EM IT Insight

by Jill Barson Gilbert

CAUTION: DATA AT RISK!

WHAT HAVE YOU GOT TO LOSE?

Newer, faster computers, the Internet, and a new generation of software applications have all contributed to a significant increase in the amount of data we store electronically each year. But when was the last time you backed up your data? If your answer is, "I can't remember" or "More than a month ago," then you could be putting your business at risk of data loss. Whether you're a sole practitioner or a member of a large organization, you should have a process in place to back up and recover business-critical data. This column considers ways to help environmental professionals understand and manage the risks associated with data loss.

DATA AT RISK

Within every business organization, data exist in a variety of forms. These include employee knowledge, hard copy documents, and electronic files. In addition, data reside within disparate systems, such as databases, office applications, e-mails, and business-specific software, more numerous than you might imagine. Further, some data sources may be accessible only to limited parties (e.g., files stored on a laptop computer) and, thus, not available to others who might need them. It is important to identify and manage the business-critical data within your organization. An organization may suffer negative consequences if any of these data were lost, ranging from a mild inconvenience to business interruption to regulatory agency fines.

If you've ever experienced a computer "crash," accidentally deleted a needed file, or suffered a power outage without first saving your work, then you can begin to understand the consequences of data loss. Common threats that could result in the loss of digital (i.e., electronic) data include natural disasters, accidents, theft, human error, network failure, hardware or software failure, and electrical outages. Each data source within your organization may be at risk of one or more of these threats. But don't despair—there are things every organization can do to help mitigate the risks associated with data loss. For example, storing data backup files offsite may reduce the risk of data loss due to the effects of a natural disaster such as earthquake or hurricane. Similarly, implementing even the most basic onsite security measures can help reduce the risk from theft. Employing preventive maintenance can help alleviate hardware failure and using uninterruptible power supplies may avoid the potential loss of data as a result of electrical outages.

When it comes to digital data loss, Bryan Bergeron, in his 2001 book entitled *Dark Ages II: When Digital Data Die*, suggests implementing a commonsense approach to managing

Tips for Protecti

- ✓Develop a written data backup and recovery plan—and follow it!
- ✓Test backup and recovery procedures—ensure that they work well for your organization.
- ✓Use storage media appropriate for the volume of data to be archived and for the organization's time constraints for backup and recovery.
- ✓Back up your backups—create multiple backups and store one copy offsite.
- ✓Consider offsite storage on a Storage Area Network (SAN) or other secure site.

risk. A reasonable strategy might be to determine what data are at risk and what they're worth, then use that information to determine the resources that should be applied to reduce the risk ("Why Your Digital Data Could One Day Disappear," *Harvard Business School Working Knowledge*, February 11, 2002).

THE VALUE OF DATA

What have you got to lose? Most important, what can you afford *not* to lose? The annual Toxic Release Inventory (TRI) calculations that took your company months to complete? Ten years' worth of groundwater sampling data? Agency correspondence? A presentation you worked on for more than a week? A document you started 10 minutes ago? Some data are more valuable than others, depending on the time and materials required to create them, the replacement costs, and, sometimes, sentimental value. For example, a printout of an environmental regulation that was downloaded via the Internet does not have the same value as, say, a 1-MB spreadsheet file stored only on your computer's hard drive. Some data are not worth recovering at *any* cost; other data are not worth recovering at *all costs*. But no data are priceless. The key is to identify the business-critical data.

ng Digital Data

- ✓Develop a document retention policy that includes electronic documents and data—and follow it!
- ✓Take proactive measures to protect data throughout its lifetime (e.g., virus protection, auto save features, supported hardware and software, reliable data storage media, frequent backups).
- ✓Maintain critical documents in a secure storage location—not as e-mail attachments.
- ✓Avoid keeping unnecessary data on file, such as preliminary calculations or drafts.
- ✓Perform periodic data audits to keep the amount of data being stored under control and manageable.

DATA RECOVERY PLANS

According to an article published in *Business Week* ("Everybody has More to Store," *Business Week*, October 28, 2003), the growth in digital data storage during the 1990s was 65–75% annually. With the emergence of Web-based computing, faster and bigger computer networks, and an increase in the use of electronic devices, this growth rate has now accelerated to 85–90% per year, and is expected to continue to increase at this rate. Even with the proliferation of companies that specialize in electronic storage and newer and cheaper storage solutions, how can one manage this degree of data growth? One way to manage your data growth and business risk is to develop an organization-wide data recovery plan.

Developing a data recovery plan can be thought of as a 10-step active process:

1. Identify and quantify the data at risk.
2. Determine the value of the data.
3. Identify and rank possible threats of data loss.
4. Determine the best way to mitigate the threats.
5. Determine resource requirements for backup and recovery.
6. Decide the value of archiving data (use return on investment as appropriate).
7. Identify data to archive or protect.
8. Back up (archive) selected data.
9. Take proactive measures to manage the risk of data loss.
10. Test, evaluate, and modify the process on a continual basis.

Organizations of all sizes have a lot to lose if they are unable to quickly recover lost data. Advances in technology can sometimes cloud the issues. With the Internet, faster and cheaper data storage methods, and storage service providers quickly replacing traditional data storage options, it is essential that organizations keep data growth under control and manage and protect their business-critical data. Taking the time to evaluate the degree of risk involved with data loss, as well as the associated mitigation measures and costs, is well worth the effort. Having a proven data recovery process in place is priceless.

About the Author

Jill Barson Gilbert, QEP, is president of Lexicon Systems, LLC. She helps organizations increase business value by designing and implementing EH&S management solutions that leverage technology. A respected author and speaker, Gilbert is past chair of A&WMA's Information Solutions Committee. She can be reached at *JBGilbert@Lexicon-Systems.com*.