



By Peter High

Out of Alignment

Hugging the business too closely can squeeze the lifeblood out of IT

Much has been written about the need for information technology departments to align with the business units within their companies. IT should understand the company's strategic direction, so the thinking goes, and develop solutions to meet those needs. This trend led many IT departments to develop a return on investment (ROI) analysis for each project.

Although the advantages of IT's intimacy with the business abound, the concept raises the question: Is it possible for IT to focus on the business at its own expense?

As IT achieves more value on behalf of the business, it tends to focus less on IT, reminding us that IT's alignment with business must be balanced with an alignment of business to IT. The former has been sacrosanct, whereas the latter is rarely considered. For a true partnership between business and IT, IT must manage its infrastructure and educate the business about technology. If IT ignores its own needs, the business suffers from increased downtime and IT's inability to scale appropriately.

In the late 1990s, the IT department at Hilton Hotels performed well, but was viewed as supportive to the business. Underscoring that role,

the then-CIO reported into hotel operations.

After acquiring Promus Hotel in 1999, the organization began viewing IT differently.

Promus had developed a property management technology called System21. Under the stewardship of Tim Harvey, Hilton's executive vice president and chief information officer, the company leveraged System21, now called OnQ, into a tool that integrates reservation management, property management, CRM, revenue management, forecast and content management, Balanced Scorecard activities, and a host of other services for all the Hilton brands. Unlike competitors who have different solutions for these functions, now, as

Hilton adds about 300 hotels annually, each one need only invest in OnQ, and a holistic technology solution is in place. Although Hilton remains a hospitality company, technology is one of the main sources of its competitive advantage.

As Hilton IT delivered increased value, Harvey realized the business needed to be educated about IT to ensure enough attention was spent managing systems infrastructure. He ensured IT staff spent time with business colleagues to understand their needs and to learn business language. This enabled Hilton IT to better communicate its plans, including metrics related to on-time, on-scope, and on-budget.

For many companies, infrastructure remains the domain of techies. At Hilton, IT communicates its plans to improve the infrastructure across the business.

Dean Permenter, vice president, shared infrastructure services, explains, "We are constantly improving infrastructure efficiency through virtualization, where several applications share the server, storage, or backup capacity. The result: A true enterprise solution instead of individual systems requiring additional management and resources such as power and cooling."

Hilton IT decreased baseline costs (those costs required to "keep the lights on") even as the hotel grew. By providing the business with value metrics to represent such infrastructure successes, the inner workings of IT become tangible.

Too often, business-IT alignment is taken in that order. To be truly consultative to the business, IT must educate the business on its *own* needs and constraints and how its capabilities can serve the business.

Aligning IT to the business is just the first step toward opening the lines of communication, which should flow in both directions if companies wish to fully leverage IT. ■

Peter High is president of Metis Strategy, a Washington, D.C.-based consulting firm specializing in the intersection of business strategy and IT. Reach him at peter.high@metisstrategy.com.

▶ Read Online:
www.symantec.com/ciodigest/thinktank/high



By Stephen C. Buckley

The Reality of Perceptions

Are you secure or does it just feel that way?

When I took a job at a financial services company in Boston about 20 years ago, I had to take a course to familiarize myself with the company's products. Part of the course involved a presentation by the marketing manager, who spoke about the target audience our products would appeal to, and why. He ended his talk with some advice: "Remember, perception is reality."

Raised as a rational person, I was used to relying on facts and data, and I was often even skeptical of those. I found the notion that reality could be anything but reality preposterous. Either something was real or it wasn't.

Today, after two decades of working with people and data, I realize that the marketing manager was mostly right. Facts and data may support a given issue, but ultimately it is our perception—and assumptions—about the world that provide the basis of what we determine to be "reality." The question then becomes: Whose reality is right, yours or mine?

The realm of cybersecurity is not immune to this idea, as two researchers at the Center for Digital Business at the MIT Sloan School of Management are trying to prove. Professor Stuart Madnick and Dr. Michael Siegel are conducting a survey to measure the gap between a company's perception of its current level of security versus the desired level of security.

Madnick and Siegel have taken a holistic approach to their research, and acknowledge that good security goes beyond IT solutions. Their study examines a variety of constructs that support security, such as technology, finance, business strategy, and policies and procedures, as well as a "security culture."

The perceptions of different stakeholders—broken down by both functional areas and by positions within the organization—are also being considered. These differences are being measured not only within a firm, but also across the entire breadth of the enterprise, to include buyers, suppliers, and partners.

Examples of these perception gaps take numerous forms. There may be performance gaps, where the cur-

rent level of a security construct differs from the desired level. This is thought of as a measure of security "dissatisfaction." There may be role gaps where the IT staff believes the security is good, but the business managers think it needs improvement. Lastly, there may be inter-enterprise gaps, where an organization's perception of its security differs from its perception of

Whose reality is right—yours or mine?

the security within a partner organization.

One of the study's major findings was that significant performance gaps existed in almost every industry studied. The largest gaps resided with top executives. In other words, it was those in the executive suite who perceived the largest difference between their company's security performance and the level at which they thought it should be. This measure of executive "dissatisfaction" should inspire the curiosity of chief security officers.

Measuring these gaps is important because gaps represent opportunities for improvement and dialogue. When the state of an organization's security is below where people think it should be, some changes might need to be made. Gaps may also represent misunderstandings among various key stakeholders about the state of security within an organization, or indicate different perceptions that often result from local knowledge or needs. In global organizations, there is a multiplicity of realities to deal with.

There's a word for sharing our assumptions and perceptions in an organized, productive way: It's called collaboration. ■

Stephen C. Buckley is associate director of the Center for Digital Business at the MIT Sloan School of Management in Cambridge, Massachusetts. He can be reached at sbuckley@mit.edu

 **Read online:**
www.symantec.com/ciodigest/thinktank/buckley