CYBERSECURITY REPORT

The Overlooked Risk in Third-Party Data Recovery

"Robust risk management is a must in today's challenging environment of mounting digital attacks on vital company assets and the regulated data they are entrusted to protect."

This white paper addresses an often undetected or unattended internal and contractual risk—data recovery.

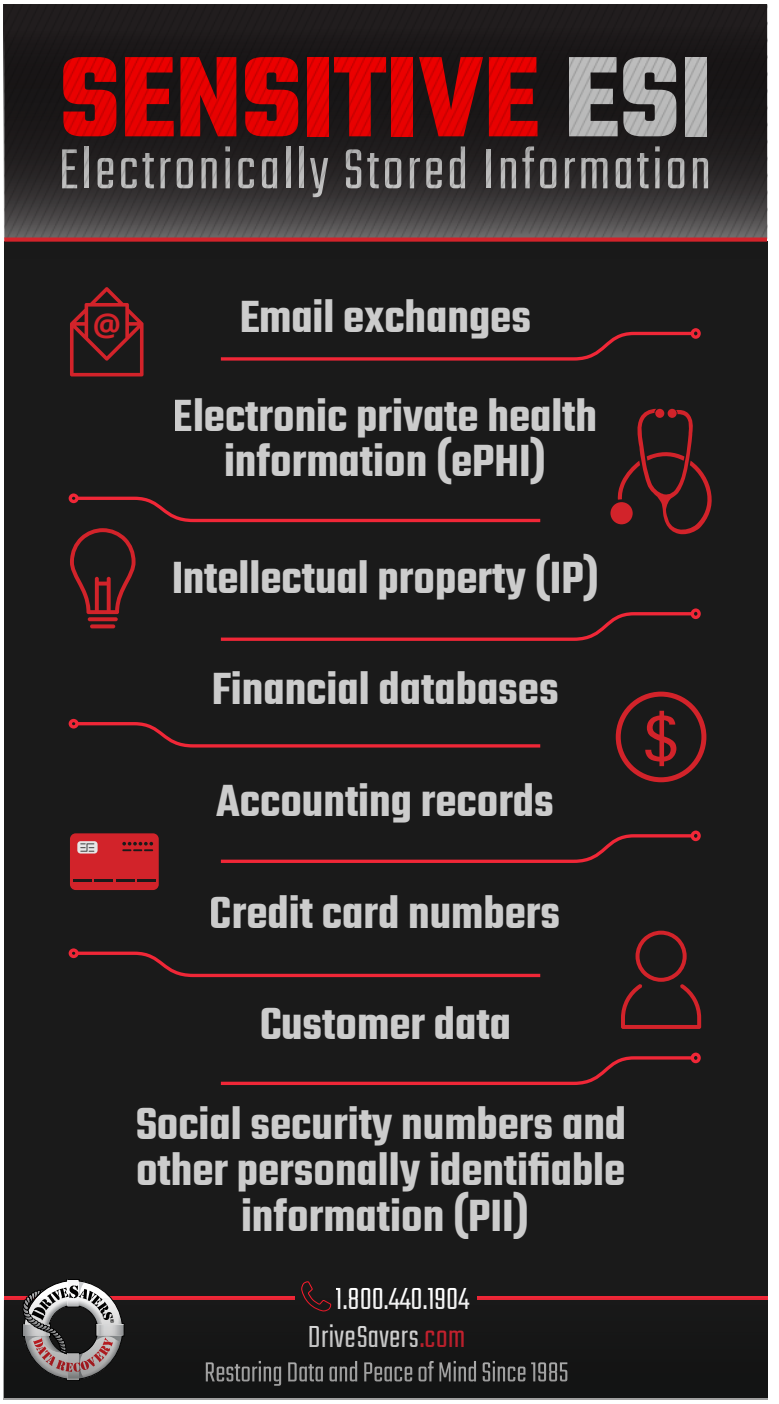
- 2021-2022 Data Breach Statistics
- Security Standards and Protocols for Data Recovery
- Points to Consider
- Security Vetting Checklist

DriveSavers Data Recovery
+1.800.440.1904 ▪ +1.415.382.2000 ▪ DriveSavers.com

2023

Introduction

Robust risk management is a must in today's challenging environment of mounting digital attacks on vital company assets and the regulated data they are entrusted to protect. Most organizations have a dynamic layered security practice incorporating multiple security controls to protect this sensitive data. The reputational and financial consequences of lost or corrupted data make this a requirement. 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 storage device fails, resulting in lost or corrupted digital data, few organizations have the internal resources to recover that data—especially in the case of physical damage or electromechanical failure. The device must be sent to a third-party data recovery vendor. Company-owned devices often hold security-sensitive electronically stored information (ESI), including critical intellectual property (IP), financial databases, accounting files, email exchanges, customer records, PCI, PII, and PHI. Most of the data recovery industry does not meet best practice standards to ensure data protection through cybersecurity; therefore, data recovery service providers must be classified as high-risk vendors. 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 significant financial and reputational damage. Inevitably, there will also be a loss of productivity.

When C-level executives and board members have not properly planned for this exception, IT personnel are left on their own to make problem-solving decisions. Without specific protocols in place to handle the data loss scenario, IT personnel may not be aware of the high-risk issue associated with this process, nor understand the critical impact of the data leaving the layered security of the corporate facility and potentially becoming subjected to negligence, fraud or abuse. Such an action could easily cost an organization millions of dollars in fines.

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

- Vetting a data recovery vendor should be mentioned in the organization's business continuity plan, disaster recovery plan, or incident response plan.
- Organizations should have vetting policies and guidelines in place for selecting a data recovery service provider.
- The most important practices to include in the policy are presented as a vetting checklist later in this report.

In addition, organizations need to address potential new threats to the security of data during the data recovery process. This includes making sure that if a cloud service provider uses a data recovery service provider, it should be required to notify the organization. While the need to recover data may be time-sensitive, it is crucial that every effort is made to ensure that the organization's confidential and sensitive data is protected during the recovery process.

This paper provides a roadmap for mitigating the potential risk of using third-party data recovery providers. The solution to this high-impact risk only requires low-cost policy and procedural changes. It ensures that the confidentiality, integrity, and availability of the organization's sensitive information are maintained during the data recovery process.

2021–2022 Data Breach Statistics

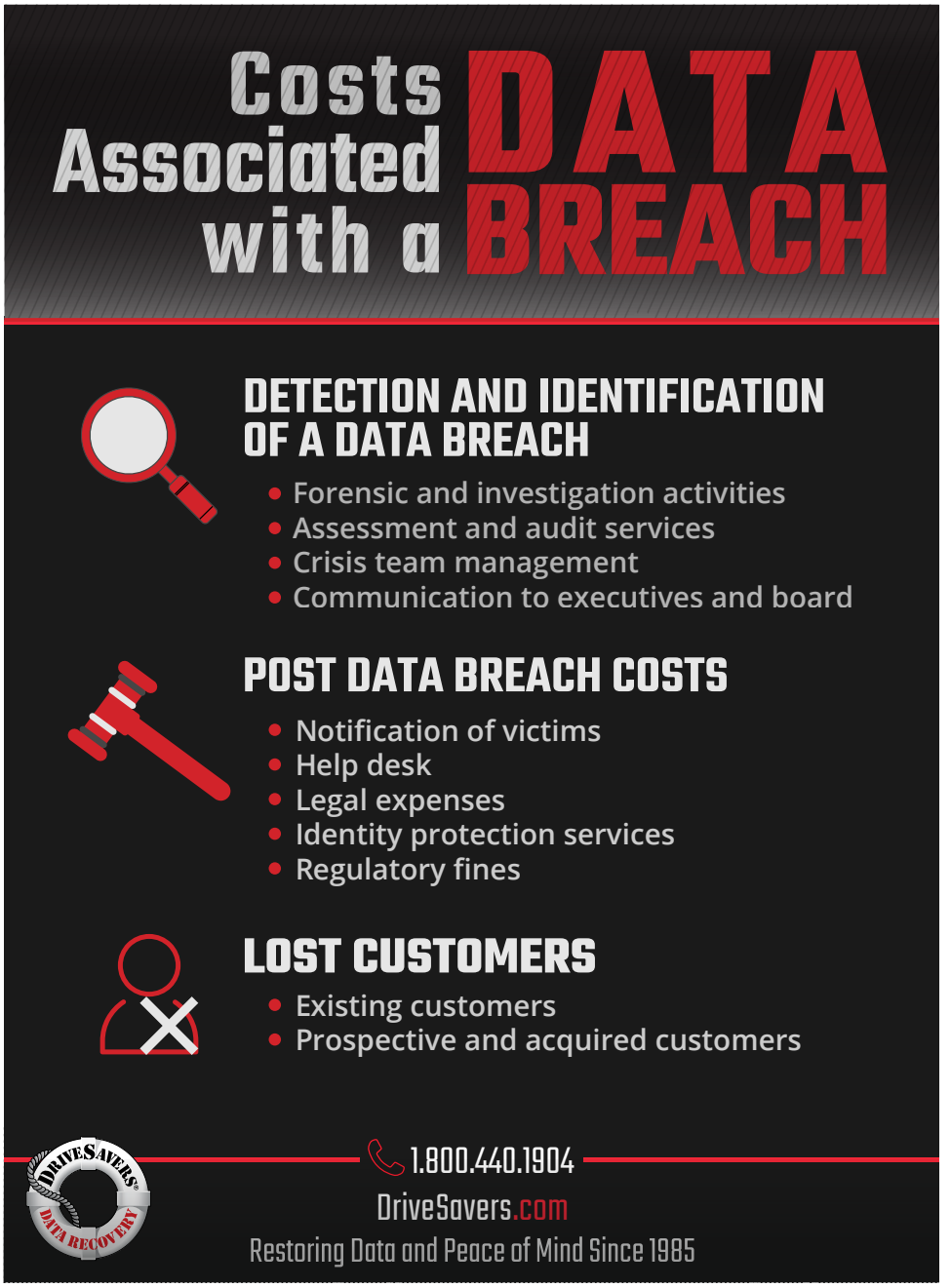
Data breaches may originate from malicious attacks, ranging from ransomware to social engineering, system glitches, or simple human negligence. A data breach can occur through internal security flaws, through a third-party vendor or a supply channel vendor.

In a July 2022 study, the Ponemon Institute interviewed members of 550 organizations who had experienced a data breach between March 2021 and March 2022. Malicious attacks that resulted in data loss included ransomware (11%), destructive attacks (17%), and compromised business partners (19%). Unintentional breaches caused by negligent actions of employees or contractors resulted in 21% of data breaches.

According to the Ponemon Institute, the worldwide average cost of a data breach during this period was $4.35 million, with the United States at the top of the chart, averaging $9.44 million for a single data breach. These costs were even higher for healthcare and financial institutions. In addition, the more records that were lost, the higher the cost of the data breach.

The following list includes costs associated with a data breach, which should be considered when developing a cybersecurity plan:

- A data breach will cost a company the unexpected and unplanned loss of existing customers. Consider implementing programs that preserve customer trust and loyalty to help reduce the number of lost business/ customers in case of a data breach.
- Negative publicity and deteriorated company reputation will lead to the diminished acquisition of new customers.
- The cost of a data breach depends on the size of the breach or the number of records lost or stolen—the more records lost, the higher the cost.
- Cost will increase with the time it takes to identify and contain a data breach. The faster the data breach can be identified and contained, the lower the costs. Disruptive technologies, access to cloud-based applications and data, and the use of mobile devices increase the complexity of dealing with IT security risks and data breaches.
- Costs associated with the detection and escalation of the data breach incident: forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and the board of directors.
- After a data breach, a business must notify and accommodate victims. Associated costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services, and regulatory interventions. There may also be fines associated with data security compliance inefficiencies.



Security Standards and Protocols for Data Recovery

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, HIPAA, FERPA, 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 the National Institute of Standards and Technology (NIST) and the latter from the Shared Assessments Groups.

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

"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?

SSAE 18 SOC 2 Type II

Compliance with auditing standards, such as the Statement on Standards for Attestation Engagements (SSAE) and Service Organization Control (SOC), assures that every aspect of the facility and network is secure and will 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 a service provider's data hosting control objectives, activities and related processes measured 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 it 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 SSAE SOC audit has become the Corporate Industry Standard for an overall control structure. While a SOC Type I audit verifies the "description" of controls and safeguards that a service organization claims to have in place, the SOC 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.

In 2017, the American Institute of Certified Public Accountants (AICPA) enacted updated attestation standards for SOC 1 and 2. All service organizations who wish to certify as maintaining security measures compliant with these protocols must pass Statement on Standards for Attestation Engagements (SSAE) No. 18, otherwise known as SSAE 18, rather than the previous standard, SSAE 16.

The new standards are meant to converge the varying degrees of compliance standards that previously existed and bring all U.S. standards up to international standards of compliance. New requirements by these regulations include regular risk assessment and detailed reporting of the security practices of third-party services used by a company.

General Data Protection Regulation (GDPR) for the European Union (EU)

Organizations based in the EU that handle data from customers must comply with the General Data Protection Regulation (GDPR), which went into effect on May 25, 2018. The regulation is designed to ensure the security and confidentiality of personal data.

The GDPR not only applies to organizations located within the EU but will also apply to organizations located outside of the EU if they offer goods or services to or monitor the behavior of EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

The GDPR standards are meant to converge the varying degrees of compliance standards that previously existed and bring all U.S. standards up to international standards of compliance. Requirements by these regulations include regular risk assessment and detailed reporting of the security practices of third-party services used by a company.

According to the GDPR, organizations must:

- Only process data for authorized purposes
- Ensure data accuracy and integrity
- Minimize subjects' identity exposure
- Implement data security measures

SSAE 16	SSAE 18	SOC I	SOC II
Previous protocol did not address company risk assessment or consider security of third-party services used by a company	New protocol requires regular risk assessment and detailed reporting of security practices by third-party services used by a company	Review of company documentation; verifies documentation of security protocols	Review of company security systems in place; physical on-site review of security protocols

Points to Consider

Before engaging the services of a third-party data recovery vendor, organizations must improve their due diligence in order to mitigate the risk of a data breach. Here are some questions to consider:

1. How does your organization measure the security, reliability, and expertise of third-party data recovery services?
2. With respect to the protection of sensitive or confidential data during data recovery, how would you rate your company's vetting process for selecting a secure third-party data recovery service provider?
3. Does your organization conduct a risk assessment of third-party data recovery services before selecting them?

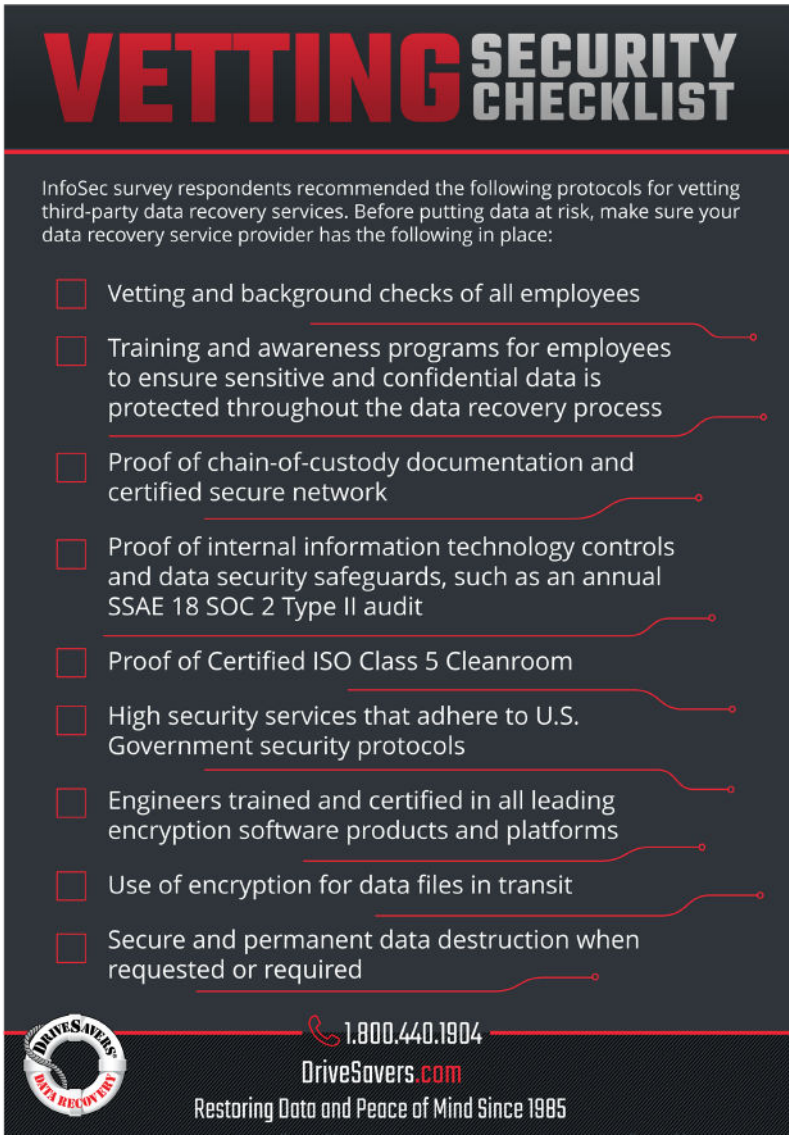
Conclusion

Data recovery service providers still play a large role in the organization's information life cycle as the number and complexity of devices increase to facilitate the flow of information.

Board members and C-level executives must work with senior IT directors to close the policy and security gap posed by the organization's need to engage third-party 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.

Security Vetting Checklist



About DriveSavers

DriveSavers is the worldwide leader in data recovery, with a solid reputation built on outstanding customer service, consistently high success rates, and the fastest Standard Service turnaround time in the business.

For over 35 years, DriveSavers has performed data recovery on every kind of storage device, including hard disk drives (HDDs), solid-state drives (SSDs), smartphones such as iPhone and android phones, tablets, USB flash drives, camera cards and enterprise-level RAID, NAS, and SAN servers.

The company handles every kind of data loss situation, including mechanical failure, physical, water and fire damage, data corruption, file deletions, head crashes, and more.

DriveSavers conducts HDD data recoveries, including hermetically sealed helium drives and other advanced HDD technology, inside a Certified ISO Class 5 Cleanroom that is dust-free and static-free—the most technologically advanced data recovery cleanroom in the industry.

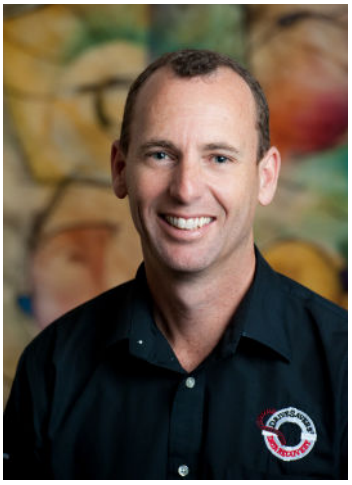
The flash device recovery team includes some of the industry's best minds and most skillful microsolderers. This is the type of data storage that is experiencing the most rapid change and advancement, and DriveSavers repeatedly recovers data that others have deemed unrecoverable. The talented data recovery engineers at DriveSavers were the first in the world to recover data from Apple M1 and T2 logic boards that were catastrophically damaged beyond repair.

With annual SOC 2 Type II certification, DriveSavers provides customers with the highest degree of security available in the data recovery industry today. In addition, DriveSavers data recovery engineers are experts in encryption and encrypted data storage technology.

You can view all DriveSavers authorizations and certifications on our website at **www.drivesavers.com/proof**

About the Author

Mike Cobb
Director of Engineering
Chief Information Security Officer (CISO)



As Director of Engineering, Mike Cobb manages the day-to-day operations of the Engineering Department, including the physical and logical recoveries of rotational media, SSDs, smart devices and flash media. He also oversees the R&D efforts for past, present, and future storage technologies. Mike encourages growth and ensures that each of the departments and their engineers continues to gain knowledge in their field. Each DriveSavers engineer has been trained to ensure the successful and complete recovery of data is their top priority.

As Chief Information Security Officer (CISO), Mike oversees cybersecurity at DriveSavers, including maintaining and updating security certifications such as SOC 2 Type II compliance, coordinating company security policy, and employee cybersecurity education.

Mike joined DriveSavers in 1994 and has a B.S. in Computer Science from the University of California, Riverside.

Fortune 500 Companies Worldwide Trust DriveSavers