Feds May Unleash Six Sigma On Terrorism

By Del Jones, USA TODAY

At a time when fighting the war on terrorism has become arguably the most important issue facing the USA, authorities are looking into an unlikely weapon to aid their fight: Six Sigma.

Six Sigma is nothing like a laser-guided smart bomb but rather a statistics-heavy regimen of analyzing problems that has saved corporations billions. (**Related story:** Taking the Six Sigma approach)

Even 99% accuracy falls short

Six Sigma is a set of statistical and management tools that can make leaps in improvement. When something reaches Six Sigma, it has a failure rate of 3.4 per million, or 99.99966% accuracy. However, being just 99.0% accurate can sometimes spell disaster. It means:

- At least 200,000 wrong drug prescriptions each year.
- Two short or long landings at major airports each day.
- 5,000 incorrect surgical procedures every week.
- 20,000 lost articles of mail per hour.
- No electricity for almost seven hours each month.
- 50 dropped newborn babies each day.

Source: American Society for Quality

Can an arcane management process save lives by helping prevent terrorist attacks? Mikel Harry, often called the father of Six Sigma, says it can, in a major way. He estimates the USA would be safer from terrorist attacks by a factor of hundreds or thousands.

Companies like to brag about improving efficiency, but as a matter of policy, the secretive Central Intelligence Agency won't say whether it is investigating Six Sigma as a way to strengthen its terrorism-fighting arsenal. However, Six Sigma experts say they have been called in to consult with various homeland security agencies.

Whether corporate success can be repeated in a federal bureaucracy is an open question. Six Sigma is "powerful stuff" that could work even in the sprawl of the U.S. government, Dell Computer CEO Michael Dell says.

First used by Harry and the late Bill Smith at Motorola in the mid-1980s, Six Sigma symbolizes 3.4 mistakes per million opportunities. The process was originally used to eliminate assembly-line defects but has expanded into almost every corporate operation. It uses a complicated approach to problem solving called DMAIC (define, measure, analyze, improve and control).

Experts say it could be used in thousands of homeland security projects.

Consider the mountain of information that floods into the CIA, such as intercepted phone calls, applications to pilot schools, etc. Suppose an e-mail is intercepted that includes a disguised threat on the Golden Gate Bridge. A quick decision must be made to discard the e-mail or take it seriously. Discarding bad information is crucial because useless data can paralyze decision makers further up the line.

There may be 50 points where such pass-fail decisions must be made about the usefulness of a piece of information. In Six Sigma talk, these points are called "decision nodes." If each of those 50 nodes passes judgment on 60 pieces of information each day, there are 300 opportunities for a decision error each day as intelligence moves up the chain to Security Chief Tom Ridge and President Bush.

If decision nodes average 99.38% accuracy, they are at Four Sigma, which is about the accuracy of services such as prescription writing by doctors and airline baggage handling.

If improved to Six Sigma, accuracy is 99.99966%. That means only one of about every 294,000 pieces of vital information would be erroneously discarded.

At Six Sigma, there is a 99.9% chance that all 300 decisions are accurate on a given day. There is a 97% chance all decisions in a month will be right. Where there is only a 15% chance that all decisions are right on a given day at Four Sigma, there is a 15% chance that all decisions will be right over a five-year period at Six Sigma.

Such efficiency would be invaluable when lives are at risk. "A quantum difference indeed," Harry says. That's how attaining Six Sigma in the war on terrorism could make the USA 1,800 times safer, Harry estimates.

Not everyone is so optimistic. Even fans like Michael Dell warn it could take years for U.S. intelligence agencies to fully implement Six Sigma but adds, "It's possible."

Six Sigma is lousy at fixing rare and random problems, says Elizabeth Keim, president of the American Society for Quality and a Six Sigma consultant. And terrorism, at first glance, seems to be the very definition of rare and random.

But Keim and others schooled in Six Sigma see events like the Sept. 11 attacks as the catastrophic result of a breakdown in the millions of frequent and mundane preventive steps that must be taken with vastly greater efficiency. These steps are drudgery: identifying the millions of people entering and leaving the USA, mapping the entrances to water plants or detecting E. coli in farm products.

"The particulars of Six Sigma are not exciting" when used in business or in war, says Dan Burnham, CEO of Raytheon, a defense electronics company steeped in Six Sigma and which makes such anti-terrorism technologies as facial recognition. It's the results that are striking, he says.

Deploying Six Sigma against terrorism would be little different than when it was used to determine that most steps in a Japanese patent system's application process were wasteful. The cost of each filing was slashed to $1,200 from $48,000. Communication satellites are rented out by the second and are not always used efficiently. General Electric used Six Sigma to make sure its satellites were being used 97% from 63%, adding $1.3 million a year in revenue. Former CEO Jack Welch, who drove Six Sigma deep into GE's culture before his retirement, counts himself among the cautious optimists that Six Sigma could work against terrorism.

Fighting terrorism isn't really much different than marketing, Harry says. Marketing executives, like intelligence experts, must digest mountains of mostly useless data, analyze the fraction that is important and persuade decision makers to get the right product on the shelf just as consumer tastes are changing. At its best, marketing influences consumer tastes, which like terrorists, are a moving target.

Even after hearing about the billions saved at companies like GE, others have abandoned the Six Sigma effort in frustration. Fewer than 15% of the *Fortune* 1,000 are using it in a significant way.

Burnham says it won't work without an "obsessive, compulsive" CEO. Welch says he was a "raving lunatic" about it. Some GE employees privately say that the most common-sense solutions can no longer be made easily but must pass a rigor of charts and statistics.

Companies that don't stick it out for at least five years soon revert and lose all progress. That doesn't bode well for the federal government, where attention spans often don't survive election cycles. "The federal government makes GE look like an ant on an elephant's back," Harry says, and there will be a "a gantlet of pain" to get it implemented.

Former House speaker Newt Gingrich, who speaks at Six Sigma conferences, says he would be surprised if the CIA is seriously considering Six Sigma but says it eventually will have to because of the nation's inefficient counterterrorism.

There is no better chance than during a time of emergency, experts say. And the government isn't starting from scratch. Military contractors are among the early implementers of Six Sigma, and generals and admirals are among the converts. Air Force Secretary James Roche came from Northrop Grumman, a defense contractor steeped in Six Sigma.

At least one local government is using it. A Six Sigma project helped get 98% of the potholes in Fort Wayne, Ind., filled within 24 hours. It also will help the city figure out how to get twice as many contaminated people through the showers of a moving van converted for emergency use, Mayor Graham Richard says.

A Six Sigma onslaught against terrorism would produce many byproducts for the government, including cost savings, Keim says. She predicts that it will improve the fight against all crime. Statistics will lead to profiling, but it will be profiling based on science, not prejudices, she says.

It may be coincidence, but CIA Director George Tenet is sounding like a convert. In his Oct. 17 testimony to the Senate Select Committee on Intelligence he used some Six Sigma vocabulary in calling the intelligence breakdown relating to Sept. 11 an "error" that exposed weaknesses in the process. He used the word "customer" for the recipients of intelligence. Six Sigma at corporations is built around customer needs.

"In the counterterrorism business, there is no such thing as 100%," Tenet said.

Neither is perfection achievable in business. But in the quest for the near perfection of Six Sigma, companies say they have achieved improvements that did not seem possible. "You can't tweak the existing system and get there," Harry says.