

Closing an Overlooked Vulnerability

Agencies are often lax on vetting third-party data recovery vendors

BY HENRY KENYON | GCN STAFF

MANY GOVERNMENT and private-sector organizations consider recovering data from damaged laptop PC hard drives to be a minor budget item that third-party vendors can best handle. But a seemingly inexpensive fix could lead to compromised or stolen data, network breaches and other security nightmares because organizations typically do not vet data recovery vendors.

The National Institute of Standards and Technology has issued new guidelines to resolve that problem, but it will be at least a year before agencies are required to fully comply with it.

When recovering intellectual property or sensitive documents stored in damaged equipment, major security problems can arise if agencies or companies have not paid attention to vetting data recovery vendors, experts say.

The NIST guidance, which appeared as part of the institute's Special Publication 800-34 Rev 1, "Contingency Planning Guide for Federal Information Systems," represents a small part of the publication that covers the

entire breadth of data recovery procedures for federal agencies, said Marianne Swanson, NIST's senior adviser for information systems security.

The section about vetting data recovery vendors consists of a few sentences that state: "Organizations may use third-party vendors to recover data from failed storage devices. Organizations should consider the security risk of having their data handled by an outside company and ensure that proper security vetting of the service provider is conducted before turning over equipment. The service provider and employees should sign non-disclosure agreements, be properly bonded and adhere to organization-specific security policies."

NIST published the document, a revision to an older version, in June, and agencies have as long as a year to begin implementing its guidelines, Swanson said.

After NIST releases guidelines, the Office of Management and Budget can mandate them in its policies. If agencies are putting together a new system, they should use the new guidance, but they "don't have to throw away everything that they've done," she said.

The guidance was inspired by DriveSavers, a Novato, Calif., data recovery firm that conducted a survey that found that few, if any, federal guidelines covered the data recovery industry.

DriveSavers contracted the Reymann Group and Ponemon Institute, which surveyed 636 information technology security and IT support personnel who worked on

JUPITER IMAGES



data security and data recovery operations. The companies presented the survey's findings to NIST to highlight the security risks posed by sending equipment to unvetted vendors for repair and recovery.

Security should be the first criteria for choosing a data recovery company, but that consideration is often at the bottom of most organizations' priority lists, said Michael Hall, DriveSavers' chief information security officer. When an organization requests a data recovery, the decision to select a vendor often falls to help-desk or technical support staff members, who are instructed to recover the data as quickly as possible.

"That's what they base their criteria on — speed," Hall said. "They don't even bring into account the security aspect associated with speed. It's a bad way of going about things."

That inherent security problem was one reason the firm approached NIST to update the regulations.

Many organizations vet third-party vendors for IT support such as disaster recovery. But those judicious reviews often do not

extend to data recovery. Or if an inspection is done, it is not invoked at the right time, Hall said. Organizations should be vetting companies at the start.

"The first chance at a data recovery is the

"Best practices are best practices, and they should be adhered to across the board but particularly in a data recovery environment."

— MICHAEL HALL, DRIVESAVERS

best chance," Hall said. "They want to make sure that they're putting their information in someone's hands who is completely competent, qualified, safe and secure."

Hall noted that DriveSavers has received Defense Department approval to process information up to the top-secret level. In addition, DOD has listed the company as an approved organization, and all of the company's certification and information is available on its Web site. However, few customers have asked to vet the company, he said.

"When we get to the point where people ask to vet us, it's because there's a very conscientious security officer on the other side, and when they need a data recovery, he doesn't let the help desk handle it, he handles it himself," Hall said. "It starts from the top down instead of the bottom up as far as picking a data recovery vendor and what criteria should be adhered to," he said.

However, top-down participation in vetting data recovery vendors is an anomaly. Hall said the biggest security-related problem he sees is that organizations have inadequately small staffs and budgets. As a result, data recovery is often seen as the least-important problem, even though it could potentially compromise an organization. "Best practices

What IT Shops Want From Data Recovery Companies

The officers of DriveSavers had a suspicion that government agencies and other organizations rarely vetted third-party companies they contracted to recover lost data.

Why? Because DriveSavers knew that agencies rarely vetted the data recovery company's people.

The company, along with the Ponemon Institute, conducted a survey of 636 information technology security and IT support personnel, and the results confirmed the company's contention that a large number of security breaches are associated with third-party vendors, said Michael Hall, DriveSavers' chief information security officer.

The two companies presented

the survey's findings to the National Institute of Standards and Technology, which has prepared guidelines for improving the vetting process.

The survey also asked participants to develop criteria for vetting third-party data recovery vendors. The criteria include:

- Proof of internal IT controls and data security safeguards, such as compliance with Statement on Auditing Standards 70 Type 2 auditing. Organizations "want to know that the company that they're sending their information to can meet their compliance criteria," Hall said.
- Training and certification for data recovery engineers in all leading encryption software products and

platforms. Hall said that is important for state and federal government organizations mandated to provide encryption on portable devices.

- Proof of chain-of-custody documentation and a certified secure network. Potential customers wanted to know where their data was at all times, and they wanted to know that it was being stored on a secure network.
- Vetting and background checks on all employees of the data recovery company.
- Secure and permanent destruction of data when required.
- Re-encryption of recovered information so that it cannot be compromised when it is returned.

— Henry Kenyon

are best practices, and they should be adhered to across the board but particularly in a data recovery environment,” he said.

Paul Reymann, chief executive officer of the Reymann Group, agreed that vetting data recovery vendors is a low priority for most organizations. “This is a weakness or a sleeper risk in not only the overall information security program but in risk assessment methodologies,” he said.

Most information security policies and manuals don’t cover data recovery, Reymann said. Those publications might specify where to store data and how to manage the data, back it up and evaluate potential costs of recovering it after a disaster. “But they forgot that you don’t always back up data, and frequently someone will be in a position where their device fails and they have to go to a third party to recover the data. And that’s the sleeper risk — they didn’t really think about it.”

Reymann said unvetted repair and recovery operations might employ personnel with criminal backgrounds, which creates a potential risk for data loss. “It’s outside of the

existing information security program of the organization or federal agency because it is such a small item from a budget perspective,” he said. “It doesn’t get picked up.”

Reymann said he hasn’t seen third-party data recovery vendors listed as potential high-security risks that require vetting. “This is a perfect example of a low-profile, high-impact threat event,” he said.

Swanson said service guidelines exist to vet vendors that conduct various lines of business with the government, but she is unaware of any that specifically apply to data recovery vendors. She said many organizations that want some accreditation will hire a third party to assess data recovery vendors for compliance with the Federal Information Security Management Act or NIST Special Publication 853, a catalog of security controls and assurances that must be included in information systems processing federal data.

Although the new NIST guidelines are a significant step toward providing a vetting framework for data recovery vendors, stronger vetting standards are still necessary, Rey-

mann said. He said the screening and security process must be applied outside a traditional disaster recovery scenario to handle everyday problems, such as equipment failures. For example, many organizations will not enact a contingency disaster recovery plan if an employee’s laptop crashes the day before a major presentation, he said, adding that vendor vetting should be part of overall agency risk assessment policy guidelines and procedures.

Federal agencies that are seeking data recovery vendors can refer to the General Services Administration’s schedules. However, Reymann said, GSA does not conduct information security background checks. Agencies can also go outside GSA and submit a request for proposals for a vendor. Some vendors will complain that they cannot compete for government business if they must meet due diligence requirements. But Reymann added that although meeting FISMA requirements can be expensive, it is the cost of doing business with the federal government. ■