



So much for secure storage

By Jon Oltsik

http://news.cnet.com/So-much-for-secure-storage/2010-1015_3-5182004.html

Story last modified Wed Mar 31 04:00:16 PST 2004

With information security figuring so prominently in the headlines, you might assume that people in their right mind wouldn't still ignore security. But examine the latest goings-on in the storage industry and you'll trip across a very different reality.

The storage gang finds itself in a post-bubble state of euphoria over an initiative called information lifecycle management (ILM). Simply defined, ILM provides storage devices with application and business intelligence rules and policies to improve information management, automate mundane tasks and cut expenses.

A high-priced ILM infrastructure obviously does not deliver much value when no one can access information.

You want to access, backup and archive critical pieces of corporate info? No problem; ILM will automate the whole process.

This sounds like a great idea until you realize that the ILM vision completely minimizes any notion of security. Ridiculous, but true. Examine any slide in a vendor's ILM presentation and you're likely not to see the word "security" anywhere. This is a serious oversight.

You would think that any discussion on information lifecycle management would by definition include information security. But when storage guys talk about security, the discussion usually defaults to data protection technologies like backup or disaster recovery. So security-related issues such as antivirus, content filtering, intrusion prevention or digital rights management trigger blank looks.

Isn't it about time to wake up and smell the polymorphic worm-infested coffee?

Suppose that ILM becomes reality and a network of ILM servers control and manage critical information throughout the enterprise. A hacker couldn't ask for a richer target. Stealing intellectual property for extortion or industrial espionage would no longer require time-consuming snooping or risky server break-ins.

Rather, if the bad guys can compromise the ILM servers, they can gain access to oodles of valuable corporate information in a single attack. This is a serious problem. According to the 2003 survey conducted by Computer Security Institute (CSI) and the Federal Bureau of Investigation, theft of intellectual property caused a greater financial loss than any other type of security incident. Without ILM security, the study's numbers ought to skyrocket.

A disgruntled employee intent on causing disruption to a business would simply launch a denial-of-service attack against the ILM network and take the corporate information offline preventing access to data. Not to belabor the obvious but a high-priced ILM infrastructure obviously does not deliver much value when no one can access information.

The nightmare scenario features an ILM logic bomb that corrupts random files on a regular basis over several months. It would slowly damage more and more business information, and a lot of important data would get wiped out by the time the attack got discovered. Because this kind of attack would have lasted so long, the backups would be useless and result in days--if not weeks--of downtime. Users complain when the e-mail system is down for an hour. Imagine what customers would do when the ILM infrastructure is offline for a week. Better have the lawyers ready.

**Why has the
storage industry
dropped the
security ball with
ILM?**

There are other fundamental ILM security shortcomings, such as the lack of any plans for strong authentication, data encryption, key management, information access and usage policies. I could go on all day, but you get the point.

Oddly enough, while the storage folks have co-opted the ILM moniker for automated storage, the term has also gained popularity within a security niche called enterprise Data Rights Management (eDRM). Vendors like Authentica, Liquid Machines, Tablus and Verdasys enforce controls on information to prevent would-be sleazebag employees from saving the top-secret product plans to CD-ROM and selling them to a rival. This seems like a pretty important part of information lifecycle to me. Might not be a bad idea for the storage and eDRM guys to get together and kibbitz about a joint future?

Get Up to Speed on...

[Enterprise security](#) ▶

Get the latest headlines and company-specific news in our expanded GUTS section.

Why has the storage industry dropped the security ball with ILM? History shows that these specialists are used to dealing with data, not information. But what about the human-readable information a few rungs up the technology stack that represents a company's intellectual property? This is the stuff that ought to be protected with the digital equivalent of padlocks, surveillance systems and armed guards.

If the storage industry wants to succeed with ILM, it can't any longer dance around security. Users won't incorporate technologies that put their critical intellectual property at risk. ILM is a nascent concept, so there is plenty of time for vendors to get it right. That means support for security along with the development of products that store, backup *and* secure critical information.

But if they continue to ignore security, it's highly likely that ILM will wind up DOA.

[Copyright](#) ©1995-2008 CNET Networks, Inc. All rights reserved.