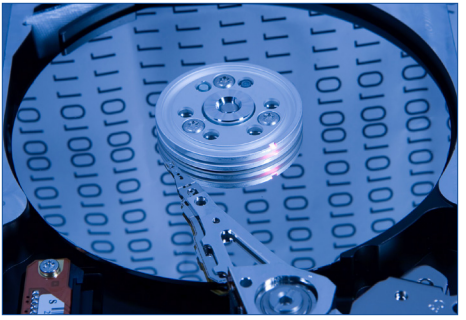

Ponemon INSTITUTE

Trends in Security of Data Recovery Operations

An independent study conducted by Ponemon Institute, LLC

"According to the Ponemon Institute's latest study among IT security and IT support practitioners, there is a lack of awareness among respondents about the importance of vetting data recovery vendors. Of the 87 percent whose organization suffered a data breach, 21 percent of them occurred when a drive was in the possession of a recovery service provider, an increase from 19 percent in the previous study. Respondents point to the provider's lack of security as the cause. Vetting of these parties is considered fair by only 30 percent of respondents and 9 percent say it is poor."

Source: Security of Data Recovery Operations Study

The following protocols are recommended by the InfoSec survey respondents. Before putting data at risk, make sure your data recovery service provider has the following in place:

Data Security Checklist for Vetting Third-Party Data Recovery Service Providers

- ☐ Vetting and background checks of all employees
- ☐ Training and awareness programs for employees to ensure sensitive and confidential data is protected throughout the data recovery process
- ☐ Proof of chain-of-custody documentation and certified secure network
- ☐ Proof of internal information technology controls and data security safeguards, such as annual SOC 2 Type II audits
- ☐ Proof of Certified ISO 5 cleanroom
- ☐ High security services adhere to U.S. Government security protocols
- ☐ Engineers trained and certified in all leading encryption software products and platforms
- ☐ Use of encryption for data files in transit
- ☐ Secure and permanent data destruction when requested or required

Download a complete copy of the Ponemon survey at:
www.drivesaversdatarecovery.com/ponemon