



## 2004-2005 IMATION DATA PROTECTION SURVEY

### *Key Findings*

Imation surveyed more than 200 IT directors and network storage managers of small-to-mid-sized companies on their perceptions of data backup, disaster recovery and storage practices and challenges. Following are the key findings from the survey. For a detailed survey report, visit <http://www.imation.com/dataprotectionsurvey>.

#### **Data Hosted on Laptops Presents an Overlooked Risk for Data Loss**

According to the survey, 40 percent of small and mid-sized companies polled rely on an extensive network of laptops for their employees. Even though the use of laptops in business is growing, 57 percent of companies hold the individual employee responsible for backing up data onto the company server. Two in five companies (42 percent) leave it up to the employee to determine what data needs to be backed up. Moreover, less than one-third (29 percent) of those companies use software to backup changed files to a corporate network.

#### **E-mail Viruses Remain Top Concern for Companies and Number One Reason Companies Review and Change their Data Protection Procedures**

According to the survey, e-mail viruses have had the most profound effect on data backup procedures. More than half (59 percent) of the companies surveyed reported that e-mail viruses are the number one reason they review and/or change their data backup procedures. And this is no small concern. According to McAfee Inc., a leading supplier of network security and availability solutions, more than 100,000 threats exist today and cost \$12.3 billion in damages last year alone.

Other top concerns prompting companies to evaluate their data backup procedures:

- Cyber attacks (31 percent)
- Natural disasters (28 percent)
- Terrorist attacks (22 percent)
- Government regulations (19 percent)
- Employee sabotage (17 percent)
- Homeland security issues (15 percent)

Despite these concerns, respondents said they are most confident in restoring data after accidentally deleting a two-day old file or after major power outage, and they have the lowest level of confidence in restoring "mission-critical" data after a regional disaster if their data center is unavailable.

(more)

**Regular Testing of Disaster Recovery Procedures Not Yet a Common Business Practice for SMBs  
– Leaving Companies Vulnerable to Potential Data Loss**

Clearly, businesses have become more proactive in protecting their digital assets. In fact, 71 percent of companies surveyed have a disaster recovery plan in place. But, when it comes to protecting data, if a company doesn't establish regular testing and review of those disaster recovery practices, they are leaving themselves vulnerable to significant risk. In fact, nearly half (40 percent) of small-to-medium-sized companies don't test their disaster recovery plan after each update. Unfortunately, 28 percent of companies admit they take a wait-and-see approach and test disaster recovery processes and people only "after a problem" occurs or "never" at all.

For more information, contact Mary Rawlings-Taylor, Imation Corp at 651-704-6796 or [mjrawlings-taylor@imation.com](mailto:mjrawlings-taylor@imation.com) or Matt Schwarz, Fleishman-Hillard at 612-573-3117 or [schwarzm@feishman.com](mailto:schwarzm@feishman.com).

###