FEBRUARY 2017

RISK

From scenario planning to stress testing: The next step for energy companies

Utilities and oil and gas firms have long used scenario analysis, but extraordinary times call for new measures.

Sven Heiligtag, Susanne Maurenbrecher, and Niklas Niemann

Strategic and financial scenario analysis has a long, venerable history at energy companies. Shell Oil popularized the technique in the 1970s, and almost all of them have adopted it as a vital part of their decision-making processes. But as executives know well, scenario planning has its pitfalls; 40 percent of the leaders we surveyed in 2013 said that it didn't meet their expectations. Often, companies fall prey to one of several tendencies, such as availability or stability bias, that hinder the exercise and produce unusable results.

Energy companies are finding that in today's volatile world, one flaw of scenario planning is particularly acute: when business leaders consider a range of scenarios, they tend to "chop the tails off the distribution" and zero in on those that most resemble their current experience. Extreme scenarios are deemed a waste of time because "they won't happen" or, if they do, "all bets are off." But this approach leaves companies dangerously exposed to dramatic changes.

Consider the shocks and disruptions of recent years. The 2010 Deepwater Horizon disaster had far-reaching effects on the oil companies involved, and many others. The 2011 Fukushima earthquake and tsunami upended nuclear policy in Japan and elsewhere, changing the industry's structure. Geopolitical shocks have upset the plans of energy companies in too many countries to name. Most recently, the rise of antiglobalization sentiment has thrown a new wrench into energy planning.

It's hard to overstate the consequences of events like these. Take the German experience of *Energiewende*, the nation's transition to sustainable energy. To predict the effects on electricity prices, most energy companies relied on the classic scenarios—a base case, with best and worst cases that skewed slightly to either side. However, the Fukushima disaster vastly accelerated the switch to renewables. The price of power tanked by more than 50 percent—far worse than the gloomiest projections (Exhibit 1). The effect has been devastating: power producers had to write off tens of billions of euros.

Enter stress testing

At most companies, scenario analysis looks for the likely development of core risk factors over time. That approach can work well in an era of gradual change. But at times like the present, it is extreme risks, not the everyday ones, that should most concern energy companies. Likewise, it is the prospect of chaotic overnight change, not gradual shifts, that should keep energy executives awake at night.

Enter stress testing, a form of scenario planning focused on the tails of the distribution. Scenario planning and stress testing are methodologically identical; they differ only in the likelihood of the scenarios they consider. Stress testing therefore requires a shift in mind-sets. In today's environment, the sum of low-probability events quickly adds up to a high probability that one of them will actually happen. The banking industry offers an example: the financial system has become so volatile, and subject to so many unexpected disruptions, that regulators now require banks to conduct comprehensive stress tests.

Let's be clear: stress testing will not prevent stress. Nor can it identify, with total confidence, precisely which stressful scenarios might play out in the future—especially those that feature "unknown unknowns." But it can help senior executives to consider some previously overlooked sources of stress, the potential magnitude of their impact, and the adequacy of the company's risk-bearing capacity to absorb them. Stress testing should be only one element of a risk-management system, but done well, it can be a tool to build the resilience that today's environment requires.

What 'extreme' means

Companies need to be bold as they imagine extreme scenarios; almost nothing is too strange or ridiculous to consider. To show the range of ideas that energy firms might contemplate, we offer five extreme scenarios covering several kinds of risk, from compliance and legal risk to business-model disruption to full-bore crisis.

Energy for free

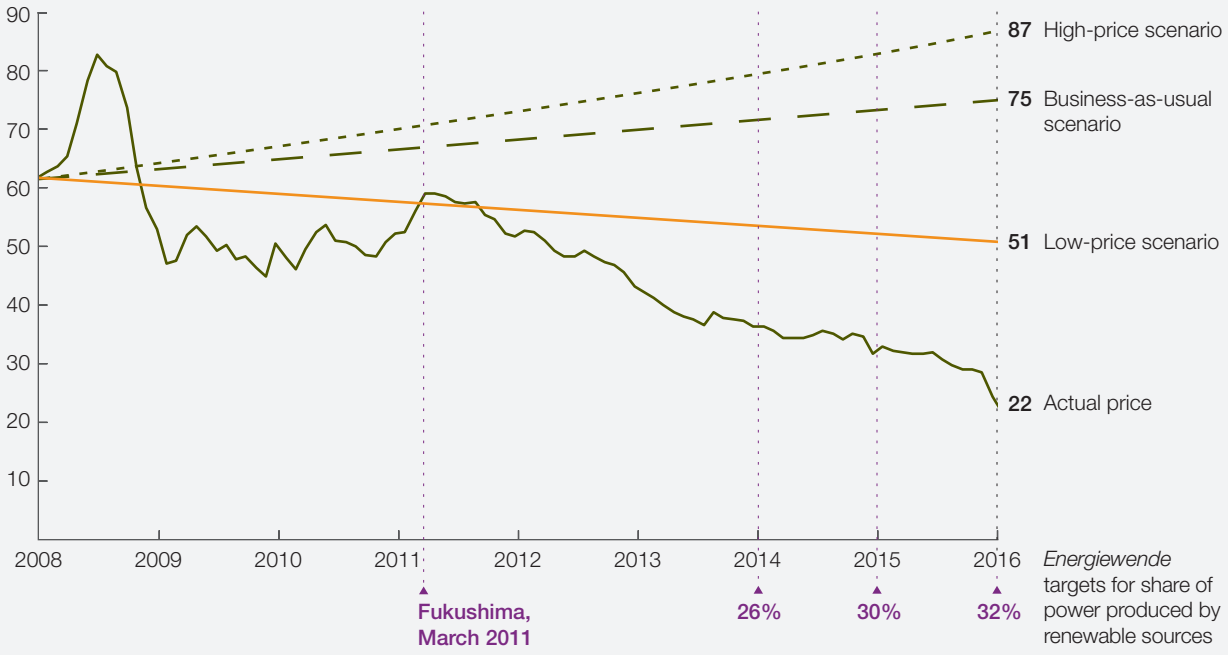
Real-time energy-consumption data are increasingly seen as crucial for a knowledge of customers and their behavior patterns. Smart meters can identify the appliances in operation. Combining data sets on electricity use, heating use, and mobility could provide even more detailed insights. Data-driven companies such as Amazon might challenge incumbent utilities by offering "energy for free" in exchange for personal data. In this scenario, utilities lose the customer relationship and are reduced to mere suppliers of commoditized power. Given the negotiating power, agility, and customer-centricity of digital giants, margins erode significantly.

A decentralized energy landscape

New entrants focus on serving customers in a completely decentralized energy regime, bundling solar photovoltaic rooftop systems with power-to-heat technologies, powerful batteries, and electric cars. An integrated solution and a strong, emotionally compelling brand (such as Tesla's) help these attackers to reduce residual demand for grid-based power substantially and to capture the customer relationship. As in the first scenario,

Exhibit 1 **German power prices far underperformed even the low-price scenario.**

German wholesale power prices, 2008–15, €/MWh



Source: BBC; European Energy Exchange; Umweltbundesamt; McKinsey analysis

utilities are reduced to suppliers of commodity power, infrastructure operators, and backup providers. Volumes and margins shrink quickly in the wholesale and retail businesses, and generation assets lose value rapidly.

An emissions fraud

A data leak reveals that a power company has manipulated processes affecting human health—say, flue-gas purification at a coal plant or the handling and disposal of waste—and has thus emitted substantially more pollution than allowed. Subsequent investigation shows that the manipulation was deeply anchored within the organization: top leaders knew that analyses and impact assessments had intentionally been skewed. As a result, all energy companies suffer a loss of public and political trust. They are then subjected to intense scrutiny of their assets and processes, and this leads to increased regulation, massive penalties, and personal liability in the form of substantial fines and imprisonment.

A cyberattack on critical infrastructure

Popular movies have frequently exploited the idea that the infrastructure of modern life is vulnerable to well-staged cyberattacks. But the real-world Stuxnet virus succeeded better than anything out

of Hollywood in proving that power plants and other nuclear assets can indeed be sabotaged. A cyberattack that takes critical infrastructure offline is more probable than ever now that power and gas grids, street lighting, and traffic control are more and more connected; the Internet of Things is beginning to reach into every home and building; and autonomous, connected vehicles are set to emerge over the next few years. In such a scenario, terrorists hack into the distribution network and shut down national power systems or even make key assets malfunction or self-destruct. Public trust would disappear, and energy companies would be subject to enormous pressure from regulators. Those deemed vulnerable to further attacks might even lose their operating licenses.

Radical price transparency

Price-comparison websites, such as Verivox in Germany, have established a strong position in several European countries. They greatly increase price transparency in retail markets for power, gas, mobile telecommunications, banking, auto rentals, and broadband, so retail customers change suppliers more frequently. In a transparency scenario, price-comparison portals help customers to change their electricity and gas providers regularly—for example, by acting as energy agents or through an automated process that selects the cheapest offer at the end of a contract. Verivox recently announced the first steps in such a process.

With such rapid churn, utilities may lose many customers—even some who have never indicated any desire to change their suppliers. Once again, companies might be reduced to providers of commoditized electricity. Retail margins would wilt in the face of the negotiating power, agility, and customer-centricity of energy agents.

Assess the stress

To understand the potential impact of these five extreme scenarios, we modeled their effects on the profits and losses, balance sheet, and cash flow of a hypothetical utility for each of several business segments: generation, renewables, trading, distribution, and retail. After modeling the effects of a scenario separately for each business, we combined them to show the effect on the enterprise. To be clear on the overall effects, you must understand, in detail, that the scenarios have specific impacts on different business units.

Exhibit 2 offers a heat map of these effects, highlighting the areas of greatest impact. For example, it shows that the energy-for-free and decentralized-energy-landscape scenarios would of course have a direct and massive impact on revenues, leading to a substantial loss of equity and an increase in net debt. On the other hand, an emissions fraud or cyberattack would have almost no relevance for revenues—but equity would suffer substantially.

This exhibit also highlights the key drivers of these effects: for example, in the energy-for-free scenario, B2C volumes and market share would decline sharply, and retail prices would fall by 5 percent. In an emissions-fraud scenario, operating and maintenance costs would soar by 50 percent, and utilities would pay regulatory penalties of up to 5 percent of revenues. If a cyberattack should take down a national grid, affected utilities would have to write off 5 percent of their physical assets; to replace them, they would boost their budgets for property, plant, and equipment by 7.5 percent. Earnings would crash, though the effect would be milder after taxes and depreciation.

The financial implications would be considerable across the scenarios, though none would necessarily bankrupt a company. Significant profit and liquidity risks appear, especially in the generation and retail businesses. In the absence of successful countermeasures, all five scenarios lead to negative recurring earnings before interest and taxes, revealing major risks for the sustainability

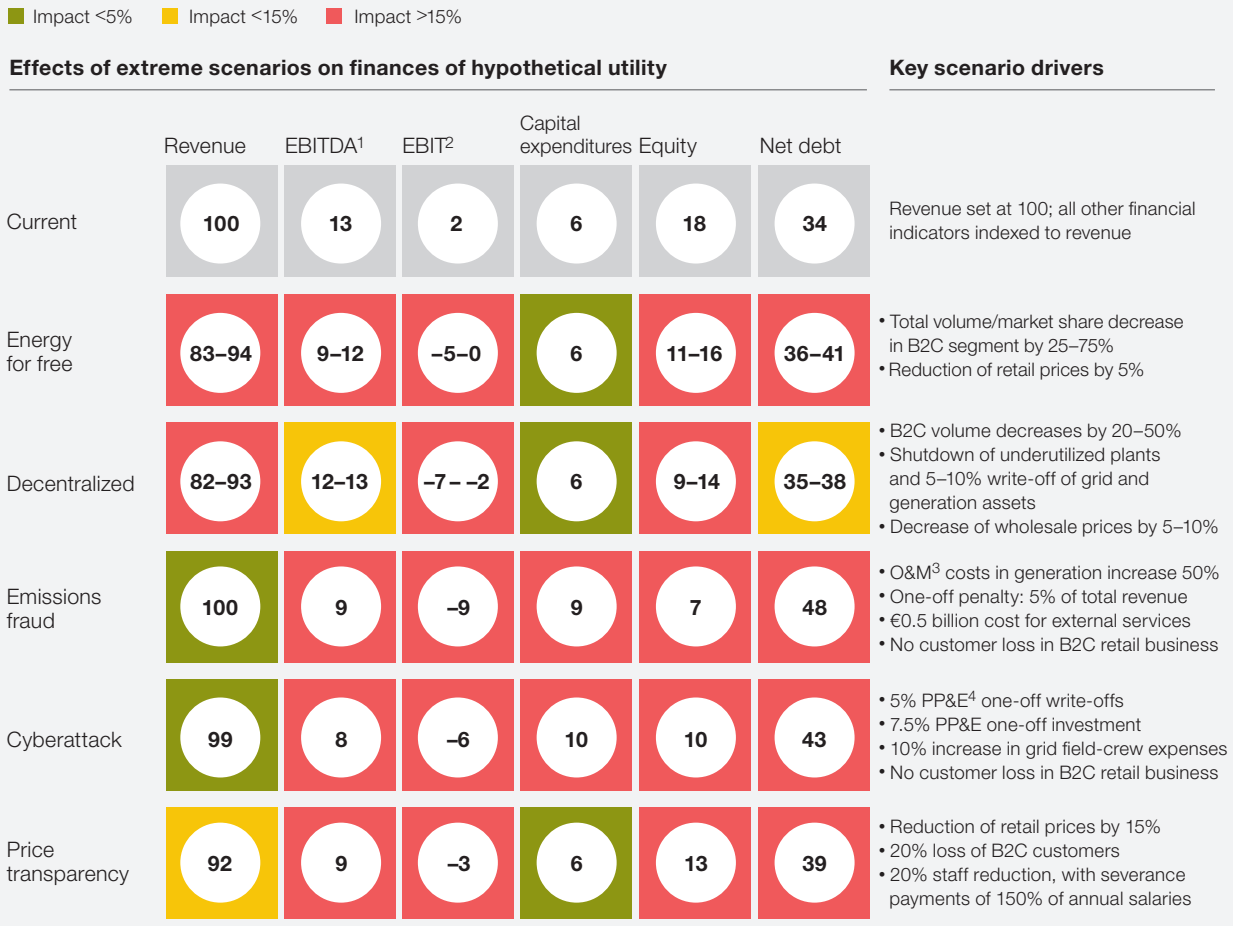
of the current business portfolio. Furthermore, the scenarios suggest a 10 to 60 percent drop in equity and a 5 to 40 percent increase in net debt—which might trigger liquidity concerns.

Get ready to improve resilience

Of course, utilities can forestall or mitigate many of the effects of stress. Hedging and insurance offer some protection. Establishing a crisis-response team is a no-regrets move for most companies.

Better preparation, such as stronger analytics and more transparent reporting, can help identify problems such as legal fraud or cyber vulnerabilities and help companies negotiate with regulators. The German government, for example, asked utilities to stress test their balance sheets and cash flows for a planned change in the disposal and storage of nuclear waste. As a result of the tests, the government took responsibility for these activities.

Exhibit 2 **Stress tests show the material impact of a scenario.**



[1]Earnings before interest, taxes, depreciation, and amortization.
[2]Earnings before interest and taxes.
[3]Operations and maintenance.
[4]Plant, power, and equipment.

Source: McKinsey analysis

A cyberattack taking critical infrastructure offline is now more probable, as power and gas grids, street lighting, and traffic control are highly connected.

Energy companies should also monitor external developments closely. Today, many utilities are watching the development of battery costs, since if they fall sharply, as they have in solar photovoltaics, generation and retail businesses would be vulnerable. Some utilities are partnering with or investing in battery companies. Many long-term strategic options are available, including nimble resource allocation and the transformation of companies into digital utilities.

All these techniques for building resilience are well covered elsewhere. Our point is that only by building a stress-testing capability can a company know where to focus its efforts for resilience. Leaders need to make stress testing an integral part of the DNA of decision making. They can start by defining a set of suitable stress tests in two ways: conducting a thorough review of the business system (to see around corners) and questioning basic assumptions. Then they can quantify the potential impact of any risks and assess the resilience of the company and its individual business units.

Adding a stress-testing capability isn't onerous. Companies will probably need one or two additional researchers to complement their current market-intelligence and analytics teams. In all likelihood, the scenario-planning models currently in use can be repurposed for stress tests.

The strategy function is stress testing's natural owner, as part of the main strategic-planning process and linked to financial planning. The businesses should offer input much as they do today. Decision-making groups (such as the executive, strategy, or investment committees) should use stress-test results in their work, integrating the new capability into the organization. The traditionally strong links among strategy, finance, and operations should insure smooth integration and interaction. ■

Sven Heiligtag is a partner in McKinsey's Hamburg office, where **Susanne Maurenbrecher** is a consultant; **Niklas Niemann** is a consultant in the Cologne office.