

## in this issue

1

The Essential of Leadership

2

Social Security

•

CEOs: Blog or Die

3

7 Ways to Avoid Deep-Sixing Six Sigma

•

Microsoft Shares Longhorn Networking Details

4

Ten Not-So-Simple Rules for Using the Internet

## The Essentials of Leadership

Countless business books explore the key ingredients of leadership. But one professor, who's studied winning streaks, has come up with the fundamentals for leading a sports team or organization into success:



According to Harvard Business School professor Rosabeth Moss Kanter, author of *Confidence: How Winning Streaks and Losing Streaks Begin and End*, the most critical component of leadership is not self-confidence. Even more important is having and inspiring confidence in others. To lead, we must get others to put forth their strongest efforts and guide those efforts in a clear direction, she says in a passage excerpted by Harvard Business School Working Knowledge.

In the excerpt, Kanter points out that organizations in winning streaks build a momentum that coincides with the emergence of many leaders at different levels--some are promoted while others are self-appointed. Reiterating this point, Duke's men's basketball coach Mike Krzyzewski liked to say, "leadership is plural." Writes Kanter, "Even at the top, leaders often come in pairs, trios, and quartets, operating as a unit in spirit even if one of them has final authority in law."

Indeed, leadership is not about larger-than-life individuals who single-handedly turn an organization around. It's about creating an environment in which people are given the support they need to excel and thus, leadership from many different places can emerge. Need proof? Look at three-time Super Bowl champ New England Patriots, who encourage multiple leaders to step up. Observes Kanter, "Sports certainly produces a very high number of prima donnas and big egos, yet I was struck by how many of the winning teams were led by unpretentious people who boosted others."

1 Establish a culture of straight-talkers. They must foster open communication and create "humiliation-free zones," where both positives and negatives can be discussed without fear. For instance, Gillette, Verizon, and Continental Airlines have environments where data is abundant, and people are dissuaded from denying or covering up facts.

2 Lay out expectations. Continually reminding people about standards and clearly delineating goals lets them focus on both the big picture and the day-to-day execution. While making people own up to their responsibilities, leaders should also place them in positions where they can meet those responsibilities. In short, "leaders should set people up to succeed," says Kanter.

3 Ensure that information is transparent and accessible. If performance information is widely and abundantly available, people will be better equipped to place high standards on their performance, on those of others and on the system as well. Tools such as mass meetings, voicemail updates, quarterly report cards, and regular performance appraisals encourage accountability. In short, leaders must make sure that people are taking on responsibility and have the support to handle it well.

Social Security is not in crisis - yet. But it's surely headed there if nothing is done to change funding or benefits. How to fix Social Security is the question. Any solution is sure to cause someone pain.

Social Security is a pay-as-you-go system. Money coming in from current workers is used to pay benefits for current retirees. For most of the program's history, there were many more workers than retirees, which made funding benefits relatively easy. Since 1983, when Social Security taxes were hiked, more money comes in than is needed to pay current beneficiaries. But these annual surpluses held in the trust fund aren't locked up. The surplus trust fund money is loaned out to our federal government to help finance the federal budget. So the surplus is really a stack of IOUs, which this year total \$1.8 trillion.

By 2042, the fund surplus will be gone. The government will almost certainly need to borrow money once they start to pay back the Social Security surplus. This will most likely increase the national debt and potentially drive up interest rates and cause some kind of financial harm to the economy.

Numbers tell the story of why Social Security is heading for trouble. Every outsourced US job is one person less currently funding Social Security. A large number of retirees will be eligible for benefits starting in 2008, when the first members of the baby-boom population bulge hit 62, the age when about half of seniors retire. About 3.3 workers per retiree currently fund the system. Within 40 years, there will be only two workers per retiree. Looking back to 1950, there were 16 workers per retiree.

In 1940 the life expectancy was just under 78; today it is just over 83, and it is sure to get longer. All of these signs spell disaster to the Social Security system unless something is done to fix it.

Social Security will be one of the hottest topics of discussion. Everyone will have an opinion, and most assuredly, every politician will have their own solution. The fact remains, that funding and benefits of Social Security most certainly will change. The real question is what impact will this change have on you?

Tim Dyson. David Geller. Anne Stanton. These are three of the most recent CEOs to begin expressing their opinions in Web journals, a.k.a. blogs. Not exactly household names. If the blogosphere is so hot, and joining it so important, the silence of the high-profile CEO is telling. But telling us what?

If you look at the list of business leaders who have begun posting, you might think these bloggers come from two lines of work. They are heads of technology companies, disposed to use and evangelize new forms of digital processing; and public relations companies, with a vested interest in teaching existing or potential clients, a.k.a. corporations, how to get messages out.

The big news will be when a CEO such as Lee Scott at Wal-Mart or Rick Wagoner at General Motors begins to blog.

The same can be said for CEOs of any company of any size that matters. Or wants to maintain or grow market share and profits. (Could your company be one of those?)

This is the first time in the progress onward from the Gutenberg press that every head of a corporation has the chance to interact every day with every part of every market he or she deals with. Whether he or she leads the commentary, sets the agenda and shapes opinion—or leaves those tasks to someone else—is up to each CEO. Who do you want in charge of public opinion? Lawyers? Regulators? Disgruntled employees or customers?

The precedent for CEOs to step to the mike has been set in the other medium that reaches every American every day: broadcast television. Remember Victor Kiam, picking up the image of Remington razors by famously saying he was so impressed with the one he purchased that he bought the

company? Or Lee Iacocca, who saved Chrysler in the early '80s and made an on-air campaign for his company's products a central part of the rescue?

Of course, television is a one-way medium. You speak. Others listen. You don't have to deal with feedback around the clock.

Well, Michael Dell has made a fortune dealing with feedback around the clock. Every comment about his products that comes across the transom, by phone or computer, he feeds into refining what he does.

Do you think this man, who just turned 40, handles all the feedback himself? No. He has set up his organization to do it.

A confident CEO can and should regard a blog as an opportunity akin to television, but with the benefit of backtalk. And that backtalk can be scanned, summarized and focused by staff, if need be.

But look around you. If you faced the kinds of labor and economy-wrecking charges that Lee Scott does, don't you think you could and should find a half-hour once a week to set the record straight? And another half-hour a week to post your own agenda? If you're trying to convince customers that your products really do match up with those made by the Japanese and Germans—or that they're better—don't you think Rick Wagoner ought to be getting the message across in a steady drumbeat? And dealing with the direct experience and perceptions of customers, instead of just the filter of formalized statistical "market research"?

Time is not the issue. You devote your time to what matters. If your business matters, sooner or later you're going to be either defending it or going on the offensive. Where the conversation takes place.

# 7 Ways to Avoid Deep-Sixing Six Sigma

Six Sigma is renowned for helping companies deliver near-perfect products and services. But many manufacturers are actually dissatisfied with the results of their Six Sigma projects. So what are they doing wrong?

Six Sigma is all about rooting out errors in processes and products, and delivering that savings to the bottom line as increased profitability. But while many executives and managers have embraced it because of its ability to compress cycle times, minimize product defects and enhance customer satisfaction, some are less than impressed with its results.

## 1. Provide sufficient, streamlined information for Six Sigma initiatives.

The Quality Magazine article recommends utilizing a “consistent set of questions to gather, sort, organize and analyze information.” For example, one high-tech manufacturer instructed all of its customer support representatives to ask the same group of questions at the outset of each call to define problems and to pinpoint variations. By enforcing uniformity in information gathering, the company trimmed the average time it took to iron out customer issues by 58%.

## 2. Choose appropriate projects.

Companies using the portfolio approach—instead of focusing on specific functions such as the shop floor and the purchasing department—tend to be more successful in implementing Six Sigma. Quality Magazine suggests

plotting out all products and services in two dimensions: volume and margin. Those belonging in the high-margin/low-volume quadrant can be taken off the table. Since their high margin suggests high efficiency, such projects will most likely benefit from better marketing, not Six Sigma.

## 3. Anticipate future problems.

Don't forget to ask the all-important implementation question: “What could go wrong?” According to Quality Magazine, “every implementation plan should include an analysis of potential problems, their likely causes, and preventive and contingent actions.” Companies should turn to customers and suppliers for input and direct the team's efforts to preparing for potential stumbling blocks.

## 4. Listen to your customers.

It's simple and basic (in fact, it's the first rule of Six Sigma!), but many are neglecting to do this. In fact, a survey conducted by Greenwich Associates found that only 3 out of 13 companies “mentioned customers as critical success factors” when they were asked to spell out what made a project effective. Many companies are mistaking the “voice of accounting” for that of the customer or placing too much emphasis on benchmarking.

## 5. Attack the root of the problem.

According to Quality Magazine, most Six Sigma teams make the mistake of rushing into action. Pressured to make improvements quickly, they fail to fully grasp the reason for shoddy process

or product performance. “Without identifying, verifying and removing the root cause of the problem, teams almost always fall short of reducing variation,” says the article.

## 6. Follow a disciplined project-management approach.

All team members should be on the same page about how to manage the project. Before planning, each team should be made to define the project's scope and deliverables. They should be armed with “clear assignments, accurate sequencing and realistic timeframes,” according to Quality. Once they enter the implementation phase, they should track progress through milestones and regular reviews. For example, some companies employ a Six Sigma Project Dashboard, which lists all ongoing improvement projects and depicts how they're doing against objectives, schedule and costs with red, yellow and green indicators.

## 7. Take account of the “human side of change.”

While technically sound, many solutions can be bound for failure because they do not consider the human side, which is composed of five elements: situation, performer, response, consequences, and feedback. The implications of the project on each element must be considered. For example, make sure that people are made aware of how their job situation will change and are trained on the new required skillset.

## Microsoft Shares Longhorn Networking Details

Microsoft execs have been reticent to talk about changes that Microsoft is making to Windows' core “Fundamentals” pillar with Longhorn. But on Tuesday, a handful of Microsoft's top Windows Longhorn networking officials opened up a bit.

Led by Jawad Khaki, corporate vice president of Microsoft's networking and devices technologies division, the Microsoft Windows execs participated in an hour-long Web chat on the topic of

Longhorn Networking.

Ironically, the chat, attended by nearly 300 participants at one point, was plagued by constant connectivity problems. Nonetheless, the execs provided answers to a number of high-level Longhorn networking questions.

Longhorn client is due out in 2006; the server variant is slated for 2007.

Microsoft has said to expect Longhorn

to consist of three core “pillars,” or subsystems: Avalon, the presentation subsystem; Indigo, the communications one; and a catch-all “Fundamentals” category, consisting of enhancements to Windows' core networking, security, performance and reliability functionality.

Microsoft is expected to release a Longhorn alpha around the time of its Windows Hardware Engineering conference in late April. A first beta is expected by testers this summer.

# Ten Not-So-Simple Rules for Using the Internet

Even technically sophisticated users lose perspective on security at times. We all want breaches of security to be someone else's fault and we don't want to have to deal with the inconveniences of running a secure system.

But there are certain security rules that apply to all computing platforms. These rules are expressed well in an article on Microsoft's TechNet site called Microsoft's Ten Immutable Laws of Security. These laws are worth keeping in the back, and often the front, of your mind.

**Law No. 1:** If a bad guy can persuade you to run his program on your computer, it's not your computer anymore. The first law, appropriately, is the most important one. It's a truism so true that it often gets dismissed as trite when it's actually at the heart of many attacks. It is at the heart of many social engineering attacks, including spyware and almost all e-mail worms, including Bagle and Netsky.

**Law No. 2:** If a bad guy can alter the operating system on your computer, it's not your computer anymore. I really hope this is obvious. Some programs on the computer must be trusted, and—significantly—I lump device drivers in this as well. Microsoft has actually put good protections into Windows against such threats with system file protection, which looks for modifications to critical system files and undoes them.

**Law No. 3:** If a bad guy has unrestricted physical access to your computer, it's not your computer anymore. There is no security without physical security. Consider that someone alone with your computer can boot it up off the floppy or CD drive and run his or her own software while none of the software on your computer can protect it. The attacker could install spyware, compromise your own

security provisions, or just wipe out the disk.

**Law No. 4:** If you allow a bad guy to upload programs to your Web site, it's not your Web site any more. "Upload" is such an official way to put this; the real-world way this often happens is to invoke a buffer overflow on the server in order to run arbitrary code on it, but there are other ways it can happen.

**Law No. 5:** Weak passwords trump strong security. If I can guess, quickly, that your administrator password is "admin" or something else easily surmised, then Law No. 1 comes into effect because I can run whatever I want on your computer. I can do a lot of damage with just a user password as well.

**Law No. 6:** A computer is only as secure as the administrator is trustworthy. Microsoft uses business examples in this case to show how important it is to a business that the system administrator be trustworthy, and this is an essential point. Every consultant you hire may require administrative access and need to be trusted with the assets of your business. But it's true at home, too. Are your teenagers trustworthy with your computer? Maybe they shouldn't be administrators.

**Law No. 7:** Encrypted data is only as secure as the decryption key. In public key cryptography there is a private key that only you should have, and it's called the "private" key for a reason. If it's stored on the computer, then an attacker could get access to it. The same is true of passwords. You need to memorize them or store them in a place that can't easily be compromised. This is inconvenient, but at least be aware of the vulnerability you're creating if you make passwords and encryption keys too convenient.

**Law No. 8:** An out-of-date virus scanner is only marginally better

than no virus scanner at all. "Marginally" is a debatable way to put it. No doubt about it, it's better to be up to date, but the most prevalent threats out there are quite old. If the user is not too credulous and you do update the scanner before too long, it's not disastrous.

**Law No. 9:** Absolute anonymity isn't practical, in real life or on the Web. Much of the Web appears to be a place you can visit and interact with anonymously, but this is largely a mirage. Unless you're very careful and sophisticated, you are always leaving clues around as to who you are and how someone could track you down. This usually doesn't matter because, realistically, who cares about what Web sites you're surfing? But don't assume that you are the wind and that you can whisk in and out of sites unseen.

**Law No. 10:** Technology is not a panacea. Security is, unfortunately, a series of trade-offs with other goals we expect from computing, with convenience usually at the front of the list. Novices may expect security suites that claim to be comprehensive will protect them, but this can never be the whole truth.

The fact that security can't be perfect isn't a reason to criticize anyone—it's just a fact of life. You can't do a perfect job, but you can do a good job, and knowing the limitations of the technology is a good place to start.

