

# Avoiding IT Pitfalls

BY ROBERT P. GREEN, CPA AND SCOTT COOPER, CMC

Unauthorized access, ineffective processing and reporting, theft, manipulation and loss. These common information technology plagues for smaller and middle-market businesses can be avoided with a well-designed and well-deployed IT strategic plan.

However, before you can start work on an IT strategic plan, you need to learn from others' mistakes and consider some of the challenges to implementing IT effectively.

## RELIANCE ON CUSTOM SOFTWARE AND ITS AUTHOR

Consider the following not-so-unusual case study.

Brandon, a light-manufacturing business owner, has outgrown QuickBooks. He also wants an improved website to conduct business more effectively with his customers.

Brandon feels his business is so *unique* that he *must* have custom-written software.

Without researching suitable software available in the market, and without consulting others about how to successfully engage custom software programmers, Brandon hires Joe Programmer—a one-man programming firm and friend of a tennis buddy—to write and deliver his dream software. Brandon assumes that his custom software will handle *all* of his business transactions.

Joe spends numerous isolated years developing, testing and installing Brandon's software and website without a plan, process map, status meeting, software development contract or documentation of a single line of code. Rather than selecting the most suitable programming language and databases, Joe uses obsolete ones with which he is familiar.

Seven years and many thousands of dollars later, Brandon still lacks his dream system. Instead, among the gems he owns, is a vulnerable, frequently hacked website from which customers buy merchandise using credit cards over a nonsecure connection. His system processes accounting information but frequently crashes, corrupting the database. He can't trust his Accounts Receivable Aging, Vendor Payable Listings or monthly P/L reports to be accurate. And his dream report, the Daily Sales Report, is unreliable.

Brandon's CPA urges him to develop an IT plan because his business suffers from unreliable accounting reports, weak information systems and, more importantly, is at risk because he has placed all of his company's data in software written and supported by *one* person.

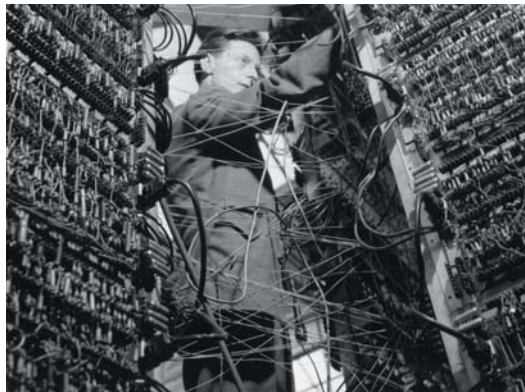
Brandon replies, "I'm not making any changes—I've spent so much on Joe and his program that I can't justify any significant expenses in that area. Besides, Joe is getting belligerent with the

staff around here, so I really don't want to let him know I'm interested in making a change. He might just leave me high and dry."

In effect, Brandon's business data is held hostage by Joe, the only person who knows how it is stored, processed, accessed and managed.

To avoid the costs and risks of this predicament, Brandon could have implemented a proven, current, reputable, widely available, multi-functional and industry-specific software application.

And if a custom software solution was absolutely necessary, Brandon could have engaged a sound, professional programming firm with extensive knowledge and experience as well as the ability to provide years of reliable support.



Others' Mistakes Can Be  
Your Guide to IT Success

## A FAILURE TO UNDERSTAND

To ensure that information for effective and proactive business decisions is available, management must determine exactly what information is vital to business success. Consider these points when undertaking IT projects, particularly when procuring new software systems:

- Determine the necessary system outputs that can be used to measure how effectively the business is performing (e.g., ratios, statistics, key reports—not just financial data).
- Understand the time needed to implement and maintain a new system. Don't overlook the time required from department managers during design and implementation.

- Be ready to manage the myriad tactical, technical and functional changes that occur naturally new software is implemented.
- Provide training for all staff who will use the systems. The garbage-in, garbage-out syndrome comes from ill-prepared staff entering the wrong data.
- Invest in system maintenance, administration and software and hardware upgrades.
- Never expect to find a fit for all your processes and transactions in one software application.
- Seek expert advice to help make technology investments.
- Beware of software and service brokers who may not have your best interests in mind, but instead, a quick referral fee.
- Be *very* skeptical if software is free or too low priced compared to others.
- Remember that software alone will *not* improve a business. It takes planning, patience, effort, investment and commitment.

## CLONE EQUIPMENT AND THE LOCAL COMPUTER GUY

Everyone wants a bargain, however, you truly get what you pay for. To avoid problems, you should:

- Be skeptical of clone equipment. Rely on reputable, brand-name components that come with onsite, prepaid warranties. Otherwise, you risk improper and insecure configuration of all system software, as well as noncertifiable network design.
- Be certain that any system you install is servicable by more than one individual. If the consultant who builds the network is the only one who can service it, you are backing yourself into a corner from which you'll find it tough to emerge.
- Diligently research service providers. Ask for—and check—references. If you are installing a large network, visit a business whose network they created and scrutinize the work. Check for professional liability and workers' compensation insurance. And always obtain an engagement letter or service agreement.

### UNNECESSARY SECURITY VULNERABILITIES

Your data is what makes your business unique. It is a valuable asset that needs protection against loss. Implementing prudent security practices and equipment is common sense, yet companies with poorly configured or otherwise ineffective IT security lose billions of dollars annually. Ask yourself:


- Who has access to my files, software and website?
- What data travels via e-mail? Confidential files? Trade secrets? Accounting records?
- Are hackers accessing or manipulating my data?
- What are employees doing on the Web? Does their behavior expose me to liability for sexual harassment?
- Are all meaningful data (documents, accounting records, etc.) and applications backed-up regularly? Who has the tapes? Are the tape contents verified and stored securely?
- Am I protected against power outages and surges, fire or total system loss?
- Are viruses being identified? If so, are they identified throughout the network—or just on the server?

### WE-HATE-OUR-SOFTWARE SYNDROME

Businesses often fail to take advantage of existing features in their current software. When employees and their managers say, "We hate using XYZ software," they just may be unfamiliar with the product's capabilities.

Before you needlessly throw out software, assess first what your business really needs the software to process and report, then ask:

- What are our needs from our systems—whether we use XYZ or another application?
- Do we really know how to use XYZ?
- Can we make changes to XYZ's configuration, or its reporting functionality, that would enable us to meet our needs or make better-informed decisions?
- Is scrapping XYZ the right answer?

These pitfalls are just a sample of the IT challenges facing small and mid-sized businesses. You can best avoid them by developing, deploying and maintaining a well-conceived IT strategic plan. 

## Positive Solutions

**Robert "Bob" Green, CPA, and Scott Cooper, CMC** are principals at *INSYNC Consulting Group, Inc.*, which provides IT solutions in the areas of software selection and implementation, IT security, network design and implementation, technical project management and electronic discovery/forensics. You can reach them at [Bob@INSYNCCusa.com](mailto:Bob@INSYNCCusa.com) and [Scott@INSYNCCusa.com](mailto:Scott@INSYNCCusa.com) or (310) 446-8600, x650.