Compliance, Policy, and Audit Management; Threat and Vulnerability Management; Business Continuity Planning and Management; Third Party Management; VRM; and Operational Risk Management.