



HOW UTILITIES CAN MANAGE SUPPLIER RISK

by Robert Tevelson, Mike Lewis, Joao Maciel, and Steve Spencer

TO KEEP PACE WITH the rising demands of operating in an increasingly complex business environment, utilities are turning to external suppliers as never before. They're looking for help with tasks ranging from the relatively mundane (such as vegetation management and the handling of customer calls) to the complex (including the facilitation of distributed power generation and the execution of large infrastructure projects). While the benefits of leveraging supplier capabilities are clear, the risks—including cyber, reputational, financial, legal, and regulatory ones—generated for utilities are potentially vast. The practice can also unwittingly thrust utilities into the headlines, as illustrated by the recent, rather unflattering press coverage of a number of high-profile incidents in which utilities' suppliers played a prominent role.

Fortunately, the risks associated with the use of suppliers can, in fact, be identified and mitigated. (See Exhibit 1.) But that requires taking a comprehensive, well-constructed approach—one that few utili-

ties, in our observation, currently employ. Reasons vary for the absence of such an approach to supplier risk management among many utilities, including the complexities of program design and difficulties securing organizational buy-in for the needed investment.

But BCG has created an effective approach that can substantially reduce your chances of being blindsided by a major supplier-related event and enhance the strength and quality of your organization's response if an incident does occur. It is tested, can be melded into your day-to-day operations relatively quickly, and can translate into tangible results almost immediately. What's more, implementing it can produce broad benefits—including a more risk-cognizant culture and simplified, more automated procurement and supplier-management processes—within your organization.

Suppliers and Risk

The business and operating backdrop for

EXHIBIT 1 | How Well Is Your Company Managing Risk?



What are your company's highest-risk contracts with vendors?



What controls and mitigation measures does your organization have in place to manage the risks associated with those contracts?



Who are the point persons responsible for managing the associated contract risk and vendor performance of each high-risk contract?



What is your organization's process for identifying and managing the risks of **new** contracts that might pose high risk?

Source: BCG analysis.

utilities is becoming ever more complex. Utilities are expected to execute their day-to-day functions flawlessly, 24-7, amid tightening regulatory and safety standards and a general rise in customer expectations—all while keeping costs in check.

Simultaneously, utilities are expected to plan, manage, and execute major capital projects; adroitly navigate a rapidly evolving technological environment replete with smart meters, renewable energy sources, and other potentially game-changing developments; and keep investors and regulators happy. In addition, utilities must keep all of these balls aloft under close scrutiny, where the slightest miscue can be surfaced quickly and broadcast far and wide through social media.

Given this sweeping range of demands—and the associated breadth of expertise, skills, and work capacity necessary to meet them—it is hardly surprising that utilities are turning to suppliers more and more. Indeed, for many utilities, contracted labor now accounts for more than half of their total labor hours and for spending that is equivalent to as much as half of the utility's revenues: many large utilities now spend multiple billions of dollars each year on suppliers.

This growing reliance on outside parties amplifies the traditional risks that utilities face, such as the following:

- **Cyber.** The supplier's security protocols might be more lax than the utility's, unduly exposing the utility's systems and customer data to hackers. (See the sidebar "Supplier-Driven Cyber Risk: A Growing Threat That Could Be Very Costly.")
- **Operational.** The supplier fails to follow established health and safety standards, resulting in injury or death.
- **Reputational.** The utility is held implicitly accountable by the media and public for errors committed by its suppliers.

Greater utilization of suppliers introduces new types of risk to utilities as well. Among these are the following:

- **Fourth Party.** The supplier engages subcontractors that the utility has not vetted.
- **Contractual.** The utility is prevented by contract restrictions from effectively monitoring the supplier's work.

SUPPLIER-DRIVEN CYBER RISK: A GROWING THREAT THAT COULD BE VERY COSTLY

By the very nature of their operations, utilities are common targets of cyber attacks and highly vulnerable to the effects of a successful incursion. Many utilities have beefed up their defenses against direct attacks through stronger firewall protection. But a utility's ties with its suppliers can often pose vulnerabilities. Phishing e-mails to customers (in cases where billing or another function is handled by a supplier), a "watering hole" attack (in which a supplier used by multiple utilities is targeted and infected with malware), and the like are relatively simple for a committed attacker to launch. But they can have painful consequences for a utility when successful, whether it be the exposure of customers' financial data or,

in the worst scenario, access to the utility's operational controls.

Whether a breach primarily affects a utility's operations-related systems (such as those that monitor or govern devices, industrial controls, or processes) or information-based ones (including those related to the utility's internal systems, communications, and customer and employee data), the cost and logistical demands of halting and undoing the damage and making good with stakeholders can be vast. And both the number and creativity of attacks seem likely to rise, spurred by the widening web of potential vulnerabilities associated with utilities' growing use of suppliers.

- **Concentration.** The utility becomes too dependent on a single contractor and either loses internal expertise and negotiating leverage or sees upward price pressure or deteriorating performance.
- **Financial Distress.** The contractor experiences severe financial difficulties and is unable to deliver the contracted services.

What's more, the logistics of utilities' business—including the need for 24-7 operations and accessibility for customers—make it difficult for utilities to reduce these risks through tighter supplier management. Utilities' domains often span hundreds of miles, which makes the tracking of suppliers problematic.

A utility's service area can also fall under the jurisdiction of multiple regulatory bodies, resulting in varying requirements for suppliers depending on location and exacerbating the challenge of monitoring and control. Contractor-reliant plants or facilities that need to operate around the clock (or at odd hours) pose similar practical hur-

dles, as does the sheer number (often hundreds) of contractors a utility may need to employ. The bottom line is that, even with the best of intentions, a utility can find it quite hard, if not impossible, to keep a sufficiently close watch and tight rein on its suppliers.

A Rigorous Approach to Supplier Risk Management

Some utilities have instituted formal programs to try to contain supplier risk, but we have noticed that many of these efforts fall short on at least one level. Some have an incomplete focus, concentrating on only a few specific kinds of risk or parts of the business. Others are backward looking, measuring only suppliers' past performance or lagging indicators and offering no visibility into the likelihood of future problems. Still others fail to formally track supplier compliance with utilities' or regulators' guidelines or are siloed when a business unit fails to share information about a poorly performing supplier with others. And then there are those that misalign the probability or potential consequences of a given risk with their efforts to mitigate it.

An effective supplier risk management program, in contrast, will have six attributes. (See Exhibit 2.) It will:

- Be comprehensive, addressing all types of risk
- Forge a consistent interpretation of risk, establishing clear criteria so that the potential for varying individual assessments is eliminated
- Emphasize proactivity, focusing on the definition of preemptive measures that can prevent potential risks from being actualized
- Be pragmatic, accommodating and adjusting to changes in risk probabilities and causal factors, as well as user-centric in design and functionality (placing heavy emphasis on dashboards and other visual elements), especially from a contract manager’s perspective

- Establish accountability, incorporating compliance verification measures to ensure that the risk management process is being adhered to and applied consistently
- Be adaptive, applying an agile methodology and enabling continuous learning and adjustments to the process

BCG’s approach to supplier risk management has all of these attributes. It is based on gaining a thorough understanding of each supplier and its particular mandate with a utility, and it’s grounded in a four-step process: identify, quantify, mitigate, and monitor. (See Exhibit 3.)

The process ensures that all relevant risks are surfaced; that risks are graded according to severity so that management knows where to concentrate its time, energy, and resources; that steps to mitigate risks are identified and shared with the appropriate

EXHIBIT 2 | The Right Approach to Managing Supplier Risk

CHARACTERISTICS OF AN EFFECTIVE PROGRAM



Source: BCG analysis.

EXHIBIT 3 | BCG Tools Underpin the Process to Identify, Quantify, Mitigate, and Monitor

BCG's Approach Ensures That All Risks Are Identified and That the Severity of the Risks Is Quantified Consistently

BCG

Does vendor create, transmit, store, or access non-public data as defined by the Information Protection Policy (e.g. photographs of facilities, engineering drawings, business plans, customer data)?

Does vendor have physical exposure to the Bulk Electric System (BES) or CIP assets?

Is vendor providing IT services (e.g. data center hosting, telecommunications, application development, etc) or electronic hardware (e.g. controllers; transformers; servers, etc)?

BACK **NEXT**

A short survey helps employees identify potential supplier risks

BCG

How many customer records can the vendor create, transmit, store, or access?

Select all information that vendor would have access to in addition to customer information:

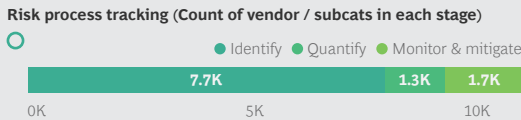
	Yes	No
Business plans	<input type="radio"/>	<input type="radio"/>
Trade secrets	<input type="radio"/>	<input type="radio"/>
Market forecasts	<input type="radio"/>	<input type="radio"/>
Employee personal information (non-sensitive)	<input type="radio"/>	<input type="radio"/>

Is vendor providing IT hardware or physical copies of software?

Yes
 No

If a risk is present, more detailed questions help quantify its severity and ensure consistency of assessments

BCG's Process Ensures That Appropriate Risk-Mitigation Measures Are in Place



Risk backup

Risk	Supplier	Mitigated (H)	Mitigated (M)	Mitigated (L)
Business Continuity	Vendor A	13	12	11
Business Continuity	Vendor B	12	13	11
Business Continuity	Vendor C	17	15	7
Business Continuity	Vendor D	10	8	6
Business Continuity	Vendor E	10	7	15
Total		916	899	830

Dashboards give visibility to supplier screening and risk-mitigation measures

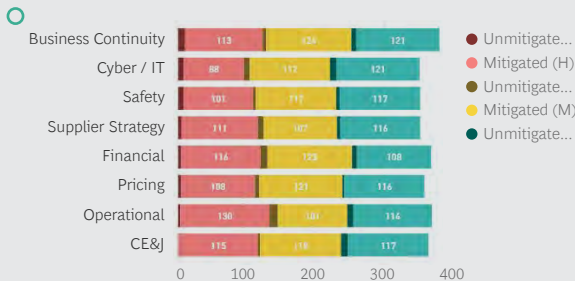
Thresholds and mitigation measures are customizable to fit your company's needs

Proactive / reactive	Process stage	Category	Risk type	Low	Medium	High
Proactive	Strategize	Verification of vendor claims	Reputation	Require supplier to submit documentation for all agreed upon credential	Require supplier to submit documentation for all agreed upon credential	Require supplier to submit documentation for all agreed upon credential
Proactive	Strategize	Verification of vendor claims	Compliance	Require supplier to submit documentation for all agreed upon	Require supplier to submit documentation for all agreed upon	Require supplier to submit documentation for all agreed upon
Proactive	Strategize	Verification of vendor claims	Operational	Require supplier to submit documentation for all	Perform internal review of supplier documentation, ask	Perform an audit of relevant supplier information (e.g.
Proactive	Strategize	Verification of vendor claims	Political	Perform internal review of supplier documentation and credentials (e.g.	Perform internal review of supplier documentation and credentials (e.g.	Perform internal review of supplier documentation and credentials (e.g.

BCG builds the process to your standards and designs it so that your company can adjust it as necessary going forward

BCG's Dashboards and Recommended Actions Enable Easy Monitoring and Effective Management of Risks

Risk distribution (Mitigated v. Unmitigated)



Risk escalator for executive attention

Vendor (Risk)	Metric exceeding threshold	Action taken?	Need next step
Vendor B (Risk)	Metric 2	No	Submit docume...
Vendor C (Risk)	Metric 3	Yes	Perform review...
Vendor D (Risk)	Metric 4	Yes	Perform review...
Vendor E (Risk)	Metric 5	Yes	Submit docume...
Vendor F (Risk)	Metric 6	Yes	Perform review...

Dashboards highlight risk ratings, recommended actions, and indicators that need to be monitored

Select risk metrics (only those with significant change)

Risk	Relevant contracts?	Metrics tracked	Value	Implied next step
Safety	All	Number of bystander complaints associated with vendor's safety performance	↑ 5	Work with project manager to modify mitigation
		Vendor team's average tenure	↓ 10yrs	Work with project to ensure appropriate training / oversight

Management is notified of a change in status of a risk indicator, enabling and triggering preemptive action

Source: BCG.





people at both the utility and the supplier; and that the risks are sufficiently monitored at the management level by both the utility and the supplier. No stone is left unturned, no base is left uncovered. Simultaneously, the program accomplishes its goals without either interfering with the company's ability to run its core business or demanding too much time from people.

Implementing such a program requires a multipronged approach. Leaders must commit to the program and make their commitment visible on an enterprise-wide basis: if leadership doesn't lead, then the business and functional units are unlikely to follow. The business and functional units, in turn, must work in close collaboration with the supply chain and procurement functions. The enabling technology that underpins the dashboards and other visual elements necessary to make the program operate at scale must be designed, launched, and supported by training. A change management campaign, designed to get broad buy-in across the organization for the new approach to risk mitigation, must be undertaken. And the program's phase-in must be user-centric, with particular attention paid to the needs of contract managers.

Admittedly, successful implementation isn't easy. But the potential rewards for getting it right are sizable. Most visibly, the number of negative supplier-related incidents can be greatly reduced. This can spare the utility potentially large regulatory fines and costs associated with undoing or compensating for any damage caused by suppliers. (See Exhibit 4.) It can also strengthen the utility's relationship with regulators and improve internal morale. In addition, time and resources that would have been devoted to managing supplier-driven crises can be dedicated to more productive activities. And the demonstration of control over supplier risk can foster broad cultural benefits across the organization, including a generally elevated focus on risk and risk mitigation.

Conversely, the downside of unsuccessfully implementing the program, or deciding to refrain from even trying to tackle supplier risk in a concerted manner, can be enormous. The number of negative supplier-related incidents could climb, leading to escalating fines and costs. The degree of regulator scrutiny could rise and remain elevated for an extended period. The utility's reputation could suffer; customer attrition could surge.

EXHIBIT 4 | Supplier-Related Risks Can Have Devastating Effects for Utilities

EVENT	IMPACT ON UTILITY
 <p>After substantial execution delays and cost overruns, a critical vendor falls into financial distress</p>	<p>Project cancellation after more than \$1 billion in sunk costs</p>
 <p>Vendor fails to ensure sufficient cybersecurity, exposing customers' personal and financial data</p>	<p>Data compromised for up to 2 million customers</p>
 <p>Vendor fails to properly train workers conducting infrastructure inspection</p>	<p>Millions of dollars in regulatory fines</p>
 <p>Subcontractor fails to ensure sufficient level of onsite safety, resulting in a worker's death</p>	<p>Millions of dollars in regulatory fines</p>

Source: BCG analysis.

In short, we think that, for most utilities, this is worth doing and doing well. We can help.

Why BCG?

BCG brings a wealth of relevant experience and capabilities to the table. We have worked with major energy companies, including a large utility, on managing third-party risk and have extensive risk management experience across industries. (BCG has worked with more than 50 companies on projects related to third-party risk in the past two years and has more than 20 risk experts in North America alone.)

We have substantial general experience with utilities, having worked on more than 1,800 projects in the past five years. We have a seasoned team of more than 300 experts devoted specifically to the power and utilities space as well as a depth of experience across the entire energy value chain. We have developed market-leading propri-

etary databases, benchmarks, and market models.

We can work quickly, efficiently, iteratively, and in close collaboration with you, using agile tools and methodologies and employing a “training by doing” approach with your teams. We can move rapidly from assessing your current risk management approach to designing a more optimized custom program, if necessary—one that is truly individualized and specific to your needs. We can guide and assist in all aspects of implementation, from launching pilots with a subset of suppliers to facilitating cultural change so that the program becomes part of your organization’s DNA. Throughout the process, we will challenge you and expect you to challenge us; together, we will arrive at a solution that meets your specific needs.

If you are interested in learning more about our approach to managing supplier risk and what we think BCG could do for you, we would love to hear from you.

About the Authors

Robert Tevelson is a managing director and senior partner in the Philadelphia office of Boston Consulting Group. You may contact him by email at tevelson.robert@bcg.com.

Mike Lewis is a managing director and partner in the firm’s Houston office. You may contact him by email at lewis.mike@bcg.com.

Joao Maciel is a managing director and partner in BCG’s Houston office. You may contact him by email at maciel.joao@bcg.com.

Steve Spencer is a principal in the firm’s Houston office. You may contact him by email at spencer.steve@bcg.com.

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we help clients with total transformation—inspiring complex change, enabling organizations to grow, building competitive advantage, and driving bottom-line impact.

To succeed, organizations must blend digital and human capabilities. Our diverse, global teams bring deep industry and functional expertise and a range of perspectives to spark change. BCG delivers solutions through leading-edge management consulting along with technology and design, corporate and digital ventures—and business purpose. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, generating results that allow our clients to thrive.

© Boston Consulting Group 2019. All rights reserved. 8/19

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting Group on Facebook and Twitter.