

# BIG TIME BLUNDERS: MISTAKES IN MANAGING IT

By Sharon D. Nelson, Esq. and John W. Simek

© 2009 Sensei Enterprises, Inc.

Management barks orders. IT obeys. What choice does it have? Law firm management calls the shots, pays the salaries and has the power to fire the disobedient. Yet management is not always right. In a law firm, it has been our experience that management frequently makes some very poor calls based on faulty premises and insufficient (or dead wrong) information. Some of the major blunders are these:

1. **Determine that the firm must have the latest and greatest technology.** Look, it's simple. If you lead, you bleed. IT experts will tell you to let a new product draw someone else's blood. Give it six months or more so all of its flaws can be uncovered, documented and fixed. Do not join the lemming horde and run cheerfully en masse over the cliff. Early adopters of the iPhone were almost lustful in their desire to be the first kids on their block to own this much-heralded gadget. And yet, the iPhone, in its first iteration, was not at all suited to be a business phone. It is far better now, though we still wouldn't recommend it for all business purposes. But it was foolhardy for a lawyer to use it as a business phone when it was first released.
2. **Adopt an Ebenezer Scrooge posture when it comes to IT.** If you try, for instance, to put a consumer grade computer in a business environment, it will not perform well. It is not designed for heavy multitasking, frequent power cycles, using modern software packages, many of which are resource hogs . Thinking that you can run a law firm on a shoestring is dangerous. Business grade machines are needed, and the failure to purchase them will result in everything from higher support costs to slow response times to the inability to use multiple programs simultaneously. You may not need a Porsche, but a Hyundai won't cut it either. The proper approach to managing IT purchases is to make sure that you are meeting your business requirements (which you must define!) and then getting the best bang for the buck.
3. **Treat the IT staff like third class citizens.** You might be surprised at how many law firm IT employees hold management in contempt. From their foxhole, they give management solid advice which is frequently ignored in a quest for lower costs, because a partner's son-in-law recommended a particular software package or simply because a particular management partner is fixated on a specific technology. Though IT attempts to explain to management all ramifications of its decisions, many IT employees have a hard time communicating with management because the two parties speak completely different languages. Respect on both sides will bring optimum results, so it should be a priority to work on communication skills. The lawyers need to avoid legal-speak and the technical folks need to avoid geek-speak.

The lawyers need not to speak from “on high” and assume that their law degrees somehow convey a superior stature. The imperious attitude of some in management often results in a “cover you’re a\*\*” mentality in IT or a “I’m not going to ask them, I’m going to just do it and I’ll ask forgiveness later if need be.” On the other side, some IT employees believe they know it all – and they don’t. They also sometimes believe that those in management are technical idiots and therefore it is worthless to consult them. Making IT and Management feel like they are both on the same team presents a considerable challenge.

4. **Ignore the “it’s my turf” mentality of some IT departments.** Frequently, because IT staff thinks management is clueless, they make decisions without getting management approval. Not all of those decisions are prudent. Unfortunately, in some law firms, the prevailing view is: “As long as IT keeps us up and running, we don’t interfere.” SOMEONE in management needs to understand and approve all major IT changes. As an example, if IT wants to do cloud computing, a very common thing these days (look it up in Wikipedia if you need information about this), someone in management had better understand what cloud computing is and make a reasoned analysis of the various security risks presented by cloud computing, particularly in light of a lawyer’s duty to keep client data confidential. We’ve seen IT determine, on its own, to upgrade to new hardware, which drew too much power and finally caused power outages. By this point, the systems administrator had left on vacation and no one knew precisely how to bring the system back up. Does this remind you of the infamous scene from *Jurassic Park* when Dennis Nedry left the control center and no one knew how to bring the system back up when he sabotaged it and brought it down? There needs to be redundancy of IT knowledge – and IT documentation should be thorough – and easily accessible to those who might need it. And, obviously, significant IT decisions should pass through a management approval process.
5. **Fail to train.** You can give lawyers and staff the best technology in the world, but if you don’t teach them how to use it, you’ve thrown a good chunk of your precious dollars away. If your IT staff cannot teach, find those who again. And for heaven’s sake, make sure you teach lawyers and staff about safe computing, including all the tricks of the trade employed by social engineers bent on getting your data. “I’m working on your system and your managing partner told me I had to finish up by the end of today or get fired – someone forgot to give me an ID and password to get into the accounting package – can you help me please?” We’re such a helpful society – please such as these work at least 10% of the time, sometimes as much as one third of the time. Teach them about malware that secretly downloads when e-mail attachments are opened, and drive-by spyware installations on websites and always, always, about social engineering.
6. **Fail to physically secure your servers.** We have seen a server room (could we make this up?) located in a former bathroom. To work on the server, you literally had to sit on the toilet. We’ve always regretted not taking a photo of working there. Your servers, in most small law firms, hold your data. Do you really want someone going postal and taking a hammer to your servers? Servers should be behind a locked door at the very

least.

7. **Ignore access control.** It is astonishing how few law firms set up proper security. Sometimes, everyone in the office has access to everything except perhaps the financial records and e-mail accounts. They can see other employees' salary, their medical data and all kinds of human relations data. Who needs access to what? That's a fundamental decision which should be made about all types of data. Once management makes that determination and explains it to the IT employees, they can implement the necessary controls.
8. **Keep technology too long.** Most computers should be replaced every 3-4 years. Servers may last as long as 4-5 years. If management is trying to get more years out of hardware than is recommended, it will generally end up paying more in the end. The hardware will go out of warranty and will end up costing more to support it as the aging hardware tries to keep up with ever-changing and more resource-intensive software. Failure to upgrade to newer software also causes problems, as new operating systems are often not compatible with old software versions – and often the newer versions, especially in the legal arena, are more current under the law. Any operating system upgrade should be preceded by an analysis of what application software might need to be upgraded. At least annually, firms should survey their current software versions and determine whether any upgrades are advisable.
9. **Ignore the need for multiple, updated IT plans and policies.** What are we talking about? E-mail and Internet usage policies, disaster recovery plans, incident response plans, back-up plans and policies, document retention plans and litigation hold policies. You may even be subject to some regulatory requirements that drive your policies. All policies should be reviewed at least annually, simply to address the fact that technology is a juggernaut and its constant changes must be assessed.
10. **Trust your IT employees.** The truth is that management has three major worries: employees who steal data (60% do when they leave), employees who embezzle money (happens in law firms all the time) and employees whose specialized IT knowledge may make it easier for them, whether disgruntled or tempted by money, to destroy or sell law firm data. Trust, but verify. In the case of IT folks, you may want to log the activities of anyone you think is disgruntled. Very little logging is done in law firms – much more should be. Penetration testing, *independent* penetration testing, should be done periodically. If there's a security hole, outsiders are far more motivated to find it than those whose self-interest is at stake. And most IT employees do not hold the appropriate security certifications.
11. **Fail to account for a distributed environment.** It's not just about computers, laptops and servers anymore. Now our data is on thumb drives, iPods, CDs, DVDs, smartphones, etc. Is all of that data secure? Probably not. Do you have any restrictions on the use of USB ports? Most law firms don't. Do you log activity on those ports? Most law firms don't. And yet, many data leaks come precisely from those ports. The more legal tech

tools we use, the more we need to bring them all under a tight security umbrella.

12. **Don't test the backup.** Backup media goes bad over time. That's an unpleasant fact of life. Yet law firms, especially small ones, generally fail to have their IT staff do periodic test restores of data to ensure that the media – and the backup process – are working correctly. We've seen, as all legal technologists have, case after case of law firm management wringing its collective hands because backup data has been irretrievably lost. It's never fun explaining that to a client.

Our list of blunders is like Campbell's soup – condensed. There are so many potential blunders that we were compelled to select some of the most common ones. Law firm management tends not to have an affinity with IT – managing partners often regard IT as an evil necessity with which management must deal in order to function in the technological era. But coming to grips with legal IT can have enormous benefits – it can assure you of data security, save you money and make your firm more productive. The end game is to live harmoniously with management and IT working collaboratively for the good of the law firm. A very nice thought, but much harder than you might imagine to implement. A teaspoon of humor and a tablespoon of humility, on both sides, will make a darn good start.

*The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) [www.senseient.com](http://www.senseient.com)*