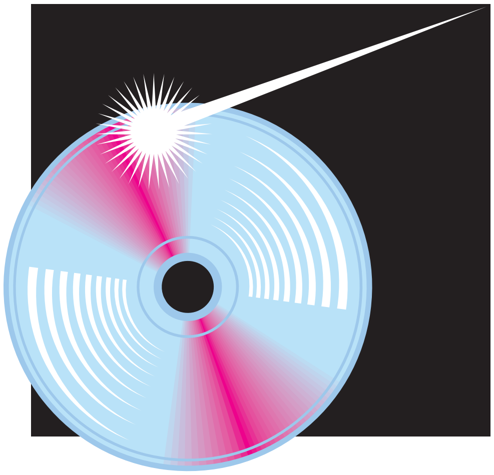
Volume XXII Number IV • FALL 2011

HYDER & ASSOCIATES MANAGEMENT REPORT

Information & Records Management Consultants ...TURNING CHAOS INTO BUSINESS ORDER®

# SECURITY ISSUES WITH CLOUD COMPUTING AND 3D STORAGE

**By: Wayne James**



This article covers general observations about two important security issues regarding how data is stored:

1. in the Cloud, and
2. on 3D Storage (high density removable disks).

## CLOUD SECURITY

The benefit of Cloud Office Software is it allows collaboration of a document across several end users on PC's simultaneously. This speeds up business decisions. It allows all involved users to make comments on the original document (which is a standard .PDF format). The changes are stored on a log file in a separate area with time and date stamps. However, loss of data regardless of where it is stored is a concern according to David Smith, professor at Pepperdine University. He estimates that 30% loss is due to human error; 40% due to hardware failure, 9% due to theft; and 21% due to viruses and natural disasters.

An example of such errors occurred to Sony. From April 17-19, 2011, hackers broke into the Sony Playstation cloud storage units. Sony reported that all of their customers' personal information may have been compromised which included credit card data. Sony recommended that all of its users notify credit companies of this personal information compromise. This is a sophisticated company which is aware of, and has protections against, such acts.

The courts have a "no excuse for data loss" policy as seen in the case of Zubulake versus USB Warburg, 2003-2004. To protect your data, ask these questions of your cloud vendors.

1. What are the various encryption security alternatives? Which of these apply during the life cycle of a record:
   a. document generation at the work station
   b. online storage
   c. archival
2. Where are the cloud and redundant back-up centers located? This is particularly important with today's financial instability of some countries.
3. What brands of security software do they use? How do these work to protect against illegal access of data and documents?
4. What security measures are in place for the protection of documents during online collaboration? This will differ among vendors. (Keep in mind that .PDF documents can be transferred into editable text by several software vendors.)

## 3D STORAGE SECURITY

This new technology is currently expensive. General Electric has announced a 500GB disk and is looking for partners to license this technology. Other vendors are claiming disks can store data ranging from several gigabytes to terabytes, and perhaps up to petabytes (1,000 terabytes of data) on a removable disk. And it's physically the size of a DVD. These disks are written on proprietary hardware. Currently the vendors' disks and hardware usually are not compatible with each other due to the different technologies that are being written to the disk. The new disks are called 3D because they write not just in two dimensions, but in three dimensions. These disks are highly redundant and can last for decades. Plus, they are not subject to data loss due to scratches like a CD or DVD. For added security, these disks are WORM (Write Once Read Many). A company can store millions of documents, pictures, Excel files, etc. on disks that are under their own control. Eventually, many of these can be stored in "Disk Farms".

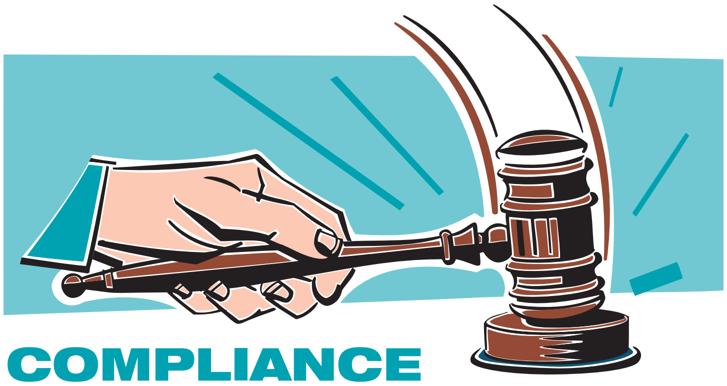
When considering 3D storage, ask the vendor these questions.

1. What is the recommended storage media used to back up these disks so you can later "write back" to the back-up disks?
2. Do they require an environmental and temperature controlled storage room?
3. Is software included that controls what can be viewed, and by whom?
4. Have these disks been certified that allows these records to be produced in legal cases?

Data and document storage is changing rapidly. It's important to question your vendor and stay informed of these issues.

*Wayne James has 40 years experience in Information Technology.*
*He can be reached at 818-773-1783*

## INSIDE ...



# COMPLIANCE CORNER

## FTC APPROVES FACEBOOK ARCHIVING

Facebook files are fair game when it comes to investigating employees and potential employees, the U.S. Federal Trade Commission (FTC) said. The FTC has approved the Social Intelligence Corp.'s practice of archiving Facebook users' posts as part of a background-checking service. The commission said the company complies with the Fair Credit Reporting Act (FCRA), which also allows the retention of consumer credit records for seven years.

If something negative about an individual pops up on Facebook or Craigslist when a search is made, Social Intelligence puts it into the individual's file and retains it for seven years, according to a Forbes report. Records that are disputed and changed are deleted and replaced by new material. Also, new employers who run searches through Social Intelligence won't have access to the materials if they are completely removed from the Intranet.

Social Intelligence's Chief Operating Officer, Geoffrey Andrews, explained to Forbes that while negative information is kept on file, it is not reused when a new employer runs a check on a person. Social Intelligence mines public data from social networking websites (e.g., Facebook), professional networking websites (e.g., LinkedIn), blogs, wikis, video, and picture-sharing websites, according to Andrews.

For the practice to comply with FCRA, a job applicant must acknowledge and approve the use of a social media background screen, just as they would a criminal and credit background check. Still, individuals should be cautious about posting questionable content online, just in case it's captured and filed away for future employers.

***Source:*** *Information Management, September/October 2011*

## FAMOUS QUOTE

***"Listening – the most important thing in communication is to hear what isn't being said."***

***— Peter F. Drucker,***
***Management Consultant***

# A MANAGER'S MOST IMPORTANT WORDS

It's tempting to think more is always better. But when it comes to words, often less is more. History remembers the heartfelt two-minute speech that followed Abraham Lincoln's Gettysburg Address. When speaking with your employees, remember the power of brevity.

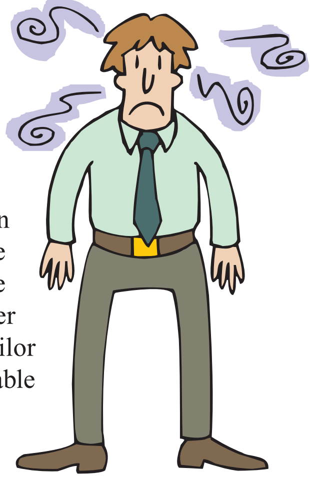
- Five most important words: *You did a great job!*
- Four most important words: *What do you think?*
- Three most important words: *I was wrong.*
- Two most important words: *Thank you.*
- One most important word: *We.*

# WHEN COMMUNICATING, SPEND TIME TO SAVE TIME

Managers spend a lot of time with their employees, but it is quality, not quantity, that really counts. By figuring out quick, efficient ways to interact with your people, you'll have more time to work on meeting all your business requirements. Here are four tips.

- **CLARIFY EXPECTATIONS UP FRONT**
  Tell employees exactly what you want, and you won't lose valuable time by having to make up for this miscommunication.
- **PRIORITIZE EVERY PROJECT**
  Prioritizing what you want is a great way to make clear what your objectives are and when you expect things to get done. Not only are time commitments clearly laid out, but employees stay focused on their own goals and yours.
- **HOLD MEETINGS REGULARLY**
  Regular meetings with employees can help everyone stay focused on the task at hand and help you monitor developments. Try to schedule one-on-one meetings as well as weekly group meetings to check on everyone's progress. By spending some time having meetings, you'll save time in the long run.
- **LISTEN CLOSELY**
  Having to juggle a lot of tasks can make it challenging for managers to pay attention to everything, and something as obvious as listening can get overlooked. By listening to your people, you won't waste large chucks of time trying to catch up with what's going on.

# THINK ABOUT THE IMPACT OF YOUR WORDS ON WORKERS



When taking a controversial stand or trying to sell others on an unpopular idea, it's not enough to think about what you're going to say. You should also give significant thought to how your words will be received.

For example, employees who have survived a round of layoffs may have an instinctively negative reaction to the word "cutbacks" when you announce the need to trim expenses. Consider employees' likely responses, and tailor your presentation to address their probable concerns up front: "No one's job is in danger, but we need to reduce some of our expenditures on supplies."

Remember, sometimes how you present an idea is more important than the idea itself.

# TRENDS...

*continued from page 4*

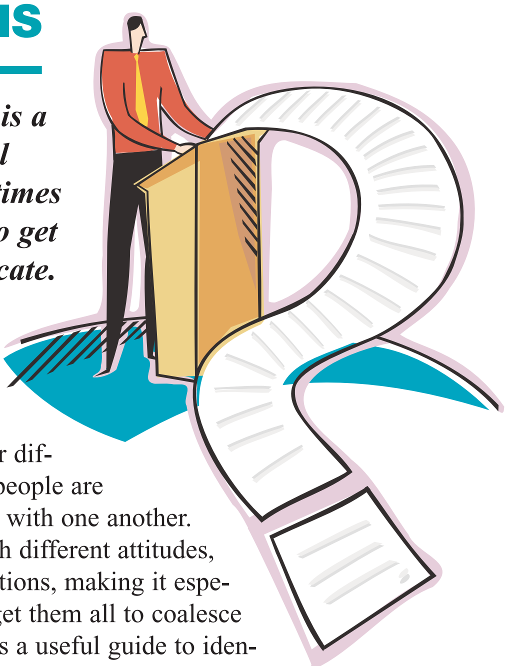
Employees don't mean to be the entry point for hackers, but they are. Below are some of the typical ways hackers enter a company.

| THE EVENT | HOW EMPLOYEES SEE IT | HOW HACKERS SEE IT |
|---|---|---|
| Opening an unexpected email attachment from a colleague | Being a good co-worker | An opportunity to inject a virus inside the corporate network, bypassing the firewall |
| Bringing a new personal gadget to the work network | An opportunity to keep up with the latest technology | A new route for viruses and spyware to make their way into corporate systems |
| Posting job detail on LinkedIn | Creating a professional presence and finding another potential job | Reconnaissance data to map out company hierarchies and target specific users with spear-phishing attacks |
| Using personal Web email for work | Making it easier to work from home or to move files between computers | A path to access critical data from relatively unprotected services |

As security problems swell due to the increase of sophisticated hackers, many companies run regular spear-phishing attacks against their own employees to teach them to be more aware. According to Kevin Mitnick, a former hacker, companies need to help executives and employees understand how vulnerable they are every day.

***Source:*** *Wall Street Journal, September 2011*

# SHARON HYDER, CMC, CRM ANSWERS YOUR MANAGEMENT QUESTIONS



***Our organization is a multi-generational work force. Sometimes it is challenging to get them to communicate.***

***Do you have any tips?***

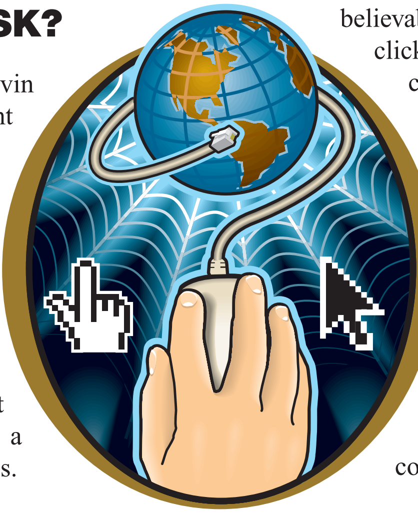
For the first time in American history, four different generations of people are sharing the workplace with one another. Each set comes in with different attitudes, behaviors, and motivations, making it especially challenging to get them all to coalesce with each other. Here's a useful guide to identifying and understanding the different generations which may help you to get them to communicate better.

- **TRADITIONALISTS ( - 1945):** Born before the end of World War II, Traditionalists tend to have respect for authority, follow the rules, and try to be productive as possible. All their years of experience earn them respect, and they generally prefer direct and straightforward leadership and structure.
- **BABY BOOMERS (1946 – 1964):** Growing up during a period of reform and social rebellion, Baby Boomers prefer a less hierarchical structure than their Traditionalist parents. They're considered to be workaholics who take pride in their accomplishments. Give them the recognition they deserve when they do good work.
- **GENERATION X (1965 – 1980):** More independent than their predecessors, Generation Xers enjoy a bit of freedom in their workplace and try to find a balance between their work and home life. Generation Xers also tend to a bit more cautious about their careers, preferring not to put all their chips into a single employers' pot. Give them as much autonomy as you can, and consider options like flexible scheduling and telecommuting to enhance their work/life balance.
- **GENERATION Y (1980 – 1999):** Also known as millennials, this generation is obviously the youngest in the workplace. Growing up around the advent of the Internet and the expansion of television, millennials multitask well and tend to be social. Take advantage of their skills, and don't assume they're all slackers. Most want to be engaged and they're looking for interesting work and a reason to care about it.

# TRENDS...

## WHAT IS A COMPANY'S BIGGEST SECURITY RISK?

Employees are the weakest link. According to Kevin Mandia, Chief Executive of Security at Mandiant Corporation, "the security gap is end users". Today we make ourselves easy targets by posting troves of information about ourselves and our jobs online. Blogs and professional networks such as LinkedIn are particularly useful sources for criminals, since many people share details about their roles at work, which can be used to help determine corporate hierarchies, among other things. That makes it easy for a hacker to whip up, for example, a message that is purportedly from the target's boss.



With LinkedIn profile information, hackers "craft cunningly believable emails that users will have a high probability of clicking on" says Dave Jevans, chairman of security company, IronKey, Inc. Hackers include dangerous traps in targeted emails, such as links leading to malware or a Web page designed to dupe the employee into entering passwords. These attacks are also known as "phishing", those often oddly worded emails that purport to be from a bank or the IRS that we have learned to ignore. The new generation of emails called "spear phishing" is harder to spot. They not only lack telltale errors like typos, but often also include the names of colleagues and company-specific lingo, and they may be sent from colleagues' email accounts without their knowledge.

*— continued on page 3*

**Contact Hyder & Associates To Solve Your Records Management Problems**

HYDER & ASSOCIATES
MANAGEMENT REPORT
501 W. Glenoaks Blvd., Suite 422
Glendale, CA 91202
(818) 507-0008
FAX: (818) 547-9908
E-Mail: hyder@HyderAndAssociates.com

**27th YEAR ANNIVERSARY**