sageza

Market Roundup
July 26, 2002

Industrial Light and Magic Deploys 600 Intel-Based Workstations
More Security FUD
HP Erases Dell Printer Deal
Above the Law (That Applies to Others)

Industrial Light and Magic Deploys 600 Intel-Based Workstations

By Charles King

Industrial Light and Magic (ILM), a division of LucasFilm, revealed that it has purchased and deployed 600 Pentium 4-based animation workstations running Linux, continuing the company's planned migration away from SGI RISC-UNIX workstations to Intel-based systems. ILM began using Intel-based systems on *Star Wars: Episode II — Attack of the Clones,* and continued with *Men In Black II* and *Minority Report.* In addition, ILM is using Intel-based systems in the development of *Star Wars: Episode III, Harry Potter and the Chamber of Secrets, The Hulk,* and *Terminator III.* According to Intel, its systems are currently being used for animation and special effects work by studios including DreamWorks, Weta Digital, Walt Disney Pictures, Digital Revelations, and Sony Pictures Imageworks. In addition, several of these studios have announced plans to either employ or evaluate Intel Itanium-based systems for future projects.

ILM's deployment of 600 Intel-based workstations offers yet another example of how things have changed (and will continue to do so) as what were once considered lower-end, commodity-based, largely consumer products develop capabilities that allow them to enter and compete in increasingly higher-end markets. From a historical standpoint, the animation and special effects space has long been dominated by SGI, whose RISC-UNIX based products played pivotal roles in virtually every special effects masterpiece (or monstrosity) produced by Hollywood over the past decade. SGI's dominance began to slip a bit, however, as the enthusiasm and deep pockets of gamers and game developers drove the creation of PCs with increasingly powerful graphics engines. As those high-octane graphical capabilities accelerated and matured, coupled with the ongoing evolution of Intel's processor family, it was only a matter of time until Intel-based products could offer price/performance qualities that caught Hollywood's attention.

Does this mean that RISC-UNIX-based products are over the hill and gone? Hardly. While Intel-based products have found places on special effects desktops and in rendering farms, most studios still use RISC-UNIX machines for more precise final animation work. SGI and other RISC-based graphics vendors may not be flat on the mat quite yet, but we expect the migration of commodity-based platform products to continue upward in the special effects biz, with Intel's Itanium processor family members gaining increasing ground in server installations and final rendering systems. Overall, we see ILM's announcement as a PR-laden win for Intel and Intel-based product vendors, a painful black eye for SGI and a warning to other RISC-based graphics aficionados that Hollywood is not likely to remain as friendly a town as it once was long, long ago and far, far away.

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144
Amsterdam +31 (0) 35·588·1546

More Security FUD

By Jim Balderston

The Business Software Alliance (BSA) announced the results of a survey it conducted earlier this year in which some 600 IT professionals were asked about U.S. business security and the chances of cyber attacks on enterprises in the wake of 9/11. According to the survey, 62% say the risk of a major cyber attack on U.S. businesses has increased since 9/11, and 47% believe that a major attack will occur in the next twelve months. At the same time, the survey indicated that 58% of IT professionals believed that U.S. businesses' ability to defend themselves against attack had increased, but that 45% thought that are not prepared for a major attack today, despite improvements. The survey also notes that IT pros believe there is a gap between threats and ability to defend against them, and that the gap has either remained the same or grown since 9/11. The survey also found that 71% of IT professionals said enterprises should spend more money and time defending against major cyber attacks than they did in proofing themselves against Y2K glitches. The survey also listed what enterprises are doing, including the installation of antivirus software, firewalls, etc. In a press release accompanying the study, BSA representatives urged that the Congress include network security as part of the Homeland Security initiatives underway in Washington, citing risks to power grids, emergency communications systems, and financial systems.

Enough is enough. This relatively unremarkable survey — noting that vague and undefined security concerns remain on IT professionals radar screens — is being touted as a warning that the U.S. government better up its commitment to "cyber" security lest evildoers take advantage of the Internet and shut down power grids or unlock dam floodgates, or the like. In our mind, this is just the kind of FUD that makes The Little Boy Who Cried Wolf look like a piker. In many ways, this type of effort goes beyond simply self-serving and into the realm of irresponsible.

Let's take a look at the survey itself, for a moment. In a rather ambiguous way, it attempts to link ongoing concerns with IT security with the 9/11 attacks, and implies that evildoers have somehow increased their ability to do harm to U.S. business interests. What the survey really says is that some IT pros believe the risk of some sort of attack is higher than it was before 9/11. One suspects that any survey asking a security question — be it physical or electronic — would elicit a similar response when coupled with the events of 9/11. The survey offers no data beyond IT personnel beliefs. Furthermore, the study offers no definition of "major" when describing a possible attack, only that respondents express concern about it. The survey also illuminates the obvious: IT security gets better every day, but is not where it should be and gaps remain — or grow in slowing economies — just as they did before 9/11. All of which is not to say that information and communication systems security is unimportant. It is and remains so. But addressing questions like national infrastructure security should be done in a level-headed, rational fashion that does not conjure up images of children's fairy tales.

HP Erases Dell Printer Deal

By Charles King

Hewlett Packard announced this week that it has discontinued its agreement to supply HP printers, cameras, and scanners to Dell Computer. According to news accounts, HP stated that the basis for the two companies' relationship was invalidated by Dell's plans to sell its own Dell-branded printers. Speculations regarding those plans arose in May 2002 as the result of a Bear Sterns research report. Dell has claimed that it is still evaluating its options, but last week company president Kevin Rollins stated in an interview with the Austin *American-Statesman* that the company would likely introduce a Dell-branded printer by the end of 2002. Dell began selling HP products in 1998.

Depending on one's point of view, HP's decision to step away from its relationship with Dell qualifies as a mere temper tantrum by a company besieged by its ablest competitor or a practical strategic move by a company in the midst of reinventing itself after completing a remarkable merger. Tantrum fanciers are likely

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144
Amsterdam +31 (0) 35·588·1546

to point to the PC market where, depending on whose projections you believe, HP currently holds a solid lead (due to the Compaq merger) or a nominal lead, or is tied neck and neck with Dell, which vaulted into the lead a few months before the merger. To these folks, HP's decision is an essentially hopeless gesture that will do little to slow the inevitable ascendancy of Dell back to its primary position in PC sales. Those who favor the practical strategy scenario would likely claim that HP is simply playing the game smartly and aggressively. The printer deal made sense at one point, but Dell's decision to bring their own name-brand printers to market (along with their less than adroit strategic footwork in concealing their tracks) gives HP little choice but to step away. Some might suggest that every sale is a good sale, but this notion is outweighed (apparently in HP's mind, anyway) by the inherent dangers of sustaining your enemy while he is preparing to attack you on a new front. Beyond the basic drama of the announcement, two things are certain. The loss of Dell's sales of HP printer will do little to dent HP's commanding lead in printer sales, and the loss of HP should not impede Dell's ability to sell PC/printer packages, since one presumes printer vendors including Lexmark, Epson, Xerox, and Canon are ready and waiting to take up the slack.

That said, should HP's desertion of Dell be considered little more than a tempest in a teapot? More like a message in a bottle, from where we stand. In the heady days prior to the HP/Compaq merger, we wrote that one benefit of the deal would be HP's unique ability to develop and deliver integrated computing and imaging packages for both consumer and business customers. That may seem a minor issue to some, but to our minds as PC's and related devices become increasingly commoditized, vendors who are able to offer customers complete product sets and one-stop support services stand to reap long term customer loyalty and financial benefits. We expect that this concept is at the heart of Dell's decision to jump into the printer business, but at this juncture HP is the only vendor that can seriously ponder or deliver such offerings. From that standpoint, HP's decision to discontinue its relationship with Dell makes perfect sense, since doing so plays to its own strengths and illuminates its chief rival's weaknesses.

Above the Law (That Applies to Others)

By Jim Balderston

Congress will consider new legislation that would allow copyright holders, specifically the music and movie industries, to actively disrupt peer-to-peer networks and disable PCs involved in violating copyrights, while granting them immunity from state and federal laws governing such behavior. According to published reports, the proposed legislation — authored by Representative Howard Berman (D-CA) and Howard Coble (R-NC) — would allow copyright holders to perform hacking activities if they have a "reasonable" basis to believe that file swapping of copyrighted material is taking place. The proposed legislation states that copyright holders must give the Attorney General's office a complete description of what measures it intends to take to disrupt P2P networks, but such descriptions will remain secret. The bill also reportedly limits the amount of damages individuals can recover through lawsuits if the hacking activity damages their computers or data stored therein. Lawsuits would only be allowed if approval was granted by the Attorney General, according to reports. The bill is expected to be taken up later this year.

As more and more details of the music and movie industries' legislative lobbying efforts come to light, we find ourselves more and more dumbfounded by their obvious desperation in the face of new and evolving consumer habits. While the industry takes baby steps forward to embrace new revenue models — like offering back catalogue tracks for download on subscription service websites — they take giant leaps backward in an effort to protect a distribution model that may be largely made irrelevant by the Internet and changing consumer behavior. This legislation — prompted and wholly supported by the entertainment industry — is such a step. A more sanguine approach, we believe, might include offering more content online, whether in subscription download models, pay-per-view/hear, or for free. This would surely decrease the incentives for piracy. Such a move should also be coupled with retail price cutting for hard copies of titles. Such is the stuff of "paradigm shifts" and inflection points. The entertainment industry has the right to protect copyrights, but it will be force by the market, not by legislation, to deal with the realities and opportunities that technology brings.

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144
Amsterdam +31 (0) 35·588·1546

This particular legislation recognizes none of these changes. The mind reels at the possibilities for abuse. Not only will all actions be largely secret, but consumers who are inadvertently damaged by industry hacker actions will have little or no recourse but to lump it. Corporate self-governance has proven to be largely a failure in the marketplace, and we have no reason to believe that somehow the entertainment industry will rise above the temptations of unfettered freedom to mess with any and everyone they have the slightest suspicion of possessing or sharing copyrighted material. While supporters of this legislation continue to argue that technology-driven theft must be fought with technology, we still must point out that law enforcement and prosecutorial behavior — including the disabling or damaging of another's property — has traditionally lain in the hands of law enforcement agencies who serve under some level of public oversight. Of course, the Law of Unintended Consequences is sitting eagerly around the corner, just waiting for the industry to go out and harass millions of moderately dissatisfied consumers, turning them into an angry consumer movement that will have ever-increasing technological tools within their reach. In such a future, we suspect P2P networks will end up the least of their worries.

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144
Amsterdam +31 (0) 35·588·1546