

Rage against the machine

Diebold struggles to bounce back from the controversy surrounding its voting machines.

FORTUNE

By [Barney Gimbel](#), Fortune writer-reporter
November 3 2006: 9:46 AM EST

(Fortune Magazine) -- Here's a five-step plan guaranteed to make an obscure company absolutely notorious.

First get into a business you don't understand, selling to customers who barely understand it either. Then roll out your product without adequate testing. Don't hire enough skilled people. When people notice problems, deny, obfuscate and ignore. Finally, blame your critics when it all blows up in your face.

With missteps like those, it would be hard to succeed in the gumball business. But when your product is the hardware and software of democracy itself, that kind of performance gets you called not just incompetent but evil - an enemy of democracy. And that is what has happened to [Diebold Inc. \(Charts\)](#) of Canton, Ohio, since it got into the elections business in 2001.

The move seemed like a good idea at the time. The \$3 billion public company, whose core products are ATMs, bank vaults and security systems, had just sold 186,000 voting machines to Brazil, where they delivered a quick and clean count in the 2000 elections.

Surely, Diebold reasoned, it could duplicate this success closer to home. "We thought if we got this right," says Thomas Swidarski, the company's CEO and president, "then we could do it across the globe."



PHOTO: HENRY LEUTWYLER

Vote here: The AccuVote-TSx is light, easy-to-use, accurate - and controversial.

[More from FORTUNE](#)
[An Apple phone is no slam-dunk](#)
[Tech targets the Third World](#)
[10 best places to own real estate](#)
[FORTUNE 500](#)
[Current Issue](#)
[Subscribe to Fortune](#)

But faster than you can say hanging chad, things went wrong. In early 2003, activists found a version of Diebold's secret software on the Internet. The code had so many security flaws that one group would later post a video of a chimpanzee changing votes.

Weeks later, Diebold's then-CEO Walden O'Dell famously wrote to fellow Bush supporters in a fundraising letter that he was committed to "help Ohio deliver its electoral votes to the President." It didn't take long for political activists, many of them already suspicious of the new voting technology, to begin diving through the company's dumpsters and picketing its shareholder meetings.

Though other voting-machine companies have also had their difficulties, it is "the dreaded Diebold," as one blogger on DailyKos refers to it, that stirs up the likes of Michael Moore. "The reason Diebold gets so much heat," says activist Bev Harris, author of "Black Box Voting: Ballot Tampering in the 21st Century," "is not because they're any worse than their competitors. It's because we got more information on them early on."

The drumbeat of bad news has never stopped. This year, researchers have found more security flaws, and another version of the software was leaked. In Maryland, Diebold allegedly knew that some of its machines had defective motherboards but did not replace them for a year. Both candidates for governor there advised their supporters to vote via absentee ballot rather than use Diebold machines.

Rolling Stone published an article alleging that Diebold helped deliver Georgia to the GOP (Diebold calls the story "fiction"). The company is an unwitting star in a new HBO documentary called "Hacking Democracy." Oh, and the SEC is investigating accounting irregularities.

Deep in a corporate nightmare, Diebold is wondering how to shake itself awake. After all, this is a 147-year-old company once headed by Eliot Ness, the storied crime fighter. Internally there is little doubt that the company rues the day it stepped out of its comfort zone and into the maw of electoral politics.

Selling political equipment to politicians is an ugly business - and thanks to lawsuits, lobbying expenses and public relations consultants, the profit margins have been stingy too. (The voting division, which accounts for just 5 percent of the \$3 billion company's revenue, only started making money last year.)

But after a close look at Diebold and its operations, it's hard to see the company as evil. Naive? Yes. Ignorant? Sure. Stupid? Sometimes. "We didn't know a whole lot about the elections business when we went into it," admits Swidarski. "Here we are, a bunch of banking folks thinking making voting machines would be similar to making ATMs. We've learned some pretty painful lessons."

A history of success

A cow, a lantern, and a straw-filled barn made Charles Diebold (pronounced DEE-bold) a household name in the banking world. It was the night of Oct. 8, 1871, when, as legend has it, the Great Chicago Fire started in Mrs. O'Leary's cowshed. When 878 Diebold safes survived with their contents unharmed, business took off.

Canton became known as "Little Germany," thanks to the thousands of immigrants who flocked to work in the Diebold factories. (German immigrants arriving in New York reportedly only had to say "Diebold" for directions to Canton-bound trains.)

By the beginning of the 20th century, the company was making jails, trapdoors for gallows, and padded cells for asylums. During World War II it made armor plating for tanks and airplanes. Then, in the 1960s, the company bet its future on a speculative technology: automated teller machines.

Diebold quickly became a global market leader. But it stayed intensely Midwestern, content to manufacture its machines locally and allow companies like [IBM \(Charts\)](#) to distribute them overseas.

In the mid-1990s, however, when rival [NCR \(Charts\)](#) passed it to become the market leader, Diebold changed tactics and took control of its worldwide distribution (today its share is 30 percent). The company began buying up suppliers around the world, including a Brazilian ATM maker, Procomp Amazonia, in October 1999.

Entering the political sphere

Around the same time, the Brazilian government was looking to fully automate its election system. Procomp got the \$106 million contract - Diebold's largest ever - to make 186,000 identical electronic voting machines for the 2000 election.

At the exact same time that Florida's officials were haggling over butterfly ballots, Brazil's were congratulating themselves on a clean and tidy result.

Emboldened by Diebold's success in Brazil, CEO Walden O'Dell set out to ensure that the company got a serious piece of the U.S. elections business.

The first problem was that the Brazilian machines weren't sophisticated enough for the U.S. market and couldn't be certified quickly. So O'Dell needed to buy a company to get into the market for the 2002 midterm elections.

In June 2001, Diebold announced it was acquiring Global Electronic Systems, based in McKinney, Texas, for about \$30 million. Global was a \$7 million operation that made most of its money printing ballots for its optical-scan reading machine. Its touch-screen system, the Accu-Vote-TS, wasn't a big seller.

Nothing was a big seller then. The elections business was populated by a couple dozen private firms that often literally sold equipment out of the back of their cars. That's because their customers were poor.

U.S. elections are intensely local affairs, run by more than 3,000 separate counties. Buying new equipment was a luxury. If county commissioners had to choose between filling a pothole or buying new voting equipment, the pothole invariably won.

That all changed when Congress passed the Help America Vote Act in 2002. With it came \$3.9 billion in grants for states to replace punch-card and mechanical-lever machines and to set up statewide voter lists.

Local election officials soon found themselves inundated by high-powered lobbyists. "I don't think those election boards had ever seen as many dinners out," says Paul Tipps, a prominent Democrat who lobbied for Diebold in Ohio.

With its main rivals - Oakland, Calif.-based Sequoia Voting Systems and Omaha, Neb.-based Election Systems & Software - making inroads in Florida, Diebold targeted other states. In March 2002, just two months after it completed its purchase of Global, Maryland put in a \$13 million order to equip four counties with touch-screen machines. In May, Georgia signed a \$54 million contract to buy 20,000 Diebold machines.

Early warning signs

After the takeover, the big contracts meant big problems. Diebold had let the Global operation alone, but it just couldn't keep up. Orders were lost, manufacturing fell behind schedule, the technical staff was overwhelmed.

Recalls Swidarski, the unit lacked "the wherewithal really to know how to manage a business. They were doing complex rollouts without the depth or breadth or skill set to deal with what they were going to do."

The same could be said of the customers. Election administrators were often unsophisticated county employees who had been in the job forever. "If we work with Bank of America and they want to roll out 1,000 ATMs, they'll have 25 professional project managers," says Swidarski. "You go to a meeting at a county and you're looking at two people."

It didn't help that Global's touch-screen system, the AccuVote-TS, was flawed from the start. It had purchased the technology from a small company called I-Mark, whose founders had designed it as an unattended voting terminal that could be used in places like shopping malls or supermarkets. "The only problem was they weren't looking at security," says Douglas Jones, a computer science professor at University of Iowa who has been testing voting machines since 1994.

Not quite the only problem. Because there was little demand for touch-screen systems before 2001, Global hadn't spent much on software development. (Jones thinks they needed to start over.)

So the system voters used in 2002 was bug-ridden. Diebold machines crashed early and often, and there was insufficient trained staff to cope with the inevitable problems. (One problem: "vote hopping," where, due to an uncalibrated touch screen, pressing one candidate counted the one next to it.) Even so, after the election, press accounts largely glossed over the problems as isolated hiccups. Orders continued to roll in. And then things fell apart.

Until recently, hardly anyone gave a thought to the mechanics of voting. Even fewer thought about hackers. But in the wake of 2000, the mechanics of voting became politicized.

One key moment came when Bev Harris heard her suburban Seattle county was considering switching to electronic touch-screen machines. Curious, she started trawling the Internet for information - and late one night in January 2003, she discovered a cache of files on an unprotected Diebold server. In it were e-mails between programmers discussing the system's problems.

"Distributing this software is extremely dangerous," a programmer wrote in 2001. "Our smart-card format has absolutely no security, so if someone were to get a copy of this software and a reader, they could stand at the ballot station and quietly burn new voters cards all day.... I can see the cover of *USA Today* in my head. Consider everyone warned." (Diebold says the problem was fixed before the 2002 elections.)

Digging further, Harris found a version of the company's secret software that ran the machines. She passed it to Avi Rubin, a computer science professor at Johns Hopkins University in Baltimore. Within an hour, Rubin says, he discovered that the software's encryption system was one "everyone knew was broken since 1998." That same day, he found that the administrative password to all the machines was the same: 1-1-1-1.

"It looked like an experimental student project," Rubin says. "If it was my student's project, they would have gotten an F." His report, which came out two days after Maryland had awarded Diebold a \$56 million contract for 11,000 touch-screen machines, galvanized those who had always been suspicious of electronic voting.

The company pointed out in a 27-page retort that the software wasn't in use and that there were checks and balances to prevent fraud. The response didn't satisfy the skeptics; an avalanche of criticism - some of it thoughtful, some of it wacko - began to bear down.

In 2004, California decertified Diebold machines and joined a civil lawsuit filed by Bev Harris that alleged Diebold lied when it said its equipment had been federally certified. The company admitted no guilt but agreed to settle, paying California \$2.6 million.

At the same time, it continued to have manufacturing problems, once shutting down production because the touch-screen machines were malfunctioning. (It took a year to replace the defective

motherboards.)

Changing gears

Soon, Swidarski, then a senior marketing executive in the ATM unit, took over the elections business. "The board understands, as best anyone can, the volatile nature of the business/media and that politics are involved," Swidarski wrote in an e-mail to his deputies in the elections division. "However, the board cannot understand how the [Secretary of State] of [California] indicates that we have lied, misled, and withheld information."

Swidarski fired many Global staff and brought in a new boss from Canton, Dave Byrd, to run the business. The voting unit began to operate more smoothly, grossing \$150 million in 2005 and making a small profit.

In December 2005, the board pushed O'Dell out and named Swidarski CEO. Just as he did with the elections business, Swidarski cleaned house: Only two of the seven top executives he inherited are still at Diebold today.

Swidarski is cut from a different cloth than his predecessor. O'Dell liked deals and was frankly bored by ATMs; he loved being known as one of Bush's Pioneers - generous Republican donors. A former senior executive with Emerson Electric, O'Dell's top priority was to make the numbers.

Swidarski, by contrast, is more focused on the customers than he is on Wall Street. (He refuses to give quarterly earnings guidance.) A former marketing executive at PNC Bank in Pittsburgh, he is straightforward and unpretentious. In his short tenure as CEO, he has changed the mood at Canton. "This place is dramatically different from a year ago," says CFO Kevin Krakora, "almost night and day."

Smart Business 100, Swidarski's \$100 million plan to cut costs and increase customer service, is beginning to show dividends. Since fading to less than \$35 in September 2005, Diebold's stock is now at \$42. Profits dropped 41 percent last year, but were still a healthy \$161 million on \$2.6 billion of revenue.

Diebold looks set to beat those numbers this year. "The new management team," says Gil Luria, a research analyst at Wedbush Morgan Securities, "seems to be on top of what they really need to do to turn around the company." Krakora puts it simply, "This company prints cash."

Dubious voting

But its voting machines continue to attract scorn. In August, Edward Felten, a computer-science professor at Princeton University, got his hands on a Diebold machine similar to those still used in Georgia. With the help of two graduate students, he posted a video online that showed him infiltrating and installing a virus in what appears to be less than a minute.

Felten found that the key to the lock protecting the memory card, which is used to both update the software and record votes, was one commonly used in office furniture and even hotel minibars. Once the door to the slot was open, he could slip in a virus-infested memory card and alter votes. "We were completely floored by how easy it was," Felten says.

Diebold disputes the accuracy, integrity and plausibility of the Princeton study, pointing out that Felten's team used an old machine with two-year-old software not in use today. Plus, the team had four months to figure it all out.

"The report all but ignores physical security and election procedures," says Mark Radke, marketing director of Diebold Election Systems. "Every local jurisdiction secures its voting machines - every voting machine, not just electronic machines. Electronic machines are secured with security tape and

numbered security seals that would reveal any sign of tampering."

Therein lies the rub, says Michael Shamos, a computer-science professor at Carnegie Mellon University who has been testing election equipment since 1980.

"Diebold doesn't fully get it about security," he says. "Their position every time somebody raises the prospect of insider manipulation of elections is, 'Are you telling me you think that these election officials would commit a felony?' And the answer is, 'Yes, that's what we're saying. They might commit a felony, and what is your system doing to prevent them?'"

Even so, Shamos doesn't completely buy the Princeton study. "What Felten found wasn't a bug in the software," he says. "It was a deliberate feature that comes from the need to be able to update the machines quickly."

Felten, he says, makes it seem like anyone with a memory card could go into a Diebold machine, root around and swing an election. Shamos points out that since the machines aren't networked, a virus would have to be tailored to the ballot and inserted into each machine one wanted to manipulate. That's a lot more work - and a lot more opportunities to screw up - than it looks like on video.

A national rollout of almost any product is bound to have glitches. But when elections depend upon the product in a country whose politics are scarred by distrust, there is little tolerance for error.

The problem critics had with the early touch-screen systems was the lack of a tangible way - such as the kind of receipt consumers get at ATM machines - to verify results. (Oddly, few made this complaint about lever machines.)

Though about half of the touch-screen systems in use today provide an audit trail that voters can see, that presents its own problems, such as installing the paper or keeping it from jamming.

What really gets the critics going, though, is the possibility of stealing or "editing" votes by the bundle, either in a specific precinct or, worse, by hacking into a central database. As William "Boss" Tweed, who effectively ran New York City in the mid-1800s, once noted, "The ballots made no result; the counters made the result."

Diebold's critics say that is the problem. But for all the sound and fury swirling around the company, there has not been a single confirmed incident of tampering with a Diebold or any other electronic machine; it's much more difficult to write a computer virus than to tinker with a ballot box. (Ah, say the critics, but prove it hasn't happened.)

So what's the prediction for this election? The primaries were a mixed bag. One big story was that Florida was not a story, but there were problems elsewhere, from poll workers unable to boot up the machines, to transmission problems, to unexpected screen freezes.

"History shows us it always takes at least three good-sized elections before we have any new system down," says Doug Lewis, the executive director of the Election Center, an organization that represents and trains local election administrators. "It would be a miracle if there weren't problems in this election."

As for Diebold, Swidarski is questioning whether the election business "fits into our product portfolio." He says he'll make a decision within the next three months. But it says something that the company recently ordered the name "Diebold" removed from the front of the voting equipment. Why? A spokesman would only say, "It was a strategic decision on the part of the corporation."

Reporter associate Susan Kaufman contributed to this article.