CASE STUDY

United States Air Force

Lost! Crucial Data from Shaw Air Force Base

DriveSavers makes a priceless recovery

Data Loss Situation

Dean Johnson, systems administrator for The Civil Engineering Squadron at Shaw AFB in South Carolina, keeps the squad's 350 computers running smoothly. But, when a simple backup procedure failed, it jeopardized access to every file on the squad's 12-drive RAID server. That's when DriveSavers came to the rescue. The crash happened in stages and Johnson initially believed he could solve the problem himself. But, when the Adaptec system controller failed, he stopped his recovery efforts. "I knew that if I fired up a new controller and it started a new array, I could kiss my data goodbye." New backups had already begun to replace older ones, and three-quarters of the new files weren't backed up at all. At risk of permanent loss were archives for the base housing office—information that Congress mandates to be kept in perpetuity. Vital training data, including fire safety and flight readiness records were also gone. If not recovered, students would be required to repeat their training. After receiving a recommendation from a technician at Adaptec, Johnson contacted DriveSavers.

"If the data wasn't recovered, we would have been illegal in the eyes of our major command. And eventually, it could have gone up to Washington D.C."

~ Dean Johnson
Air Force Systems Administrator

Data Recovery Solution

Johnson described his system to DriveSavers engineers as a RAID 5 array, that would have allowed rebuilding of the system using data stored on a spare drive. However, when the drives were analyzed in DriveSavers ISO 5 certified cleanroom, they discovered it was actually configured as a RAID 0, with data striped across all 12 drives. This presented a more difficult challenge as the drives were mixed up in an unknown order; not as they were physically arranged in Johnson's original setup. When DriveSavers engineers finally unraveled the brainteaser, they recovered a full 45 GB of the most-wanted data. "The value of the recovered data far exceeded the cost of recovery," said Johnson.

We Can Save It!

DriveSavers is the worldwide leader in professional data recovery; serving government entities, businesses and universities. With SAS 70 Type II certification and a CISCO® Self-Defending Network, we offer the most secure data recovery environment available. Our highly skilled engineers, working in ISO-certified cleanrooms, consistently recover data that others have deemed "lost forever." Satisfied customers include: NASA, Department of Homeland Security, Department of Defense, Department of Energy, Bank of America, FedEx, Morgan Stanley and many more.

Protect Your Valuable Data

All organizations need to adopt strategies to ensure business-critical information is protected from corruption and loss. They also need a recovery plan to get up and running as quickly as possible in the event of system failure.

Best Practices to Avoid Data Loss

- Never upgrade any system without a verified backup.
- Use up-to-date hardware and software utilities for data security, such as firewalls and virus protection.
- Scan all incoming data, including packaged software, for viruses.
- Use ventilation, fans and/or air conditioning to keep servers at the proper operating temperature.
- Connect systems to an uninterruptible power supply (UPS) to protect against power spikes and blackouts.
- Power down and take extreme caution when moving computers.
- Avoid static electrical charges when touching or handling the media, especially in arid environments.
- Train users to report any unusual noises and power down immediately if a drive makes scraping, tapping, clicking or humming sounds.

When Disaster Strikes

- If possible, back up the data immediately.
- If the drive makes scraping, tapping, clicking or humming sounds do not use utility software.
- Do not power up a device that has obvious physical damage or is making unusual sounds.
- Shut down the computer to avoid further damage to the drive and its data.
- Do not attempt recovery yourself on severely traumatized drives (i.e., turning the computer off and on, using over-the-counter diagnostic tools), as this may cause further damage or permanent data loss.
- Configure another computer/server to temporarily replace the problem unit, restore available backups onto the new unit and reconfigure it as necessary to begin productive work.
- Contact DriveSavers for recovery advice. Because of the broad range of complex operating systems—such as MS Windows, Mac OS, Linux and UNIX—using utility software can potentially cause data loss.

Backup Strategies

- Invest in redundant backup systems.
- Establish a structured backup procedure using software compatible with the operating system and applications to make copies of all critical data files.
- Periodically test the backups to verify that data—especially databases and other critical files—are being backed up properly.
- Keep at least one verified copy of critical data off site.

Never Assume Data is Unrecoverable

DriveSavers has successfully recovered data from thousands of drives with extreme physical and logical damage. If you've lost critical data, DriveSavers recovery service is your best and safest option.

- SAS 70 Type II Certification
- Cisco® "Defense-in-Depth" Network
- Certified ISO 5 (Class 100) Cleanroom
- Certified Encryption Recovery Engineers
- HIPAA Compliant
- High Security Service Available
- GSA Schedule #GS-35F-0121S
- Cage Code: 04PC0
- Manufacturer Authorized
- All Media—All Storage Devices

Call a DriveSavers Data Recovery Advisor

- **800.440.1904**
- **415.382.2000**
- **www.drivesavers.com**

DRIVESAVERS® DATA RECOVERY