Technology Brief...

February 1, 2011

J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA
www.jgoldassociates.com +1-508-393-5294
Research, Analysis, Strategic Consulting

INSIDE THIS ISSUE

Intel's Billion Dollar "Oops"!

Intel announced that it has temporarily stopped shipment of its companion chipset to its newly released Sandy Bridge processors, which have only been in-market for about a month. While this is a costly "faux pas" for Intel, we expect it to have a minor affect overall on the success of Sandy Bridge, and it should not be seen as a major competitive advantage for AMD processors. And while it presents some problems to system manufacturers, they should be able to recover quickly with little damage.

Intel discovered a manufacturing flaw in its Cougar Point chipset, which is responsible for I/O processing for Sandy Bridge. It was discovered when Intel received a few returns from OEMs and tracked the problem to a process issue. The problem affects a relatively small portion of chips (5%-15%) and manifests itself over a period of time through reduced SATA port performance on 4 of the 6 ports available on the chip. This translates into potentially slow disk reads and writes that significantly slow overall system performance, or even failure to connect to the drive causing the system not to be able to boot. Intel is able to fix the problem through a change in the top metal layers of the chip, and says it is not a fundamental design flaw but a processing issue. This is far easier to resolve than a chip design issue, and allows Intel to save a large number of wafers already in the production pipeline.

"…Intel announced that it has temporarily stopped shipment of its companion chipset to its newly released Sandy Bridge processors … Intel has found the flaw early in the product life cycle and has taken the proper steps to resolve the problem for its customers...."

Intel is erring on the side of caution by halting all shipments until the process enhancements to the chip are completed and the problem is solved. It means that manufacturers of next generation i5 and i7 processor based system will be required to stop current manufacturing, and also deal with warranty replacements, as Intel has indicated it will replace any existing systems with the new chipset when it starts shipping in about 4 weeks. It will delay shipments of Sandy Bridge systems from the systems vendors by 6-8 weeks. It also means that Intel's mobile version of Sandy Bridge will slip out by about 2 months delaying releases of next generation notebooks. For those vendors who don't want to delay system deliveries, there are older chipsets that can be substituted for Cougar Point. However, we advise waiting for the Cougar Point shipments to restart as the improvements available with the newer chip sets offers a major performance advantage.

There is no doubt this is a costly mistake for Intel. They estimate it will cost them about $1B ($300M in chip costs, $700M in HW repair/replacement reimbursements to the OEMs). But it would have been far more costly (both in dollars and market share) had this problem been found in 3 months or 6 months

when many more systems had been shipped, rather than now when Sandy Bridge systems are in the early delivery stages. And to its credit, Intel decided to tackle the problem up front for all users, rather than wait for the failures to trickle in over time and fix them on an ad hoc basis.

Bottom Line: While it's never a good thing when your hot new product is found to be defective, we believe Intel has found the flaw early in the product life cycle and has taken the proper steps to resolve the problem for its customers. Even though Intel believes of the approximately 8M Sandy Bridge units and chipsets that have shipped, only a small portion would exhibit the failure over an extended period of time, Intel is getting ahead of the problem now. This should offer customers some assurance that Intel is committed to providing the best chips it can, and not waiting for future failures to emerge. And it should significantly limit any potential for AMD chips replacing Intel product.

Learning from WikiLeaks: What Companies Must Do to Protect Themselves

Much has been written recently about the WikiLeaks disclosure of hundreds of thousands of sensitive government documents and cables. And despite a new method of distributing such massive amounts of information in this instance (via the web), should anyone really be surprised this happened? In fact, the whole WikiLeaks event speaks volumes about how truly un-serious the US government is about security (or worse, incompetent). This is not a new exposure area, as companies have been dealing with "data leakage" problems for years. And it's not as if there aren't lots of tools available that can track document access, allow only certain users to view/read/copy files, lock down repositories, etc. Security companies like McAfee and Symantec, and many of the major app platform vendors like RSA, Oracle, IBM, SAP, etc. have leakage prevention capabilities. Obviously, the Government ignored these capabilities to its detriment, and we believe many organizations large and small do so as well.

"…the Government ignored these capabilities to its detriment, and we believe many organizations large and small do so as well … Few enterprises look at leakage protection as an "inside job" challenge, and that is why it is critical that companies do more to eliminate this specific threat……."

The WikiLeaks event sheds light on a major security issue with huge implications for enterprises and not just for government agencies. The fact is that the highest probability of data loss or exposure will result not from an outside attack, but from inside your own organization. Indeed, right now the government thinks the leaked documents is the work of a single person – a US Army Private who was able to access millions of files and easily copy them to a CD or flash drive. And it's very likely that in your enterprise, there are many individuals who could easily access private and sensitive corporate data too, which of course is the companies' most valuable (and private) asset. In fact, it's amazing how lax data access rules are in most companies, despite the many regulatory compliance requirements (e.g., SOX, HIPAA). And if someone unauthorized did access sensitive files, would your organization even know about it?

There are steps enterprises should take to avoid being the next victim of WikiLeaks (which now says it will start releasing corporate documents as well). The most critical lesson to be learned from WikiLeaks is, trust your employees, but verify they are not doing something they shouldn't. The vast majority of employees will be ethical. But occasionally, there will be one that isn't and those are the ones organizations need to protect against, as best as is possible (nothing is 100% secure or foolproof).

Any assessment of corporate security/data protection policies should start with a number of questions. Does your company have written policies in place to handle sensitive documents? Have those policies been effectively communicated to employees? If your company hasn't, why not? Are certain areas of data/files restricted? Are automated tools in place to track document access? Is the most sensitive data encrypted so it can't be exposed? Are your employees aware of the penalties for unauthorized access or copying of files? These are just some of the components of a data protection plan that companies must create. Not having one is like leaving your front door unlocked.

Of course, that doesn't mean organizations shouldn't also be protecting assets from outside infiltration over the net. Clearly this is also a data leakage threat and there are many reported losses of data from malicious attackers. But most companies do a pretty good job of that through implementing firewalls (e.g., Cisco, Juniper) and effective segmentation of networks.

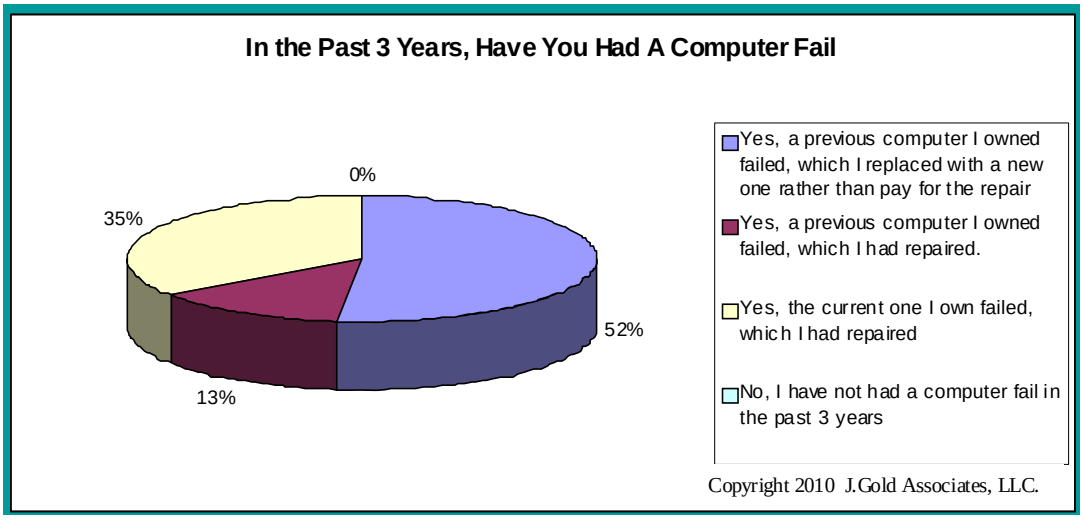
Bottom Line: Few enterprises look at leakage protection as an "inside job" challenge, and that is why it is critical that companies do more to eliminate this specific threat. This is the biggest lesson of WikiLeaks. And if your company doesn't already have a "data leakage" prevention plan, what are you waiting for?

Laptop Failures and Replacement – What Consumers Say

We recently surveyed 500 consumers for a study to assess whether they have had a laptop computer fail and what they did if such an event occurred. We asked a number of questions to gather a variety of data points, including if the broken laptops were repaired, how much they spent on repairs or a replacement, how long it took, what vendors' products they purchased, was data lost, how much effort it took to get a new machine running again, etc. Below are two brief highlights from the study, including; whether a consumer had a laptop fail, and what was the motivation for purchasing a new device.

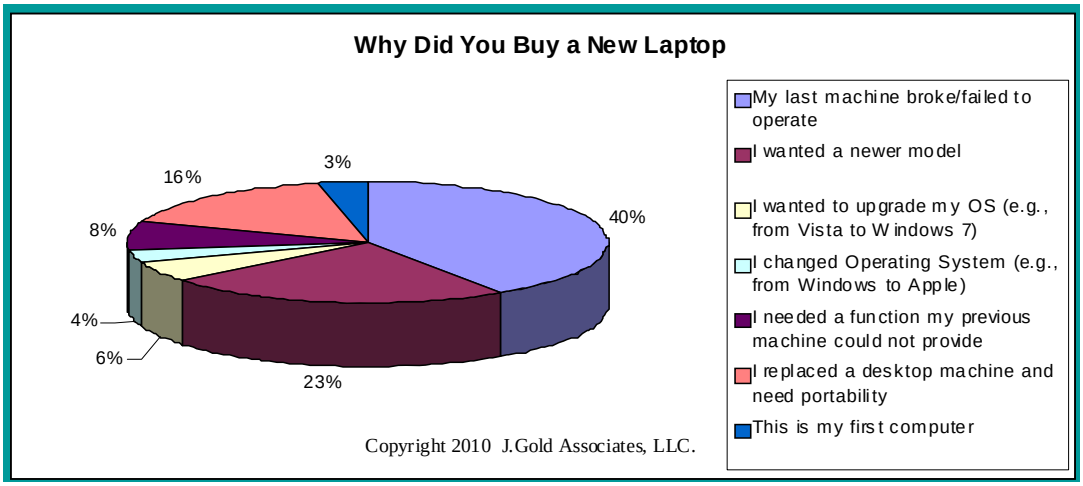
Figure 1 : In the Past 3 Years, Have you had a Laptop Fail?

"…We recently surveyed 500 consumers for a study to assess whether they have had a laptop computer fail and what they did if such an event occurred. We asked a number of questions to gather a variety of data points....."



This question assesses how many respondents have had a machine break/fail within the past 3 years. 52% indicated they had a machine fail and bought a new one rather than pay for the repair. 35% indicated that their current machine failed and was repaired.

Figure 2: Why Did You Buy a New Laptop



This question assesses the motivation for buying the current machine. The leading reason for purchasing a new machine is that a previous laptop failed (40%), followed by the desire for a newer model (23%).

Contact us for further information about this report and its conclusions.

J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

Research, Analysis, Strategic Consulting

Recent Research

Contact us if you would like to obtain any of the following research:

15 Emerging Technology Trends for 2011

- Highlights our key emerging trends for the coming 2-3 years

Commentary and Analysis

- Dramatic Changes Coming in Endpoint Security
- The Office Desk Phone is Dead!
- Tablets – Is It The Year of the Tegra?
- RIM's PlayBook Has An Air About It!
- Nokia Gets Qt
- WebOS – Is It Too Late To Matter?
- Windows Phone 7: The Winners and Losers

Technology Insights

- BlackBerry's Jam and RIM's Transformation

Technology Reports

- Solid State Drives in Notebooks: Cost Advantage or Cost Liability?
- Keeping Notebooks Past Their Prime: A Study of Failures and Costs