

# McKnight's

Long-Term Care News & Assisted Living

Home News Reports Newsletters Events Jobs Directory Subscribe Resources Drug Database

Products SearchEldercare.com News The Editors' Blog

RSS | Login | Register

## An IT essential

Julie Williamson  
December 01, 2007



Long-term care operators, take note: If you don't have a detailed information technology asset management plan in place, you're opening your organization up to some potentially devastating risks.

Failure to manage IT assets and adequately secure the data captured and transmitted on them poses problems on numerous fronts. Not only does it place providers at considerable risk of non-compliance with regulatory requirements, such as the Health Insurance Portability and Accountability Act, it also increases the risks for data loss, corruption and system failure – all of which could severely cripple an operation.

Many long-term care providers are falling short in their IT asset management responsibilities, experts say.

“[Organizations] want functionality with technology, but they often don't know what to do with it once it's there,” says Mike Wong, field services manager of VCPI, a Milwaukee, WI-based IT services provider. “There's often a lack of understanding of what it takes to protect the assets and the data they are generating from that technology.”

Some operators might lack a qualified, well-staffed IT department to effectively tackle the job. Others might not even be fully aware of their shortcomings and are operating under the assumption that they have their IT-related ducks in a row.

“Whatever the case, it's important that operators understand that they no longer have an excuse for not doing what's necessary to manage their IT assets,” stresses Jim Hoey, president and CEO of Prime Care Technologies, an IT services organization based in Alpharetta, GA. “It's not something they should consider doing. It's something they must be doing.”

### Assessing risks

So why, in the presence of such risks, are so many providers not taking the necessary steps to protect their IT assets and the data generated and stored on them? For starters, there's the misconception of what IT asset management, or ITAM, actually encompasses.

ITAM historically has been viewed as more of an administrative function – one tackled on a part-time basis by one or more individuals who might have been dividing their time on the help desk or other basic IT-related duties, says David Keith, director of strategic development for the International Association of IT Asset Managers Inc., Suffield, OH.

“Asset management is often viewed in terms of inventory control. While that may be part of it because obviously, you have to know the IT assets you have, it's really more about knowing what to do with those assets and the data that's on them,” he explains.

Although ITAM has been formally defined as “a set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment,” it's a vague description that could lead to even more confusion, and inadequate adoption.

In layman's terms, Keith defines IT assets as all elements of software and hardware found in the business environment. From there, he describes the function as being able to manage the business side of technology; that is, ensuring that the right assets are being purchased, that they're being managed properly once they're in place, and that businesses are staying compliant with contracts and license agreements.

Connecting all those dots is no easy undertaking, particularly with the number of disparate IT assets and stored files present in many long-term care environments.

“As more information becomes captured electronically, the risk of this information getting into the wrong hands becomes a distinct reality unless managed correctly,” confirms Tom Fahey, president of Health Care Software Inc., Farmingdale, NJ. He points out that providers who maintain disparate systems with multiple databases and access points generally have more costs and challenges associated with data back-up and security. “Organizations need to answer the following questions: What information is available online? Where is the information stored? And is there a plan in the event of catastrophic failure?”

### Sizing up the solutions

Experts generally agreed that moderately sized, regional organizations – those with more than five and fewer than 50 buildings – face the most IT-related challenges. And those problems can multiply in organizations experiencing aggressive growth.

“There are huge IT risk factors related to scalability, and there's the question of how organizations are consolidating all [those systems] and data. It's a challenge because they often end up with very divergent systems – a different payroll system, a different [charting] system, a different billing system, and so on, which can make it very difficult to manage effectively,” explains Alan Watson, vice president of strategic IT, CareCentric Inc., Overlook, IL.

That's not to say that ITAM challenges are limited to organizations of a particular size. While single facilities may have an easier time of keeping track of their IT assets, they must still have policies and procedures to ensure that their various assets are being properly managed and secured. They need to reduce the risk of data loss or corruption, or unauthorized access.

Even large providers, many of which have fully dedicated IT departments to keep a firm handle on ITAM, can find they're in over their heads in some areas.

"There are a lot of different strategies for managing IT assets. Some may be handled internally and others may be outsourced. There's no right or wrong way of doing it," says Peter Kress, vice president and chief information officer for ACTS Retirement-Life Communities Inc., West Point, PA. "We are a multi-campus organization and we have the critical mass to suggest that we should have an internal approach to managing and monitoring our systems and ensuring data back-up and security, which we do."

Even so, ACTS isn't afraid to seek outside support, as Kress pointed out.

"You don't have to automatically put in place a lot of internal expertise. Most of the things we need to manage have been effectively managed by external companies for some time, so relying on some of their expertise can really make our jobs easier," he said.

## Preventing piracy

Having a solid understanding of software license agreements is one proactive measure all providers should be taking, experts warn. Software piracy is a major offense and most vendor contracts authorize compliance audits. The Business Software Alliance is offering rewards up to \$200,000 for qualified piracy leads.

Choosing software that plays well with existing applications also is a must, as is choosing software vendors who can ensure that their applications meet current security standards.

Still, Kress points out, some vendors are playing catch-up in this area, which might translate into technology that resists being secured.

"You have to ask those important questions and make sure that the resources you have in place are adequately meeting the standards."

Some ITAM experts believe that having a simple desktop management solution in place is money well spent. Not only does it give a clear picture of the hardware and software assets in use, but it also allows for safeguards that further reduce the risks of noncompliance and data loss.

As Prime Care's Hoey explains, that level of transparency helps ensure that all applications installed on the network or individual PC are installed legally, while also providing insight into the capabilities of the organization's various IT assets, such as PC processor speeds, memory and the applications loaded on the systems.

"A small client that sits on each computer desktop lets you run reports against these PCs and then go back to the building and say, 'Show me where you've paid for these licenses to use this software.'"

Desktop management allows organizations to manage software distribution, making it impossible for staff to install software on the system without prior authorization. It also allows certain aspects of that desktop to be locked down for added security.

"If a PC has a floppy drive or USB port, do you really want someone to be able to walk up, put in a floppy and download the information that's sitting on the computer? Of course not, but you'd be surprised how many organizations aren't doing enough to reduce those risks," Hoey continued.

Desktop management also can simplify the software patching process, and keep it safer.

## Averting data disasters

Ensuring proper data-back up is one of the most vital, yet often overlooked, component in the ITAM process. Fortunately, it's a task that can be tackled more easily than ever.

Sources stressed the importance of continuously backing up data and then storing back-ups offsite (preferably more than one copy) to ensure that all business-related data can be recovered in the event of a technology failure, network intrusion or other disaster (think fire or flood). Some larger organizations with multiple buildings can store and recover their backed-up data at one of their other locations. Operators also have the option of using a third-party company to manage the task for them. Paying hardware vendors a nominal upfront annual service fee to make continuous system back-ups and store that information securely is another simple solution.

Whatever the case, portability of data access is imperative, stresses Watson. "If a building is evacuated or destroyed – even if it's the corporate office – they should still have access to their data."

Long-term care operators concerned that they lack the necessary resources to manage the ITAM function in-house also have the option of outsourcing it altogether.

If an organization doesn't want to deal with outsourcing, however, it might be a good idea to at least work with a consultant. That way, the provider can gain a better understanding of the risks, regulations, and ITAM priorities and hardware and software in place is another option that could pay off in the end.

From the December 2007 Issue of McKnight's Long Term Care News