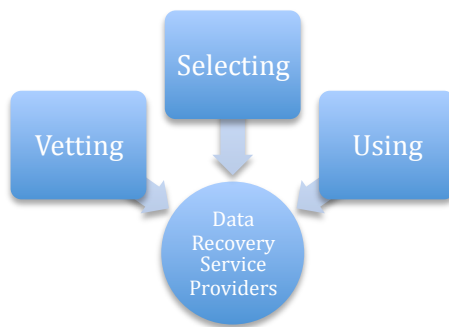


Just when you thought it was safe to tell your Board, external auditors, or examiners that you have a “no surprises” information security program in place, you don’t! There is a significant “sleeper risk” in the information security program of most organizations and government agencies that has been overlooked! It is a very small aspect of day-to-day operations in the scheme of the organization’s priorities, which is why it has gone unnoticed – until now. As one regulator commented to me recently, “this is not a potential problem – it is a real problem.” It can create a huge risk with a huge downside, if it is not controlled. Most organizations don’t even realize that this “sleeper risk” exists, until it is too late. The good news is that once you identify this “sleeper risk,” it is easy to fix.

“What is this sleeper risk?”

It is the lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers.



Data recovery and the use of third party service providers is a growing market. As a society, we continue to store more sensitive information in digital format. Organizations and individuals are using more storage capacity and various types of storage devices. It makes sense that as the demand for computer storage devices continues to rise, more equipment will be damaged or will fail due to daily wear and tear, physical damage, data corruption or natural disasters (flood, fire, etc.). If backup copies of lost data are not available, the need for data recovery services will increase to keep pace with the use of storage technology.

I don’t think that I need to explain the potential cost, fines, reputational damage, and loss of trust that an organization would experience if a breach of sensitive information occurred during the data recovery process or at any other time in the life cycle of sensitive information. It is huge!



“So why is this a sleeper risk?”

It is a matter of priorities and budget allocation. A typical security and compliance budget will allocate funds to protect people, information, and assets within the perimeter. Many companies and government agencies are also focused on protecting data on the inside of their organization from outside attacks. Kudos to these companies and agencies. Data recovery, however, frequently falls into a low priority category that doesn’t pop-up on the CISO’s radar or in an information security risk assessment. The need for data recovery is frequently associated with an immediate sense of urgency, e.g., the data contained on the damaged storage device must be recovered right away.

- Help Desk personnel or an office technician are usually tasked with the responsibility of selecting an outside third party vendor to recover the data quickly.
- Such third party vendors may or may not be listed on an approved vendor list.
- Frequently, the due diligence and selection process of such a vendor is limited to its financial stability, the cost of its services, and a fast “turnaround time”.

Don’t take my word for it. Lets look at an independent national study – Security of Data Recovery Operations – published by the Ponemon Institute in December 2009 and conducted among IT security and IT support practitioners. In this study, the Ponemon Institute confirmed that there is a gap in security guidelines when selecting data recovery service providers. Specifically,

- Sixty-four percent of the respondents decentralize the selection for data recovery vendors to the local level, e.g., Help Desk, while 24 percent are not sure how the vendor is selected.
- Sixty-nine percent of the respondents do not have or are unsure if they have a policy for ensuring the protection of data during the recovery process.
- Forty-nine percent say IT security is not involved in the selection process.
- Only 20 percent believe data security is a major selection criterion.
- Eighty-two percent say that it should be.

DriveSavers CISO Michael Hall noted that in conversations with other CISOs on the importance of considering data security when selecting a data recovery vendor, the first reaction of many is – “You are right! They think about it for a second and then propose that data recovery be mentioned in the organization’s business continuity plans, disaster

recovery plan, or incident response plans.” Perhaps some organizations have included data recovery security practices in such event-triggered plans. The challenge here is that it usually requires a material event to activate these plans. How many organizations do you know that would execute a disaster recovery or incident response plan to recover data from a failed laptop or storage device in the normal course of day-to-day activities?

Most organizations also have some additional backup and recovery procedures that overshadow the sense of urgency for more attention to data recovery practices on devices that were not backed up. In short, even with a strong backup recovery program, data recovery needs still arise. Seventy-nine percent of the respondents to the Ponemon study noted that their organizations have used or will continue to use a third-party data recovery service provider to recover lost data.

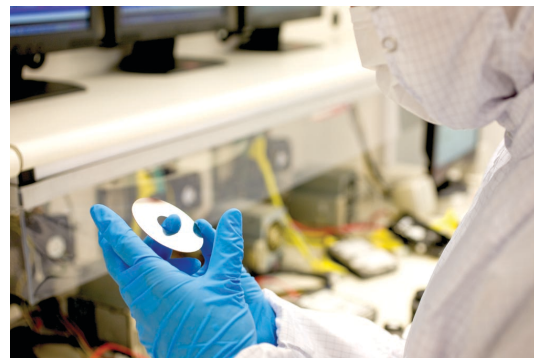
“What is the easy fix for this sleeper risk?”

Now that you are aware of this real problem, there is a simple solution that you can adopt to protect sensitive data during the data recovery process at your organization.

If you have a strong vendor risk management program, be sure to include ALL vendors that have access to sensitive data, including data recovery vendors. Mandated vendor management practices apply to all stages of the information life cycle. Specific to data recovery vendors, this includes:

- ✓ Pre-selection and negotiation of Master Service Agreements with appropriate vendors. These should be reviewed by a risk management committee and audited on an annual basis.
- ✓ Due diligence of all third party vendors (e.g., financial stability, client references, information security practices, etc.)
- ✓ Verification of the vendor’s security procedures to govern the transfer of devices and sensitive information.
- ✓ Proof of internal information technology controls and data security safeguards, e.g., ISO 27001 certification, NIST SP 800-53 Audit Report, FFIEC Service Provider Examination Report, BITS Shared Assessment Report, or SAS 70 Type II Audit Report (especially if the data recovery involves financial information). The appropriate certification and audit report will vary depending on the service provider’s client base.
- ✓ Proof of current training and certifications of engineers in all leading encryption software products and platforms.
- ✓ Adequate chain-of-custody documentation and network security.

- ✓ Vetted and performed background checks of its employees.
- ✓ Adequate procedures for the secure and permanent destruction of devices, when required.
- ✓ Capabilities for encryption of data files in transit and storage.
- ✓ Adequate clean room facilities, e.g., certified ISO 5 (Class 100).
- ✓ A security procedure for the analysis of the information and device upon return to the organization to ensure malware and other malicious software has not been loaded.



The lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers is not a potential problem – it is a real problem! Now that you are aware of it, it is one that you can easily fix.

#### About the Author

Paul Reymann is CEO, ReymannGroup. Mr. Reymann is one of the nation's foremost experts on regulatory compliance and information risk management. He co-authored the Gramm-Leach-Bliley Act Data Security Rule and several key regulatory directives and advisories on emerging risk management issues. He is a thought leader for simplifying compliance and security challenges in finance, healthcare, and other industries. You can always reach Paul at [paul@reymanngroup.com](mailto:paul@reymanngroup.com) or 410 956 7336.