

(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 22 - September 2009

DIGITAL CERTIFICATES

THE NMAP PROJECT

TWITTER THREATS

CLOUD SECURITY

DATA RECOVERY



Is your data recovery provider a data security problem?

by Michael Hall



Today's IT security professionals enforce aggressive enterprise-wide security programs to minimize the risk of data leakage and a security breach. But, what happens when a hard drive fails (and, at some point, they all do) and it must leave the confines of the company's secure environment for data recovery? Who monitors the security protocols of data recovery service providers?

The unfortunate truth is that security protocols used by third-party data recovery vendors are not on the radar of either the IT security team or the IT support organization. Location or low pricing typically trumps data security during the vendor selection process.

Data loss must be a consideration anywhere personal and confidential data can be accessed. If your data recovery service provider's network is hacked, and confidential customer data is accessed, your company could be liable. To close the gap in security when a hard drive is out for data recovery, data protection policies and systems used by third-party data recovery vendors should be scrutinized carefully.

Data recovery is an invaluable service to users who cannot afford to be without their digital data for any period of time. It is also an in-

dustry that has grown exponentially since the introduction of the world's first hard drive. Twenty years ago, there were only a handful of companies that could provide this service reliably. Today, a search on the Internet under the term "data recovery" generates over 50 million results. Who among the 50 million are truly qualified to handle confidential data appropriately?

Among the handful of companies that pioneered the Data Recovery Industry twenty years ago, a few underwent security audits that cleared them to offer High Security Service to government agencies and branches of the military. In recent years, greater demands for data security began to rise from the corporate market segment and only one company continued to adopt new data privacy and protection protocols to meet them.

Not all data recovery companies are created equal

A 2008 Ponemon Institute benchmark study on the costs of data breach revealed this disturbing fact: 44 percent of the breaches experienced by U.S. companies occurred when third-party vendors were in possession of their data. Incidents of third-party breaches have risen steadily over the past four years and cost more than breaches by the enterprise itself.

Security breaches involving electronic data have come to light largely as a result of the California Security Breach Notification Act, which went into effect in 2003. Since then, numerous data security bills have been introduced in the 109th Congress.

Regulations in 44 states, the District of Columbia, Puerto Rico and the Virgin Islands require that individuals be notified when a breach of protected personal information occurs and their confidential or personal data has been lost, stolen, or compromised. Both the U.S. Senate and House of Representatives continue to evaluate federal laws regarding data privacy and breach notification.

Considering the rise in third-party incidents of data breach, and increasing regulations that place the blame of data loss squarely on the enterprise, IT security professionals must put data recovery service providers on their radar when assessing potential security breach pitfalls. A single third-party security breach could diminish a company's business reputation, customer loyalty, and ultimately their profitability.

New security standards for data recovery service providers

In 2007, DriveSavers published data security standards for the Data Recovery Industry. Many InfoSec professionals from Fortune 100 companies have incorporated these protocols within their own supplier/contractor security standards, and use them as guidelines during the vendor selection process.

Ask if your data recovery service provider adheres to these new standards:

1. Service provider's information technology controls and processes have been audited by accounting, auditing and information security professionals, and verified to be operating effectively to provide maximum data security.

Demonstrates compliance with auditing standards, such as the Statement on Auditing Standards (SAS) 70. Assures that every aspect of the facility and network is secure and suitable to protect personal and confidential data from being compromised.

Certified, control-oriented professionals, who have experience in accounting, auditing and information security, conduct an audit of the service provider's data hosting control objectives, activities and related processes over a period of time (typically 6-12 months).

The audit focuses on identifying and validating control standards that are deemed most critical to existing and prospective clients of the service provider, and covers all aspects of security in the facility; both network and physical.

Since the introduction of the 2002 Sarbanes Oxley Act (Section 404) following the Enron debacle, the SAS 70 audit has become the Corporate Industry Standard for an overall control structure.

SAS 70 Type I audit verifies the "description" of controls and safeguards that a service organization claims to have in place. The SAS 70 Type II audit verifies that all data hosting controls and objectives are actually in place, suitably designed, enforced, and operating effectively to achieve all desired security control objectives.

2. Network security testing and monitoring are integrated into the service provider's security program. Critical systems, (e.g., firewalls, routers, servers) are configured, maintained, and certified to be operating according to the organization's security policy.

A professional data recovery provider temporarily archives recovered data on their network until the customer has received it and verified its integrity. The need for strong, verifiable security measures is necessary to protect network assets, employee endpoints, and

sensitive customer data, such as e-mail servers, databases, and proprietary information. Every element of the provider's network should act as a point of defense. It must feature innovative behavioral methods that will automatically recognize and adapt to new types of threats as they arise.

Best in breed network security solutions allow for rapid response to emerging threats such as malware propagation spread by e-mail, SPAM, and botnets; phishing attacks hosted on websites; attacks targeting increasing extensible markup language (XML) traffic; service-oriented architecture (SOA); web services; and zero-day attacks that occur before antivirus companies have developed new virus signatures to combat them.

A comprehensive "defense-in-depth" approach to network security should, at minimum, include the following:

- Regular vulnerability assessments, penetration testing, and related reports
- Management of the network firewall, including monitoring, maintaining the firewall's traffic routing rules, and generating regular traffic and management reports
- Intrusion detection management, either at the network level or at the individual host level, intrusion alerts, keeping up-to-date with new defenses against intrusion, and regular reports on intrusion attempts and activity
- Mitigation support after an intrusion has occurred, including emergency response and forensic analysis
- Content filtering services, for electronic mail (i.e. email filtering) and other traffic
- Data archival.

3. Service provider is cleared to offer High Security Service that meets U.S. Government standards.

Government agencies, law enforcement bureaus, and other legal entities in the U.S. and abroad require third-party service providers to comply with the most stringent security standards and chain-of-custody protocols.

A professional data recovery service provider can provide documentation upon request that demonstrates how data is protected from

point-of-receipt at the facility, to point-of-departure.

All of the data recovery service providers' employees have undergone background checks, a tamper proof/resistant-shipping container is provided to the customer to protect the damaged storage device during transport, and a government-approved courier is used to ship the device to the service provider.

Chain-of-custody protocols should include:

- Use of a government-approved courier service
- Barcode on storage device is scanned upon receipt by data recovery provider
- Serial number is checked against information in customer record
- Date/time and name of employee who received the device is logged into customer record
- Customer is provided with notification that the device has been received, and data recovery process has begun
- Dates/times/and personnel handling the device are logged into the customer record as the device moves through the data recovery process.

Certain data loss situations require extra security procedures. The protocols for High Security Service include all of the above procedures, in addition to the following:

- Chief Information Security Officer available on site to receive the drive and customize security levels beyond those routinely provided
- Non-disclosure agreements are signed and chain-of-custody documentation is provided
- The data recovery is given top priority throughout the entire process and performed in a secure area, on a stand-alone system running only when an authorized engineer is present and monitoring the job
- Only approved personnel with proper access cards are allowed access to the area where the recovery is performed
- Custom solutions for data recovery on encrypted drives can be provided
- Data set is always stored in a DOD-approved safe Class 5 Mosler Safe during non-working hours
- Two separate copies of recovered data are shipped to the customer via two different

courier services

- Secure, encrypted electronic data transfer service is available, if required
- No copy of the data is kept on site after the recovery is complete.

4. Data recovery engineers have been trained and certified by leading encryption software vendors to properly recover data from encrypted files and drives.

In June of 2006, a Presidential mandate required all federal agencies and departments to encrypt data stored on their mobile computers and devices to mitigate the impact of lost or stolen data that could be used to distinguish or trace an individual's identity. The U.S. General Services Administration (GSA) then awarded Data-at-Rest encryption contracts to leading encryption software companies who were contracted to protect sensitive, unclassified data residing on government laptops, mobile computing devices and removable storage media devices. Data-at-Rest refers to any data residing on hard drives, thumb drives, laptops, etc.

There are hundreds of encryption tools out there and each one is unique. The professional recovery service provider has documentation that technicians have been trained by leading encryption software vendors, and are certified experts in multiple encryption recovery techniques. The provider can offer customized data recovery solutions that will meet stringent data security requirements when handling encrypted files and drives:

- Data is restored in an image-only format. Drive is returned with original encryption still intact
- Data is restored and decrypted at recovery facility to verify integrity of data. Data is returned encrypted or fully decrypted. Encryption username, password and/or key must be provided if this method is chosen
- Engineers are trained in proper handling of encryption keys
- A secure, encrypted electronic data transfer service is available upon request.

5. The service provider offers secure and permanent erasure of sensitive data, when requested.

Deleting files, emptying the recycle bin, or quick formatting a hard drive does not permanently delete data, it simply removes the information the hard drive needs to find the data, allowing it to be recovered. A wiping or erasing utility can be used to overwrite every sector of the hard drive with a pattern of binary 1's and 0's. A degausser approved by the National Security Agency, Department of Defense, the Central Security Service, and meets HIPAA and GLB Act privacy requirements is the best method to permanently erase classified or sensitive digital data stored on magnetic media.

Choose a data recovery service provider that is compliant with data security regulations

Government regulations and industry compliance statutes for security controls and data privacy, such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA) were created to protect personal and confidential data from unwanted breach and inappropriate use.

Leading enterprise IT managers and industry analysts are reinforcing the message that corporations must closely evaluate the data protection policies used with by third-party vendors. When a hard drive has crashed and professional data recovery is required, IT security and support professionals should choose a third-party service provider that can quickly and cost-effectively restore business critical data, and is verified to be in compliance with data protection and privacy regulations. Doing so will help them protect critical data from being compromised during the recovery process—and avoid the penalties, financial losses, and customer loyalty risks associated with a breach in data security.

Michael Hall is the Chief Information Security Officer for High Security Programs and Director of PC Engineering at DriveSavers Data Recovery (www.drivesaversdatarecovery.com). With over 13 years experience in data recovery technology focusing on high-end RAID arrays, he has successfully recovered data from over 12,000 failed storage devices. Hall supports DriveSavers corporate and government accounts with security protocols designed to meet their criteria.