

Don't Let IT Hold Your Company Hostage

by **Stever Robbins**

Business leadership isn't just about people. It's also about process and systems. Your computers are part of your processes, and these days, they're too critical to be treated as casually as you'd treat a screwdriver. Yet few business leaders know anything about them, and they happily delegate strategic, life-or-death technology decisions to IT folks who haven't a clue about business.

A few weeks ago saw one of the largest email virus outbreaks ever. Fortunately, it didn't do nearly the damage it could have done. But ladies and gentlemen, we are all at risk. You may be a non-techie, but if you're reading this, your organization isn't. You use computers and they are part of your critical infrastructure.

Bad decisions cost more than you think

If an avoidable virus or IT glitch stalls your company for a day, how much does that cost? Simple. It costs the entire cost of your company for a day. Not just the salaries of the IT folks who have to clean up the mess, but the salaries of everyone who can't work because their computers are screwed, plus the utility bills, etc. Add on salaries for the time it takes people to get back to where they were before the virus attack. And if your IT infrastructure halted commerce, add on the value of all the lost orders. Now you have the cost of a bad IT decision.

IT costs are rarely allocated wisely

If you're a senior executive and you make a bad call, you live with the results. In fact, if life throws you a curve ball, you live with the results. Your new distribution channel didn't reach the market you wanted? Oops. That's time and money down the drain, it shows up in your bottom line, and it gets factored into your evaluation.

But not true of most IT departments. They get to make lousy decisions at bargain basement rates. You see, few companies charge back the cost of IT failures to the IT department. Let's

think about a virus outbreak. IT folks must run virus removal software over your network and clean up the servers that got screwed. Fine, that gets charged back to IT. But the salaries of the non-IT employees during their downtime, and the cost of the rework they have to do all gets allocated back to their departments. So what incentive does IT have to really take the time to understand the security issues? Very little. Most likely, they're evaluated and paid for the projects they have to build, but aren't charged for the business impact of what they don't build that they should. As a result, the emphasis is on rolling out new stuff, not protecting the business.

To be fair, this isn't IT's fault. Most IT organizations are chartered as development organizations, with no emphasis on security or preventing problems. Few engineers have the training or big picture to make good security decisions. But guess what—it's our fault, too. We who build the organization must make sure IT has enough staff with the security skills and judgment to build a solid IT infrastructure. If computer security isn't on your hiring radar screen, put it there, or be prepared to pay the costs.

(Speaking of which... A misconfigured web server can expose all kinds of great company documents to the web. See the URL below¹ for a column describing exactly how to get really juicy internal information almost instantly using only Google.)

IT decisions ignore the cost of failure

"If I buy this lottery ticket, I'll win a million dollars!!!" — Anonymous

We make lots of our decisions because we think they'll get us what we want. We set our goals that way: "Go build a system that can style my hair, read my email, and coordinate meetings over the internet while singing Broadway show-tunes." But every decision is a double-edged sword (even the decision not to decide). We rarely consider the downside of a decision

1. <http://www.securityfocus.com/columnists/224>



Stever Robbins is president of Leadership Decisionworks. He can be reached at: P.O. Box 400158
Cambridge, MA 02140-0002
+1 (617) 354-1446

beforehand, unless it's blindingly obvious and catastrophically unpleasant.

When your IT team is choosing solutions, chances are, they're asking, "Which solution meets our needs?" Also have them ask, "What is the cost of this solution failing?" Microsoft products have a huge advantage: they're standard, they allow interoperability, they're pretty, and, as they used to say about IBM, "nobody ever got fired for buying Microsoft" (though they should have). The downside, however, is products like Outlook are buggy and contain huge security holes. Several of the most destructive viruses have exploited holes in Outlook and Internet Explorer¹.

Upgrading can kill your company

Microsoft has certainly endorsed a dangerous trend: software that requires activation to install and run it. More and more, it's not enough that you purchase software and install it with a serial number they give you; you must also be connected to the internet or call their telephone activation center to activate the software when you run it.

The reason for this is simple: the software publishers basically don't trust their users, and want to monitor every installation of the software closely. It makes sense from their point of view, as long as you assume your users are out to screw you. But from our point of view, this trend is dangerous.

The first of these activation schemes was Adobe Corporation's "Type on Call." They would sell you a CD full of fonts, and you would call Adobe to "unlock" fonts you had purchased.

Over the years, I purchased over \$2,000 worth of fonts from Adobe. That really isn't as many as it seems, as some of the nicer faces cost upwards of \$500 to purchase all the different weights and styles. My corporate identity was built using the Adobe fonts.

Then a couple of years ago, I bought a new computer. I went to install my Type-on-Call fonts and discovered that the activation servers had been shut down. Adobe had decided to discontinue the service, and suddenly I was no longer able to access fonts I'd paid dearly for. No one at Adobe was able to help, until bombarding the upper management with letters led one mar-

keting manager sent me a CD-ROM of the fonts in question.

Herein lies the danger: in the interests of *their* fraud protection, you are integrating the business fortunes and decisions of the software vendor into your infrastructure. If they go out of business, get acquired, or just decide to stop supporting their service, the next time you need to install their software, you can't do it. If that software is critical to your business, you're just plain out of luck.

And even if they're still in business, it's still a business burden for you. You won't always have a net connection when setting up a new machine. Sometimes—for security reasons or otherwise—you might want to install your software with your new machine disconnected from the network. Whatever the case, you'll now have to jump through activation hoops². Windows already takes way too long to reinstall, thanks to its convoluted architecture. If you have to make activation phone calls and convince the \$3.95/hour clerk on the other end that you own the software you've already bought and paid for, you're spending more of your time and money just to satisfy *their* paranoia.

Of course, no company would ever use this as a technique for forcing you to upgrade. Microsoft, for example, would never abuse their activation system by dropping activation of old products, forcing you to upgrade to a new version. But if a Microsoft doobie reads this article, watch out, they just may change their mind.

Avoid Outlook like the plague

Most of the windows vulnerabilities and worms have spread through Outlook and its address book. I don't know why Outlook is so remarkably poorly written, but it really doesn't matter. Every security-conscious technologists I know uses Eudora or a text-only mail reader of some sort. Most won't even allow Outlook to be installed on their machine. I'm sure Microsoft is working to resolve all problems in Outlook, but if the development team couldn't avoid the problems in the first place, I don't have much faith in their ability to catch all the potential problems in retrospect.

1. Microsoft likes to claim, "because we're ubiquitous, hackers target us especially." That's true. But I'm an ex-techie. I've looked at a lot of the failures. They're due to bad programming practices and poor design. I would like to think that if they know they're target #1, that would make them extra vigilant about such practices.

2. Volume purchasers can often get non-activation-required versions, but smaller businesses are out of luck.

Back up regularly, off-site

It's amazing how many companies have no regular backup regime in place. Back up regularly to write-once media (e.g. CD-R), so even if a virus invades, it can't destroy your backups. Make sure to keep an off-site copy of your backups, just in case. I've seen companies lose man-months of work because they didn't do regular backups. IT isn't pretty.

I used to back up to CD-R until my drive self-destructed a couple of months ago. Now, I back up every night over the Internet, using an encrypted connection to a secure data center that can be accessed from anywhere in the world. It's a great service that costs about the same as doing my own physical backups. I liked it so much I became a distributor. Check out the URL below¹ if you'd like to download a 30-day free trial.

Teach people: don't open attachments

Yes, the software designers could have made viruses harder to spread, but this week's attack was an email attachment that requires people click on it to open it. When someone succeeds in getting people to violate their own security, it's called "social engineering." The latest virus was a masterpiece of social engineering.

It was also a testimony to how little we've educated people about computers over the last five years. The rule is simple: never open an attachment you didn't expect beforehand, even if it's from someone you know. Period. Never. If the message appears to be an error message, don't click. Is it a "cool screen saver?" Resist the impulse. How about "The latest version of that document you requested." Punt. On the other

1. <http://www.ezbackup.com/leadership>

hand, if you asked for a Monday status report from Sue Jenkins, and the attachment is "Sue Jenkins's Monday status report.doc", you're probably safe.

Don't let IT set strategy by default

There have been a number of business failures due to strategic inflexibility caused by inflexible software and/or hardware systems. For further reading, see my essay "Are Your Junior Programmers Determining Corporate Strategy" at the URL below².

Learn how to use IT well

Like it or not, we're living in a world pervaded by information technology. I've outlined a few major gotchas, from business to technical, that you should have some awareness of if you're leading an organization. But the time is past when we could afford to ignore technology. It's changing industries, it's changing businesses, and it's making us powerful and vulnerable in ways we must master if we're to succeed in our organizations.

Steve Robbins is President of Leadership Decisionworks, Inc., providing consulting, speaking, and coaching around leadership, business, and technology. He has appeared on CNN-FN, in the Wall Street Journal, and in the Harvard Business Review. You can reach him online at LeadershipDecisionworks.com or by phone at 1-617-354-1446. ●

2. <http://leadershipdecisionworks.com/articles/juniorprogrammer.htm>

A postscript for the techie reader

Yes, I know perfect security is impossible purely through software. In fact, good security usually has to be built into a system's design from day one. But most of the viruses we've seen over the last four year could have been prevented through better design. Microsoft could have created a sandbox mechanism and launched attachments in a sandbox. They could have created a security model that required downloaded code to request privileges before being able to do anything malicious. They could stop embedding full programming languages in all their products, with security turned off by default. And they could certainly use a separate stack and data space so stack overflows aren't an invitation to run arbitrary code. They could even code in a post-1980 language that detects attempts to overflow the stack and doesn't let it happen! They could even have created a firewall that blocks unexpected outgoing connections.

By the way, these aren't fanciful ideas. All of them have existed in past systems or exist today. Tiny Personal Firewall gives you the sandbox. Zonealarm, the firewall. Java gives you buffer overflow protection. And disabling active scripting, ActiveX, and deinstalling VBScript at least helps with the programming language problem.