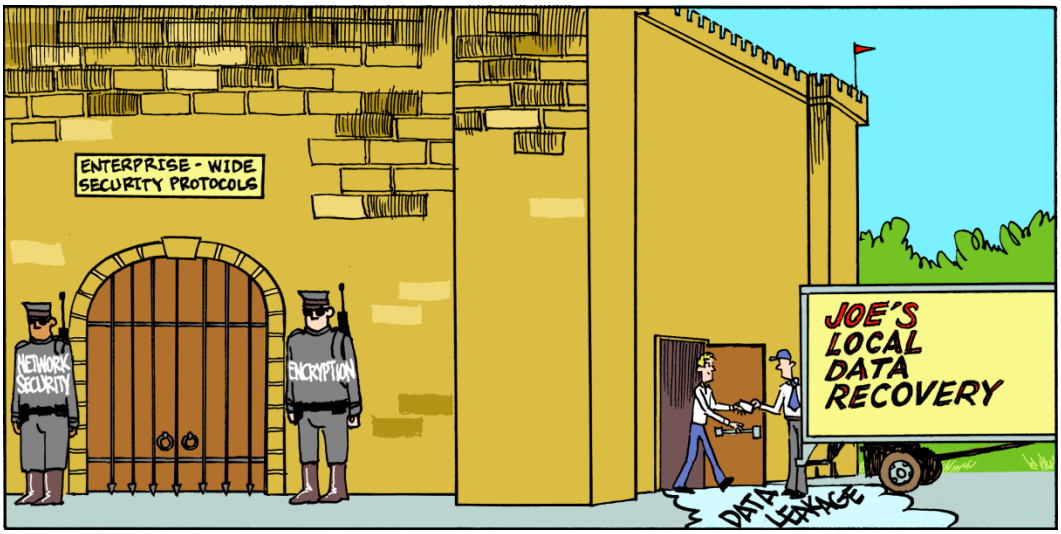
Data Recovery Service Providers:
The Low Profile, High Impact Risk to Enterprise Security



Lynda C. Martel
Executive Director, Government & Enterprise Business Relations
DriveSavers Data Recovery, Inc.

Gary R. Gordon, Ed.D.
Managing Partner
Bluewater International

January 2013

© 2013, DriveSavers Data Recovery, Inc.

Introduction

Robust risk management is a must in today's challenging environment of mounting digital attacks on vital corporate assets and the regulated data they are entrusted to protect. Most corporations have a dynamic layered security practice, which incorporates multiple security controls to protect this sensitive data. The reputational and financial consequences of lost or corrupted data require it. This white paper addresses an often undetected or unattended internal and contractual risk — data recovery — that appears to be an exception in an otherwise strong-layered security practice.

If a device fails, resulting in lost or corrupted digital data, few corporations have the internal resources to recover that data, especially in the case of a physical or electro-mechanical failure. The device must be sent to a data recovery vendor. These devices often hold critical IP, financial databases, accounting files, e-mail exchanges, customer records, PCI, PII and PHI. Therefore, data recovery organizations must be classified as high-risk vendors. However, most of the data recovery industry does not meet best practice standards to ensure data security. If a corporation does not perform due diligence before engaging the services of a data recovery vendor, it runs the risk of a data breach that will result in major financial and reputational damage.

A critical point is that C-level executives and board members in most cases have not planned for this exception. Therefore, IT personnel are left with the decision on how to resolve this problem. While they do the best they can, they are not aware of the high-risk issue associated with this process. In fact, they do not have the experience or training to understand the critical impact of the data leaving the layered security of the corporate facility, and potentially becoming subjected to negligence, fraud, abuse. Such an action could easily cost a corporation tens of millions of dollars.

The good news is that changes to internal policies and procedures, combined with contractual changes with third party businesses handling the corporation's data, will mitigate the risk posed by this exception that has been allowed to fall outside of the otherwise robust layered security protections.

Drives do fail. Data is lost. Data recovery vendors are being used at least once a week.

While most organizations have spent considerable time and resources managing risk in their information management lifecycle, a significant gap occurs when essential enterprise or regulated data is lost or corrupted. In this crisis mode, many organizations send devices to third party data recovery vendors without performing the proper due diligence, thus, exposing the organization to a potential breach. This disconnect, between the expectations of C-level executives and the corresponding IT practices, has created a security gap in the enterprise.

C-level executives believe that their organizations do not lose data, but if it is lost, the data is backed up, and that they do not send devices to third parties for data recovery. Data recovery industry revenue estimates would indicate otherwise.[1]

[1] The Data Recovery Services industry salvages computer files from damaged, failed, corrupted or inaccessible storage media. In 2012, industry revenue is estimated at $1.5 billion. The Data Recovery Services industry is highly fragmented and is dominated by small operators. The four largest companies in the industry accounted for less than 10.0% of industry revenue in 2012. Small- to medium-sized players in the industry make up the largest proportion of businesses.

© 2013, DriveSavers Data Recovery, Inc.

IT support practices indicate that data is lost, that it is not always backed up, and that they do send drives to third parties — in some large financial institutions as frequently as once a week.[2] Currently, the hiring of data recovery vendors is more often based on cost, turnaround time, and geographic location of the vendor than on risk exposure. Compounding this potentially high impact risk is the number of third party vendors handling the corporation's sensitive information, such as data backup and cloud computing service providers. Many of these providers do not have policies and procedures in place to mitigate the risk posed by data recovery. For example, when cloud storage service providers lose access to their customer's data, and hire a data recovery service provider to recover it, are they required to notify the party or corporation that owns the data that a loss event occurred? Even if the data were fully recovered, under some laws this scenario would still be considered a breach in data privacy.

Internet searches, as well as discussions with numerous corporate executives and trade association personnel indicate that there are few standards, regulations or best and reasonable practices in this area. Many of these standards and practices focus on third party vendors, but do not specifically address this security gap of sending failed drives with sensitive data out to third-party data recovery providers. Even heavily regulated industries have not addressed this issue through self-regulation, directives, or formal regulations.

Fortunately, closing this security gap and mitigating the risk can be addressed with policy and procedural changes that require little expenditure. It calls for policy changes concerning data loss caused by software corruption or storage device failure, training and guidelines for vetting and using data recovery service providers, and contractual changes governing how third party vendors handle lost or corrupted data.

System Failure and Data Loss — A Business Reality in Today's Digital World

Data loss is a common occurrence on single and multi-disk drive systems. Mobile devices, laptops and desktops suffer from user errors, viruses and malware, or physical and electro-mechanical failure due to accidental drops and bumps, age, and corruption. Even the best backup devices suffer these failures, and an increasing number storing sensitive data are being sent to data recovery vendors.

In-house and cloud data storage and backup systems are susceptible to data loss due to hardware failure, software problems, malicious employees and natural disasters such as fire, flood, electrical storms and power outages. Suppliers of data storage systems provide technical support and maintenance contracts that will cover the repair and/or replacement of failed hard drives, but they are not responsible for the lost data. Beyond common failures that plague every storage device, major data loss can occur if back ups are not regularly tested to verify the integrity of the data. Large databases, such as SQL, Oracle or Microsoft's Exchange email server, run some critical files open all the time (e.g., an individual user's email files). If the program has not been configured to back up open files, they will be skipped — sometimes, without regular testing and verification, for months. If the server crashes, when backups are accessed those open files will not be there.

---

[2] This is based on data recoveries performed by DriveSavers over the past five years.

© 2013, DriveSavers Data Recovery, Inc.

New devices operating with advanced storage technologies are making data recovery even more challenging for the enterprise. Smart phones, tablets and other storage devices based on solid state and NAND flash technologies are more popular than ever, but present a whole new set of failure issues and recovery challenges. While traditional magnetic data storage is well understood and reverse engineered with great success, solid state and NAND flash technologies are relatively new to the extremely competitive storage market. Their technological IP is highly protected. It is far more difficult to reverse engineer a recovery solution or to obtain cooperation, trust and proprietary recovery tools from the OEMs.

Multiple Data Recovery Vendors Used, Often Once A Week or More

Over 80 percent of digital data loss and corruption occurs due to the physical or electro-mechanical failure of a data storage device. In this data loss scenario, the device must be opened and parts repaired or replaced. Most corporations do not have the resources to recover the data internally.

In the 2012 Ponemon Institute study, *Trends in Security of Data Recovery Operation*[3], 769 IT security and IT support practitioners were surveyed. The majority of respondents either report to the Chief Information Officer or Chief Information Security Officer. Fifty-nine percent are at or above the supervisory level.

According to the study:

- 85 percent of the respondents report their organizations have used or will continue to use a third-party data recovery service provider to recover lost data. This is an increase from 79 percent in the 2009 study[4].
  - 37 percent use multiple third parties – 39 percent say they use third parties at least once each week or more.
  - 54 percent admit that IT security is not involved in the selection of third-party data recovery service providers.
  - Only 28 percent see data security as a main criterion for determining the adequacy of third-party data recovery service providers.

> *According to a 2012 Ponemon Institute study, 39 percent of the IT support professionals they surveyed use third party data recovery vendors at least once each week or more.*

- When rating their company's vetting process for selecting a secure data recovery service provider, only 9 percent consider it to be "Excellent" and 23 percent as "Good". A larger number, 25 percent rate their vetting process at "Fair", 11 percent admit it is "Poor" and 32 percent are "Unsure."

The Ponemon study respondents believe that their organizations are making decisions about vendors who handle the data recovery process based on advertised speed of service, successful rate of recovery and overall quality of customer service, rather than the vendor's levels of data security. As a result, data breaches are occurring.

- 87 percent of respondents report their organization has had at least one data breach in the past two years. (This is consistent with other Ponemon Institute studies about the prevalence of data breaches).

---

[3] Ponemon Institute, *Trends in Security of Data Recovery Operations, January 10, 2011*
[4] Ponemon Institute, Security of Data Recovery Operations, December 7, 2009

© 2013, DriveSavers Data Recovery, Inc.

- Of the 87 percent, 21 percent said the breach occurred when a drive was in the possession of a third- party data recovery vendor.
- When comparing this data with Ponemon's 2009 study, data breaches at data recovery vendors are trending up. In many cases, respondents cite the data recovery vendor's lack of security as the reason for the data breach

Current Standards, Best and Reasonable Practices, and Regulation

Governments around the globe are demanding that organizations monitor and take responsibility for the security of regulated data and the actions of their third party vendors handling that data. Examples of published standards, best practices, reasonable practices, and regulations include SOX, GLBA, PCI, PII, CA SBI386, CA AB 1950, MA 201 CRM 17.03, HIPAA and guidelines and directives from FDIC, FFIEC and the FCPA.

However, only a few specifically deal with data recovery vendors. Two examples are listed here: the first from NIST and the latter from the Shared Assessments Groups.

NIST SP#800.34 Rev. 1- Section 5.1.3, Paragraph #5 reads as follows:

"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."

Shared Assessments Group - SIG Risk Assessment Tool - Version 6 - Section G. Communications and Operations Management Section reads as follows:

G.4 Do third party vendors (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.) have access to scoped Systems and data? If so, is there:

G.4.1 security review prior to engaging in their services (logical, physical, other corporate controls);
G.4.2 security review at least annually, on an ongoing basis;
G.4.3 risk assessment or review;
G.4.4 confidentiality and/or Non-Disclosure Agreement requirements; and
G.4.5 requirement to notify of changes that might affect services rendered?

Closing the Security and Policy Gap

In order to close the identified security and policy gap noted in this white paper, the following five steps are recommended.

Step 1: Conduct Gap Analysis

The first step is to determine if this security gap exists within the organization. The responses to the following questions will assist in determining that.

- When a user's device, or a storage system goes down, are the failed drives being sent to a data recovery vendor? Under what circumstances?
- Is an incident report filed? Under what circumstances?
- Who chooses the data recovery vendor?
- Does the type of data to be recovered drive the vendor selection criterion?

© 2013, DriveSavers Data Recovery, Inc.

- What is the current audit and assessment processes for data recovery vendors?
- Are the vendor's security protocols vetted before engaging their services?

Step 2: Revise internal and external policies and procedures where needed.

If the gap exists in the organization, determine what internal policy, procedures, and practice need to be revised. The revised internal policies should be applied to all third party data recovery vendors who handle the organizations sensitive and regulated data. The contract modifications may be necessary for vendors to ensure they handle the corporation's data at the same level the corporation handles its internal data.

- Internal policies and procedures, business continuity, disaster recovery, and incident response plans should address the use of data recovery service providers.
- Policies and guidelines should be established within the enterprise for vetting a data recovery service provider.
- Criteria for selecting data recovery vendors and the required supporting proof should be specified (see Check List for Vetting Data Recovery Service Providers).

CHECK LIST FOR VETTING THIRD-PARTY DATA RECOVERY SERVICE PROVIDERS

To mitigate the risk of a breach, a reputable data recovery service provider should be able to provide documented proof of the following security protocols:

- ❑ Annual security audit reports (e.g., AICPA SOC 2 Type II) conducted by control-oriented third parties to verify that the provider's perimeter and network systems, data hosting control objectives and control activities are in place, suitably designed, enforced and operating effectively.
- ❑ Proof of compliance with data privacy and data security regulations such as:
  - SOX (Sarbanes-Oxley Act of 2002)
  - GLBA (Gramm-Leach-Bliley Act of 1999)
  - PII (Personally Identifiable Information) Privacy Standards
  - PCI DSS (Payment Card Industry Data Security Standards)
  - NIST (National Institute of Standards & Technology) SP 800.34 (Rev.1)
  - HIPAA (Health Insurance Portability and Accountability Act)
  - FERPA (Family Educational Rights and Privacy Act)
- ❑ Proof that all employees undergo vetting and background checks.
- ❑ Business Continuance Plan and Information Security Policy in place/reviewed annually.
- ❑ Certification of training in all leading encryption software products and platforms. Customized solutions for encrypted data recovery. Use of encryption for data files in transit. Lock boxes available upon request.
- ❑ Verification of qualifications to handle enterprise-class data recoveries.
- ❑ NSA- or DOD-approved process for the secure and permanent destruction of unwanted drives and data.
- ❑ Chain-of-custody documentation. Confidentiality and non-disclosure agreements.
- ❑ High Security Service that meets U.S. government protocols.

Step 3: Develop and operate enforcement mechanisms

Revising the policy, procedures, and practices to mitigate the gap is the first step. The following are required to ensure that the new policy, procedures, and/or practices are followed:

- Define documented and repeatable business associate risk management processes to address drive failure, data loss and the use of third party recovery vendors.
- Conduct mandatory annual security reviews of data recovery service providers.

© 2013, DriveSavers Data Recovery, Inc.

- Develop and deploy employee training and awareness programs to ensure sensitive and confidential data are protected throughout the data loss and data recovery process.
- Establish strong enforcement practices for failing to adhere to the organization's policies.

Step 4: Modify contracts with third party vendors to align with internal changes

Any internal changes to the policy and procedures regarding the use of third party data recovery vendors should be mirrored in contractual arrangements with high-risk third party vendors that handle the organizations sensitive and regulated data. In most cases, the vendor contract will have the necessary provisions but not call out the data recovery process. It is recommended that the criteria for selecting a data recovery vendor (articulated in the checklist) be used to amend these contracts.

Step 5: Ongoing monitoring of the third party data recovery vendors

Many companies have excellent vetting protocols outlined in their vendor risk management, business continuity and disaster recovery plans, but data recovery vendors may require some special consideration for ongoing monitoring. These performance-monitoring controls should include:

- Annual review of vendor's audit reports and certification documents to verify they are up-to-date.
- Assurance that the vendor is compliant with industry-mandated data privacy/security guidelines (SOX, GLBA, PCI, PII, CA SBI386, CA AB 1950, MA 201 CRM 17.03, NIST SP 800.34 (Rev.1), HIPAA, etc.).
- Annual on-site quality assurance reviews.
- Periodic analysis of the vendor's financial condition.
- Assessments of compliance with contract terms.
- Testing the vendor's business contingency planning.
- Evaluating adequacy of the vendor's training to its employees.
- Periodic meetings with the vendor to review contract performance and operational issues.
- Anonymous testing of vendor's service capabilities.

Conclusion

Data recovery service providers will play a greater role in the corporation's information life cycle, as the number and complexity of devices increase to facilitate the flow of information. Board members and C-level executives, in conjunction with senior IT directors, must work together to close the policy and security gap posed by the organization's need to engage data recovery service providers. The policy must address the internal guidelines and procedures first and then push them down through contractual modifications to all third party vendors who handle the corporation's sensitive data.

Given that there are no directives, standards, and best or reasonable practices, this paper provides a roadmap for mitigating the potential risk of data recovery. The solution to this high impact risk requires policy and procedural changes only and is low in cost. It insures that the confidentiality, integrity, and availability of the corporation's sensitive information are maintained during the data recovery process.

© 2013, DriveSavers Data Recovery, Inc.

About the authors:

Lynda C. Martel
Executive Director, Government and Enterprise Business Relations
DriveSavers Data Recovery, Inc. (http://www.drivesaversdatarecovery.com)

Lynda Martel is responsible for developing and implementing the company's strategic data security initiatives. She advises business partners and external audiences on the company's data security/privacy protocols. Martel meets often with regulatory authorities on matters that require new or revised data recovery industry guidance. She serves on the steering committee for the Shared Assessments Group and was co-chair of the ecosystem subcommittee for ANSI's (American National Standards Institute) data protection project. She is a member of HDI, a professional association for IT support professionals, HIMSS, a healthcare information and management systems society, the American Banker's Association and the Ponemon Institute's RIM Council, a select group of privacy, security and information management leaders.

Martel works with leading research groups and organizations to help develop and publish research projects and white papers related to security, healthcare and data recovery. She participated with ANSI in a series of speaking events before the U.S. Congress and the National Press Club to educate the healthcare industry on cause/prevention of protected health information (PHI) data breach. She has spoken at various industry events in the U.S. and conducted training on ways to mitigate the risk of breach when using third-party data recovery service providers.

Gary R. Gordon, Ed.D.
Managing Partner, Bluewater International (http://www.bluewaterintl.com)

Dr. Gordon is a managing partner at Bluewater International, a leading growth management and investment company headquartered in Washington DC. He leads Bluewater's strategic client group.

Dr. Gordon is one of our nation's leading security experts and thought leaders and has developed first of a kind innovative educational programs and training, conducted cutting-edge applied research to understand critical societal problems, and advised leaders in Fortune 500 corporations and governments. He has over three decades of experience addressing the emerging trends and the evolving challenges of economic crime, fraud and abuse, risk management, identity management, terrorism and cyber security. He founded and led three national level public/private partnerships comprised of federal law enforcement and government organizations, major financial service, identity management, and cyber security corporations, leading universities, and non-profits. His thought leadership and development of key partnerships have provided partners and clients with insights and guidance in risk management, information sharing, policy development, privacy, managing regulations, and governance issues.

Dr. Gordon possesses an exceptional ability to study emerging trends, forecast future challenges, and put processes in place to solve them. He is a leading expert speaker who has made numerous domestic and global presentations. He holds a doctorate in Counseling Psychology with an emphasis on organizational change from Boston University. His master's degree is in Criminal Justice from the University of New Haven, and his bachelor's degree is in Psychology from Clark University.

© 2013, DriveSavers Data Recovery, Inc.