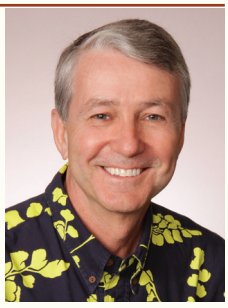
# Your IT System: An Achilles Heel?



BY GARRETT J. SULLIVAN

Under the hood of every car, there is an important, little-known piece of equipment called the serpentine belt. I had never heard of it until a few years ago when my car suddenly died. My mechanic told me that my serpentine belt had snapped and needed to be replaced. I found out then just how important the serpentine belt actually is. It silently works behind the scenes. You'd never know it was there – until it suddenly isn't.

Your information technology (IT) system is your company's serpentine belt. It runs quietly in the background until something goes wrong. That's when your company grinds to a halt. How well have you maintained your IT system?

Below are some key questions to ask yourself:

- Are you prepared for a catastrophic IT event?
- Do you have redundancies in place for Internet providers, electricity, hardware and software?
- Are there any external or internal information leaks?
- External: Ensure proper firewalls are in place.
- Internal: Ensure that employees with access to sensitive date have screen locks on their computers. These require a password when the computer has been idle for a set number of minutes. If an employee leaves his/her desk, no one else can access that computer.
- Does your company have a well thought-out plan to deal with a security breach?
- Imagine that every email, file, spreadsheet, photo and/or video stored on your company's computer system has just been made accessible to the state of Hawaii. Which items would put you and your customers at most risk? At a minimum, keep those files protected with difficult passwords.
- Inform your staff of what constitutes a security breach and what protocol they are required to follow should a breach occur.
- Does your company have a solid backup system procedure that has been validated (tested) at regular intervals?
- Computer backups should be done daily and stored onsite in a fireproof box.
- Once per week, a full backup set should be made to be kept offsite in the event of a catastrophe. If a fire, flood, or explosion occurs, the most that your organization will lose is a week of work.

If you think your company is weak in any of the above areas, it's time to have an IT audit conducted by an outside professional.

To reduce your IT risk exposure, a sample IT audit should include at the least the following:

- organization chart, roles and responsibilities of those individuals in the IT supply chain
- a review and documentation of the IT polices and procedures
- testing of the policy and procedures
- testing to see if your system can be compromised
- determination to see if your company could withstand a temporary or long-term catastrophic it event.

When Hurricane Katrina hit New Orleans, every business was under water and in need of serious help. Interestingly, most people assumed the biggest contractors would be the best prepared. Not so. Sadly, many weren't set up to even accept a phone call. Many were unable to reach their employees for weeks.

Surprisingly, it was the smaller, more savvy and prepared contractors whose robust IT systems were quickly back in operation. This gained them significant financial success.

Hawaii has been fortunate enough not to have had a natural disaster since 1992 when Hurricane Iniki wreaked havoc on the island of Kauai. In essence, we're long overdue for some kind of event.

Consider tightening your "serpentine belt" by conducting an IT audit to ensure you are well positioned to face any IT challenge that comes your way. BI

*For more reading on this subject, please visit www.SullivanHi.com. Garrett Sullivan is the president of Sullivan & Associates, Inc., a management consultancy focusing on the construction industry in Hawaii. Reach him at GSullivan@SullivanHi.com, www.SullivanHi.com, or (808) 478-2564.*