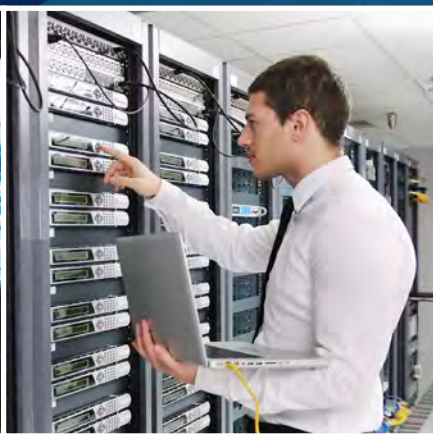
US DataVault

Recovery is Everything™

Data Protection Trends:
Validating Recovery



GET STARTED ▸

Table of Contents

This report provides detailed statistics on data recovery, providing a window into ransomware threats and pricing fairness.

Executive **Summary**

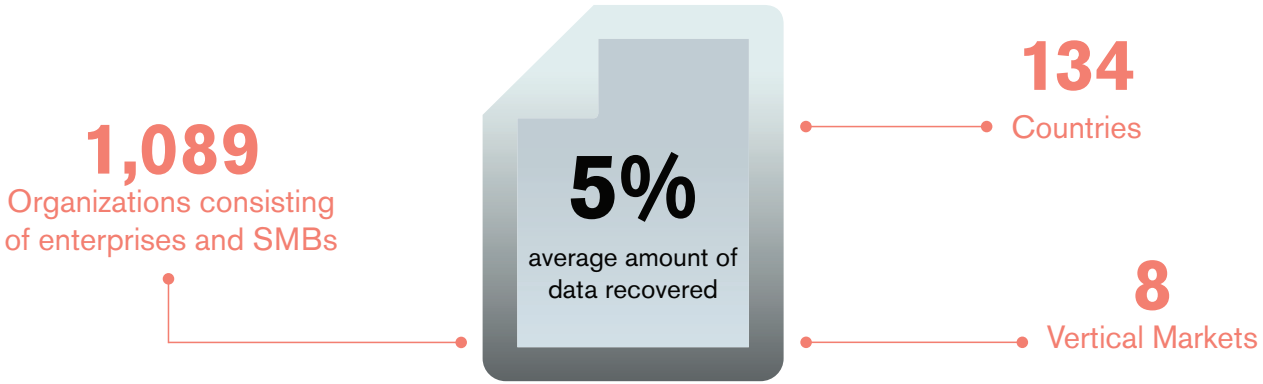
The data protection industry has long focused on the business benefits and ideal solutions for a myriad of data backup needs. USDV, a 17 year provider of cloud backup and data recovery software, in cooperation with Asigra has released the industry's first report to analyze empirical data recovery information. This information captures data recovery patterns and statistics across a set of 1,089 organizations consisting of enterprises and small businesses in 134 countries and in eight vertical markets.

This data emphasizes that the ultimate value of data protection solutions is not simply backup but the ability to recover the data as an essential element of business continuity and disaster recovery scenarios. By focusing exclusively on data recovery metrics, this report outlines the business use cases for prioritizing data recovery as the correct goal for data loss prevention strategies. Through thoroughly examining this data, we can understand the value of pricing models for data recovery based on the actual percentage of data restored.

Most data recovery businesses price their services as if their customers recover 100 percent of their available data. However, if empirical information can demonstrate that customers rarely restore that volume of data, we can evaluate the fairness of those pricing models. By focusing on the specifics of data recovery instead of simply backup capabilities – because for organizations seeking data protection, recovery is everything – we can discuss the bottom-line business value of data recovery services.

Recovery Report **Data Sets and Findings**

The study examines data recovery by industry segment, country, size of company, data types retrieved, and more. It also looks at the reasons given for data recoveries based on tens of thousands of data restores that organizations have completed over a more than two-and-a-half-year period from January 1, 2014 through August 1, 2016. This provides a view into the role that data breaches and ransomware attacks may play in requests for data recovery, amongst other insights.



It also examines the size of the datasets recovered, both measured in gigabytes and as a percentage of all data available for recovery. Analysis of this information provides insights into the volumes of data recovered by organizations in different verticals and of different sizes.

This data recovery report found:

- On average, organizations recovered less than five percent of their data during data restores. This percentage was consistent year over year during our reporting period. It is notable that companies do not recover 100 percent of their data, even when given the option.
- The average size of datasets recovered was 13 GB; remarkably, most organizations large or small recovered roughly the same average amount of data.

52%

Most Common Reason for a Data Recovery – Access a Previous Generation of Data

13%

Second Most Common Reason for a Data Recovery – User Error/ Accidental Deletion

10%

Third Most Common Reason for a Data Recovery – Lost or Stolen Device

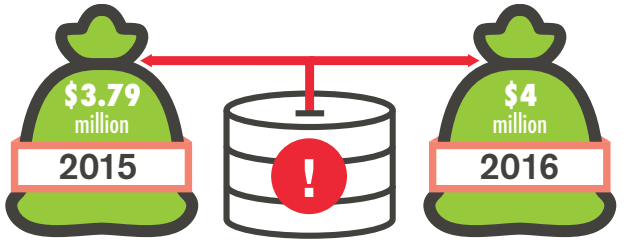
- The most common data type restored were file-level systems, not databases or data stored in enterprise applications.
- The most common reason cited for a data restoration request across all vertical segments was to Access a Previous Generation of Data, at 52 percent.
- The second most common reason cited for a data recovery is User Error/Accidental Deletion (13 percent); third is Lost or Stolen Device (10 percent).
- Data recovery drills are much more common now than in the past, and their frequency grew during this reporting period. The average number of recovery drills performed grew 150 percent over the two-and-a-half-year term of our report. If we use the rate of recovery drill occurrences through August 1, 2016 (the end of our reporting period) to project the estimated number of recovery drills for the remainder of 2016, that number exceeds the number for 2015.

This data recovery report helps to focus the discussion of data protection solutions on their ability to recover the data as an essential element of overall business strategy.

“This report confirmed what I always suspected but never had empirical evidence to back up. In the real world, organizations usually recover far less data than they pay for.”

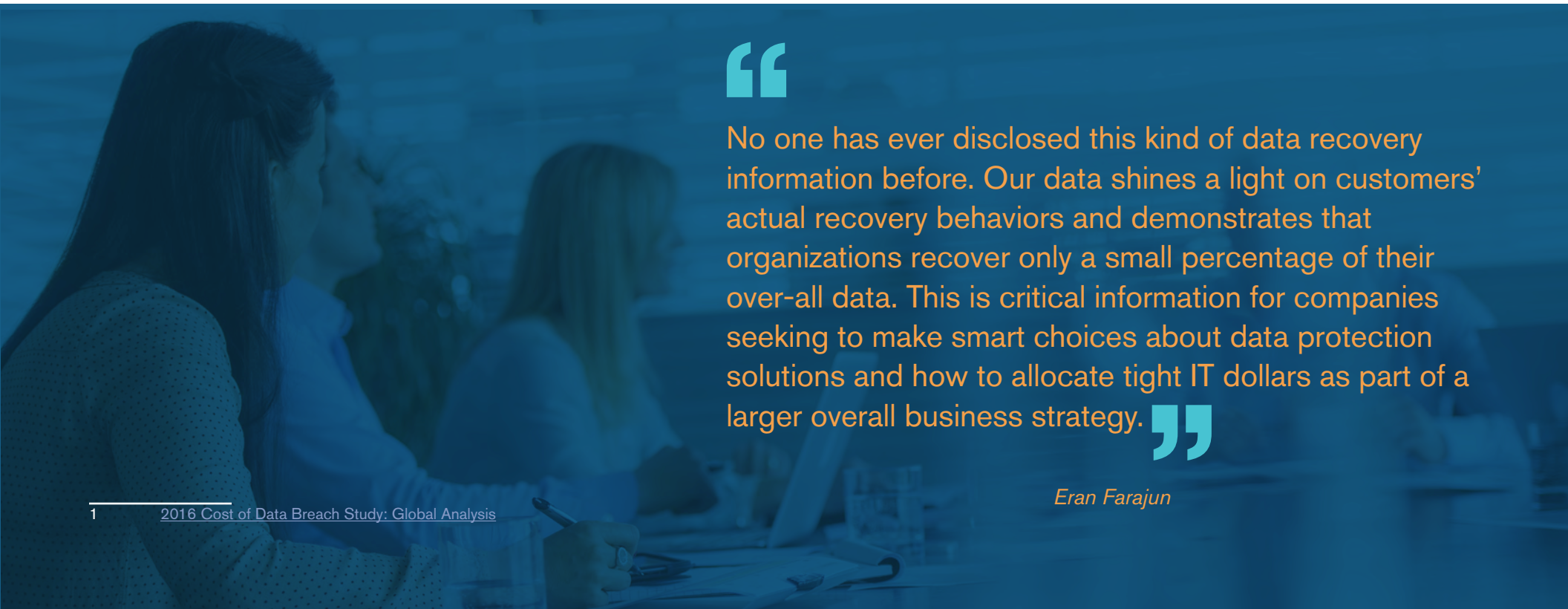
– Marc Staimer, president and cds, Dragon Slayer Consulting

Why this Matters



Why is this important? The average total cost of a data breach has increased from $3.79 million to $4 million from 2015 to 2016.[1]

The greatest financial consequence to organizations that experience a data breach is lost business, which can lead to loss of customer trust, impacting near and long-term financial results. Beyond purely financial considerations, another potential long-term consequence is brand impact. Publicity surrounding a data breach is negative, and can affect not just existing customers but prospective customers as well.



> No one has ever disclosed this kind of data recovery information before. Our data shines a light on customers' actual recovery behaviors and demonstrates that organizations recover only a small percentage of their over-all data. This is critical information for companies seeking to make smart choices about data protection solutions and how to allocate tight IT dollars as part of a larger overall business strategy.

Eran Farajun

1 2016 Cost of Data Breach Study: Global Analysis

A Business Case for Data Recovery

This report provides business leaders with detailed information about data recovery, allowing them to review their IT operational efficiency and compare their organizations with others in their vertical market and across other industries to learn if their recovery activities are in line with their peers. The report also provides businesses with information about the most common reasons for data loss so they can take preventative measures within their own organizations.

One of the most intriguing data points from the report is that most companies recover only a very small portion of their total stored data, even though they have the potential to recover much more or all of their backed-up data. Most organizations do not conduct full image-based recoveries of entire machine storage systems. Nor do they typically restore data preserved in databases or enterprise applications. The vast majority of data restored is file system data stored on hard drives and servers in data centers, remote and branch offices, and in the cloud. According to the report, customers chose to recover data from select, granular file-level systems to retrieve only the specific data they needed to resume business operations quickly and efficiently.

Restoring only the select datasets required may seem like a smart disaster recovery or business continuity strategy, but it raises other concerns. Many data protection companies charge for recovery services by pricing them as if their customers will recover 100 percent of their data. Yet this data demonstrates that this is almost never the practice.

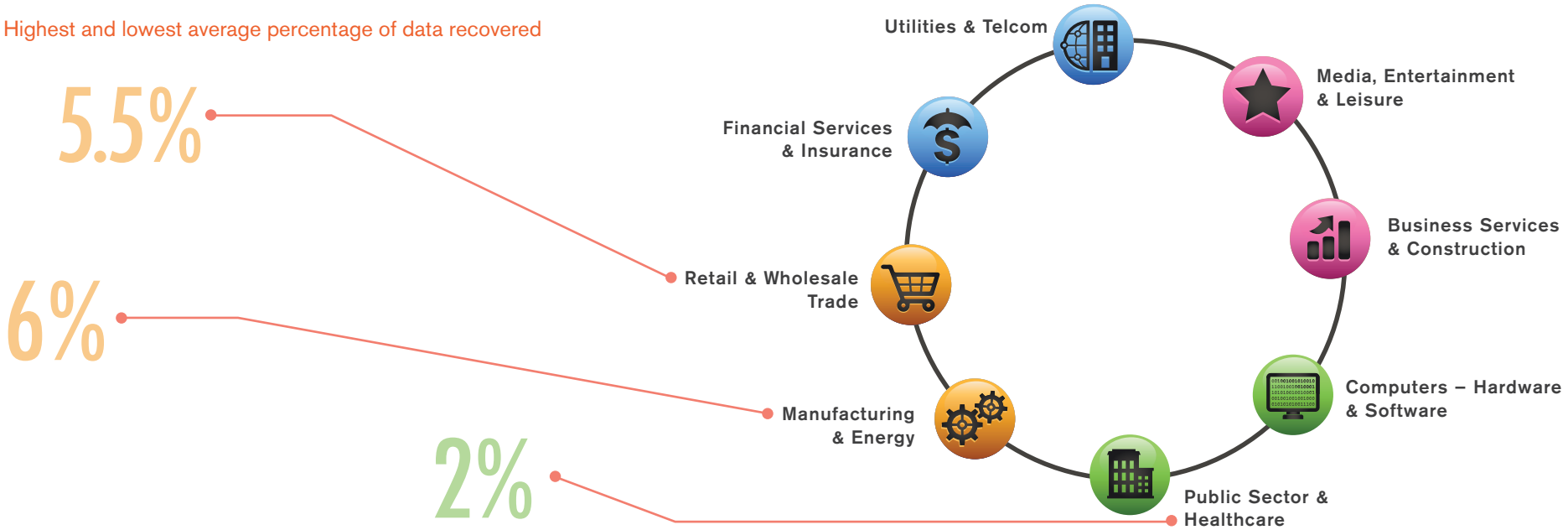
> “Businesses need a fairer pricing model for data backup and recovery that reflects the fact that the majority of recoveries are of small subsets of full storage datasets.”
>
> *Eran Farajun*

Average **Data Recovery Rate**

The average data recovery rate (as a percentage of all possible recoverable data) for all industries is less than five percent. In other words, when organizations perform a data recovery, on average they elect to recover less than five percent of the data available to them; few businesses chose to recover a full 100-percent image of an entire system, instead choosing to recover smaller amounts of file-based data.

By vertical, the highest average percentage of data recovered was the Manufacturing and Energy sector, which recovered just over six percent of its data. The second highest was Retail and Wholesale Trade, which on average recovered nearly five and a half percent. The sector with the lowest average percentage of data recovered was Public Sector and Healthcare, with just over two percent.

Highest and lowest average percentage of data recovered

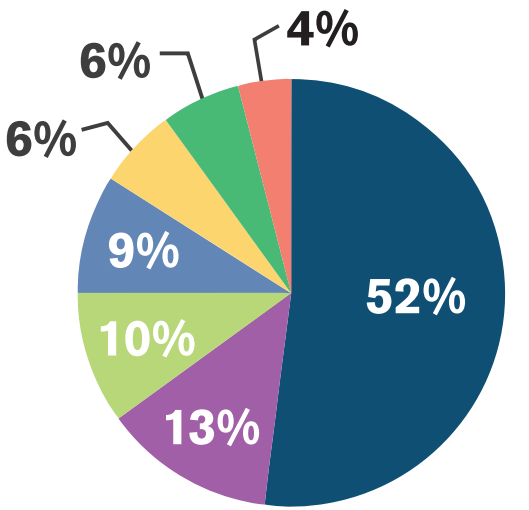


Reasons for Recovering Data

The most common reason for data recovery across all vertical segments is Access to a Previous Generation of Data, cited by 52 percent of respondents. With 13 percent, User Error/Accidental Deletion was the second most common reason. Lost or Stolen Devices was third, with 10 percent.

While Access to a Previous Generation of Data is the top reason for recovery across all verticals, its percentage share of all the reasons for recovery varies substantially from vertical to vertical. For companies in the Media, Entertainment and Leisure segment, access to a previous generation of data represented 62 percent of reasons for recovery, the highest in our report; the second highest vertical citing the previous generation data access rationale was the Financial Services and Insurance industry, at 57 percent. The sector that reported the lowest percentage of previous generation data access recoveries was Utilities and Telecommunications, at 36 percent.

Also, as a rationale for data recovery, access to a previous generation of data is consistent with the increasing frequency of ransomware attacks. According to BitSight[2], the U.S. Justice Department reported that over 4,000 ransomware attacks were committed daily in U.S. in 2015. In a ransomware situation, malware trojans, such as CryptoLocker, CryptoWall, Locker or TorrentLocker, infect a computer system with a virus that encrypts the files, making them inaccessible, and then the attackers demand ransom, usually in Bitcoin, to decrypt them.

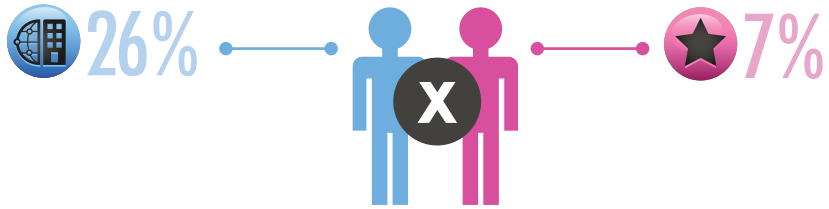


- 52% – Access a previous generation of data
- 13% – User error/accidental deletion.
- 10% – Lost or stolen device
- 6% – Hardware failure
- 6% – Disaster (fire, security incident, etc.)
- 4% – User data deletion/malicious intent
- 9% – Other

This relatively new and profitable cybercrime technique has become especially common in the healthcare sector, where personal information from patient records makes clinics and hospitals perfect targets for this kind of extortion. According to a report in Healthcare IT News[3], ransomware "is now so prevalent it's creating an economy of its own." The article cites Symantec research that lists the average ransom paid by businesses is about $10,000, and states FBI reports that CryptoWall ransomware netted more than $18 million between 2014 and 2015. Over 100 million healthcare documents were leaked on the encrypted Dark Web in 2015[4], according to the U.S. Department of Health and Human Services.

2 The Rising Face of Cybercrime

3 Ransomware to wreak havoc in 2016, ICIT study say
4 Over 400,000 sensitive healthcare records leaked on the DarkWeb



Across all verticals, the second most common reason for recovering data was User Error/Accidental Deletion, but its share of the total also varied across verticals, from a high of 26 percent of all recoveries in Utilities and Telecommunications to a low of seven percent for companies in the Media, Entertainment and Leisure segment.

This can in part be attributed to data that is deleted or lost on popular Software-as-a-Service (SaaS) platforms such as Salesforce.com, Microsoft Office 365 and Google Apps.

These SaaS vendors have become enormously popular. According to a study by Skyhigh Networks[5] of over 27 million users working at over 600 enterprises worldwide, one out of every five corporate employees used the Microsoft Office 365 cloud service, up from less than seven percent in mid-2015. In that same time period, usage of Microsoft Office 365 within these enterprises grew over 320 percent, as the percentage of employees using at least one Office 365 application more than tripled from 6.8 to 22.3 percent.

These office productivity SaaS vendors, which now store vast amounts of valuable customer data, are deeply invested in ensuring high availability and uptime. However, they are not as focused on providing long-term data protection solutions that meet an organization's needs for compliance, business continuity, and data recovery.

For instance, vendors such as Salesforce.com charge their customers a fee if a data recovery is required, and after 15 days, Salesforce.com customer records that have been sent to the Recycle Bin can only be recovered with the help of support at a cost of $10,000 per recovery. After 90 days, these same files in the Recycle Bin are unrecoverable. Office 365 and Google Apps have similar policies, which dictate that after a specific number of days, data restores may not be possible, but certainly will be expensive.

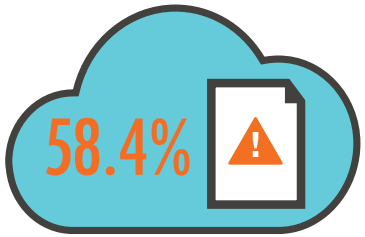
Organizations using these services can pay the SaaS vendor to back up their data. But if the system goes down, as it did for Salesforce.com in May 2016, the backup that the organization has paid for and is counting on could be in the same data center – and maybe on the same servers – that suffered the data outage. Then the business is stuck trying to perform data recovery from dead equipment.

In addition, the Skyhigh Network study cited above found that these SaaS platforms can also expose companies to high-risk security threats. The study found that of the organizations in their study that use Office 365:

- 71.4 percent had at least one compromised account each month.
- 57.1 percent had at least one insider threat each month.
- 45.9 percent had at least one privileged user threat each month (from user accounts which are officially authorized to access sensitive data, but which are used for malicious or unsanctioned reasons).

5 Office 365 Adoption Rate, Stats, and Usage

The study also found that in an analysis of over 20,000 cloud services, 58.4 percent of sensitive data in the cloud is stored in Microsoft Office documents.



These statistics speak to the growing popularity and targeting of SaaS vendors such as Office 365, and offer a potent alert to organizations that create and store data in these cloud-based platforms. Ensuring that this data is backed up and fully recoverable is now an essential part of any data protection strategy.

This report also found that 10 percent of data restores, the third most common reason cited, are due to lost or stolen devices. Data protection strategies should also include geo-location and remote wipe capabilities for mobile devices to ensure corporate data does not fall into the hands of data thieves.

Other standout findings for recovering data rationales include:

- The industry that cited Lost or Stolen devices highest as the reason for recoveries was Utilities and Telecommunications, at 27 percent.
- The segment reporting Disaster (fire, security incident, etc.) as the highest reason for recovery was Retail and Wholesale Trade, at 25 percent.
- As a reason for data recovery, User Data Deletion/Malicious Intent didn't even crack the top five reasons given for recovery, cited by an average of just four percent of respondents across all industries. The segment reporting Malicious Intent the highest in its reasons for recovery was Business Services and Construction, at six percent.

Lost or Stolen Devices

27%

Disaster (fire, security incident etc.)

25%

User Data Deletion/Malicious Intent

6%

Average Data **Restore Size**

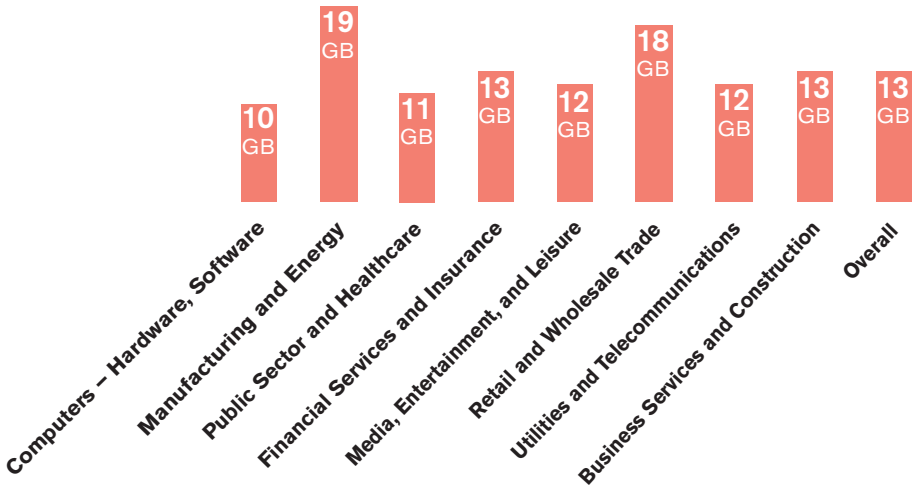
While the average size of a data recovery across all verticals during the report's timeframe was 13 GB, this total also differed across industries. Manufacturing and Energy, at 19 GB, and Retail and Wholesale Trade, at 18 GB, were the verticals with the highest average data restore size. The lowest average data recovery size was in the Computer Software and Hardware segment, at 10 percent.

These relatively small data restore sizes show that granular file-level recoveries are more common than image-based data recoveries. The smaller, targeted recoveries mean that businesses can recover just the data they need to resume business operations quickly and efficiently.

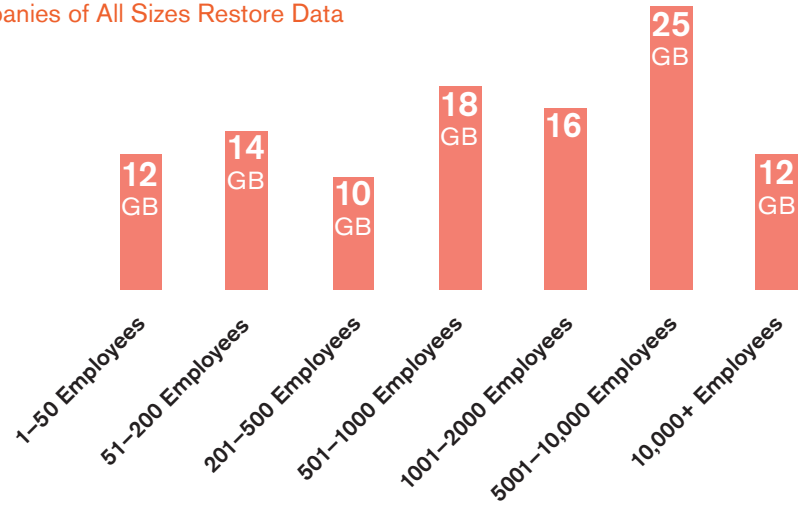
Average Data Restore Size varied by company size, with companies having 201-500 employees recovering an average of 10 GB, and companies that have between 5,001–10,000 employees recovering 25 GB of data on average.

The higher average data recovery for larger organizations could indicate that companies with more employees, and often more data, have a greater risk of data loss and/or data breaches.

Average Data Restore Size (GB) by Industry

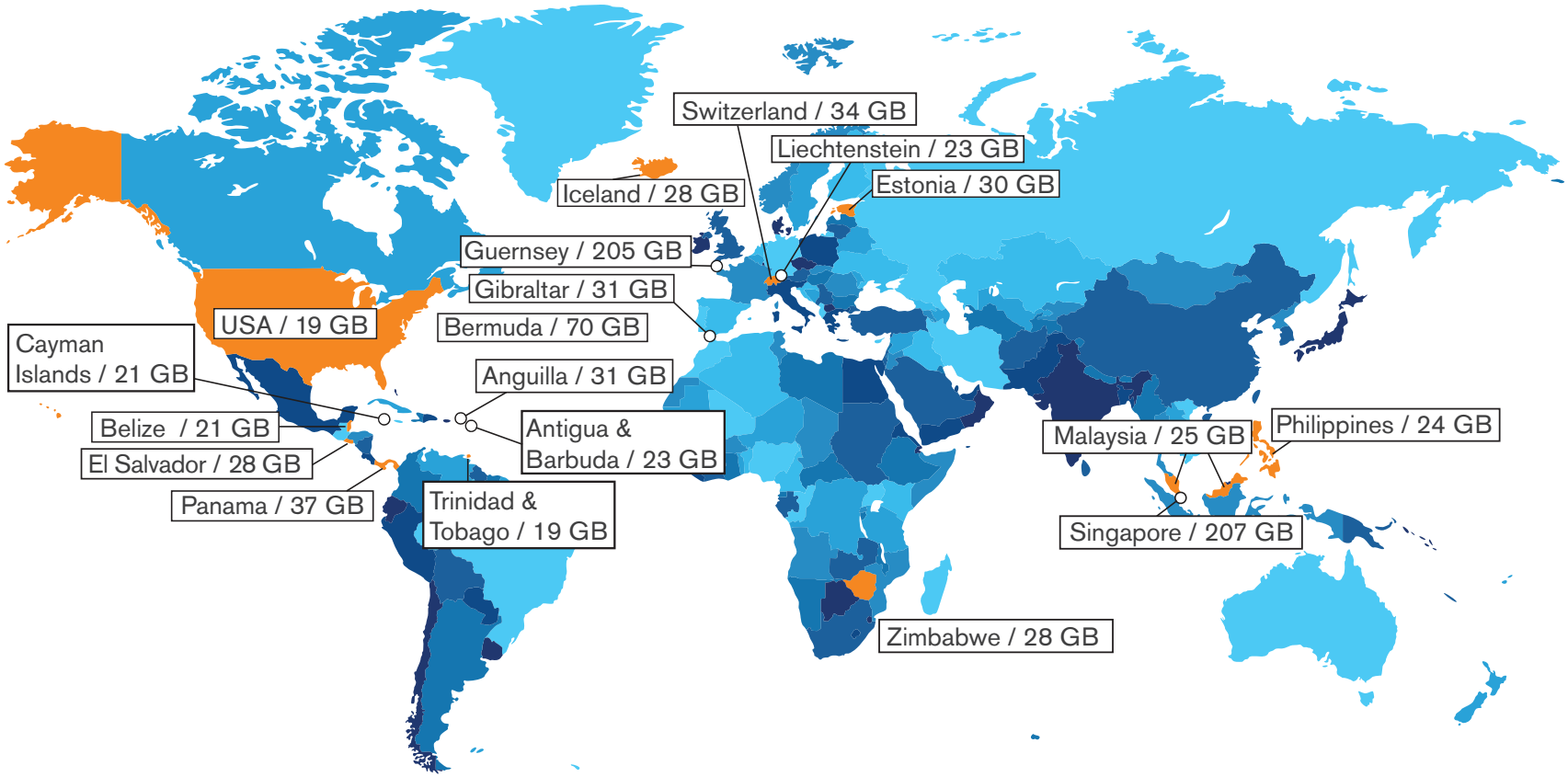


Companies of All Sizes Restore Data



The average restore size for European and Asia Pacific countries surpassed the USA by 10 times, which had an overall average recovery size of 19 GB.

The average restore size also varied by country. Two outliers within the by-country data are Singapore, which recovered an average data restore of 207 GB data, and Guernsey, whose average data restore size was 205 GB. Organizations in these two countries each restored on average more than 10 times the average data restore size of companies in the US.

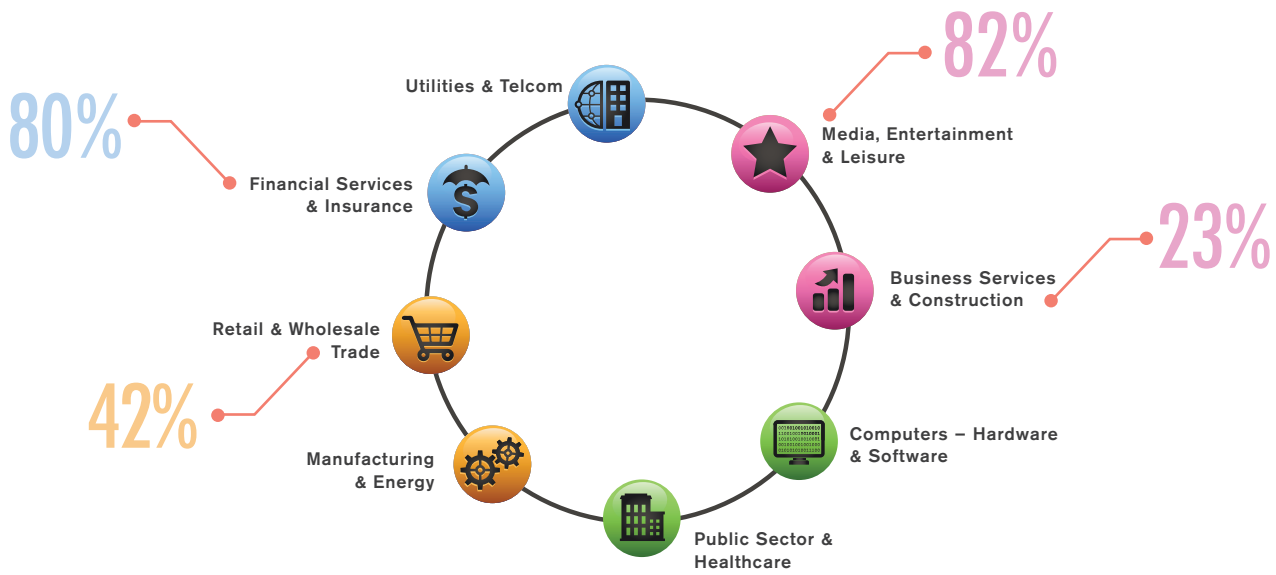


Types of **Data Recovered by Vertical Market**

This report breaks down the types of data recovered into what kind of backup and storage system or file management platform the data was housed in, including file systems, VMware VADP backup and data protection systems, Microsoft SQL Server, Microsoft Email Exchange, Hyper-V VM backup sets, and others.

Though there is variation by vertical segment in the types of data restored during recoveries, for all industries the largest data type restored was in user-generated file systems. The largest average percentage of file system data recovered was 82 percent by companies in the Media, Entertainment and Leisure sector, while close behind at 80 percent was the Financial Services and Insurance vertical. The lowest average percentage of file system data restores was 42 percent in the Retail and Wholesale Trade segment.

After file system data, the second highest data type recovered was from VMware VADP backups; these data-type restores represented 23 percent of recoveries in the Business Services and Insurance vertical, the highest for all verticals.



Demand for **Data Recovery Drills Increase**

Given the frequency of news stories on unplanned IT and telecom outages, data breaches, cyber attacks and disruptive weather events, it should be no surprise that over 80 percent of IT organizations have disaster recovery plans in place. However, of that group, only 40 percent test their disaster recovery plans regularly with mock drills[6].

However, this report indicates that this pattern may be changing. Our findings reveal that data recovery drills are being performed increasingly often, with a 150 percent increase in drills from 2014 to 2016.

The report also found that the average data size restored per recovery drill varied by vertical. The average overall data recovery size per drill across all verticals was a recovery of 32 GB. The largest average recovery size per drill was in the Manufacturing and Energy sector, with 64 GB

150%
Increase in Drills from 2014 – 2016

32GB
Overall Average Data Recovery Size

64 GB
Largest Average Recovery Size Per Drill

6 Research: 2013 State of Storage

Targeted **File Restores**

As revealed in this report, customers actually recover only small volumes of data in real-life data restores, with the majority of files recovered from file-level stores.

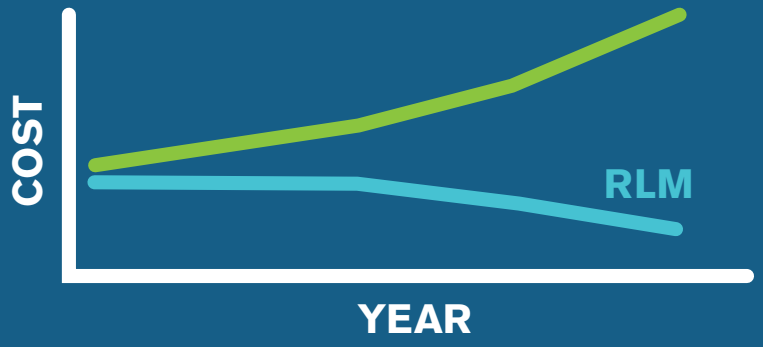
USDV's Cloud Backup offers granular file-level recoveries which allow customers to select and recover just the files they need for business continuity and disaster recovery. This is unlike data protection solutions that require image-based data recoveries. These solutions necessitate recovery of the entire machine storage and deliver a large and confusing quantity of disorganized files to customers, forcing them to organize and delete the files they don't need as part of the recovery process.

The USDV solution enables customers to select just the files needed to help get systems up and running again without burdening the recovery process with unnecessary data volumes.

Fair **Pricing**

The ability to limit the size of data restorations also enables USDV to offer a fairer pricing model for its data recovery solution. USDV created the USDV No-Cost Recovery model because most businesses recover less than five percent of their data. Unlike other pricing models in the market today, many of which charge users as if they will always restore 100 percent of their available backup data, the USDV No-Cost Recovery model pricing is based on the percentage of data recovered over the course of a contractual term.

To illustrate the difference in these pricing models, consider standard cable TV contracts which require subscribers to pay for hundreds of channels and programs that they never watch. A fairer model would ask the subscriber to pay only for the channels and shows they view. The USDV No-Cost Recovery model reflects a fairer way for pricing data recoveries, as businesses only pay for the data they store, not what they must recover.



> For those who recover less, they pay less. The No-Cost Recovery Model really does work well for our Clients given that they're able to meet those twin demands of recovering and storing more data at a lower price.

Marc Shaffer, CEO, USDataVault, Inc. (A B2B Backup and DR Services Provider for over 17 years.)

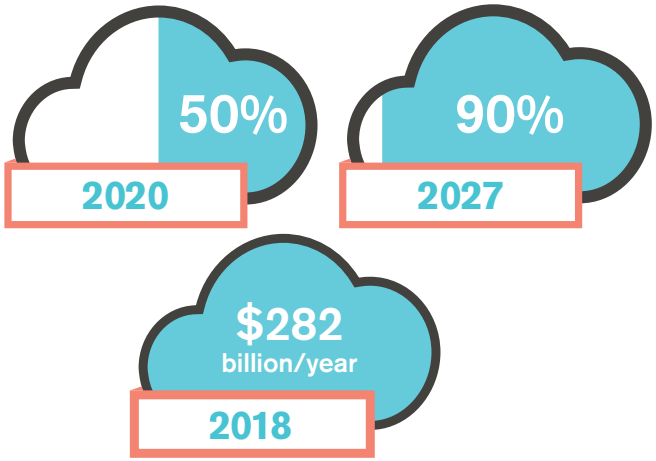
Fast **Recovery from Ransomware**

Cloud Backup by USDV provides organizations the ability to quickly recover data infected with ransomware like Cryptolocker, Locky, or other malware, and return to business as usual.

The solution's powerful restore wizard functionality enables technicians to quickly identify infected files on a server and perform multiple rollbacks to the appropriate pre-infection recovery point. Asigra allows technicians to perform a recovery of just the infected files, without having to spend the time restoring an entire server.

Protection for **Cloud-Based Data on SaaS Platforms**

Cloud-based data is growing fast, whether in platforms such as Salesforce.com, Google Docs, or Microsoft Office 365, or on cloud infrastructures such as Microsoft Azure and AWS. Gartner predicts that cloud office system adoption will have 50 percent market penetration by 2020, growing to 90 percent by 2027[7]. Gartner also foresees that $282 billion per year will be spent on cloud infrastructures by 2018[8].



User error – the third most common reason for data recovery according to this report – will become much more pervasive in the future as more organizations migrate to cloud-based office productivity suites that present their own set of data protection challenges.

Traditional data protection strategies that protect data in the data center are not able to protect data in the cloud. Organizations that are creating cloud data, or that have transferred data to storage or virtual machines in the cloud must realize that legacy data protection solutions do not follow the data.

USDV's Cloud Backup provides comprehensive data protection capabilities across multiple computing platforms, and is one of the few data protection solutions that offers secure and reliable backup and recovery of data in cloud platforms such as Microsoft Office 365 Exchange Online, SharePoint Online and OneDrive for Business. With no limits on the data size, USDV can easily scale to meet an organization's data protection needs as they move data to the cloud.

7 Do You Need to Cover Your SaaS to Prevent Data Loss?
8 Gartner Forecast Analysis: Public Cloud Services, Worldwide

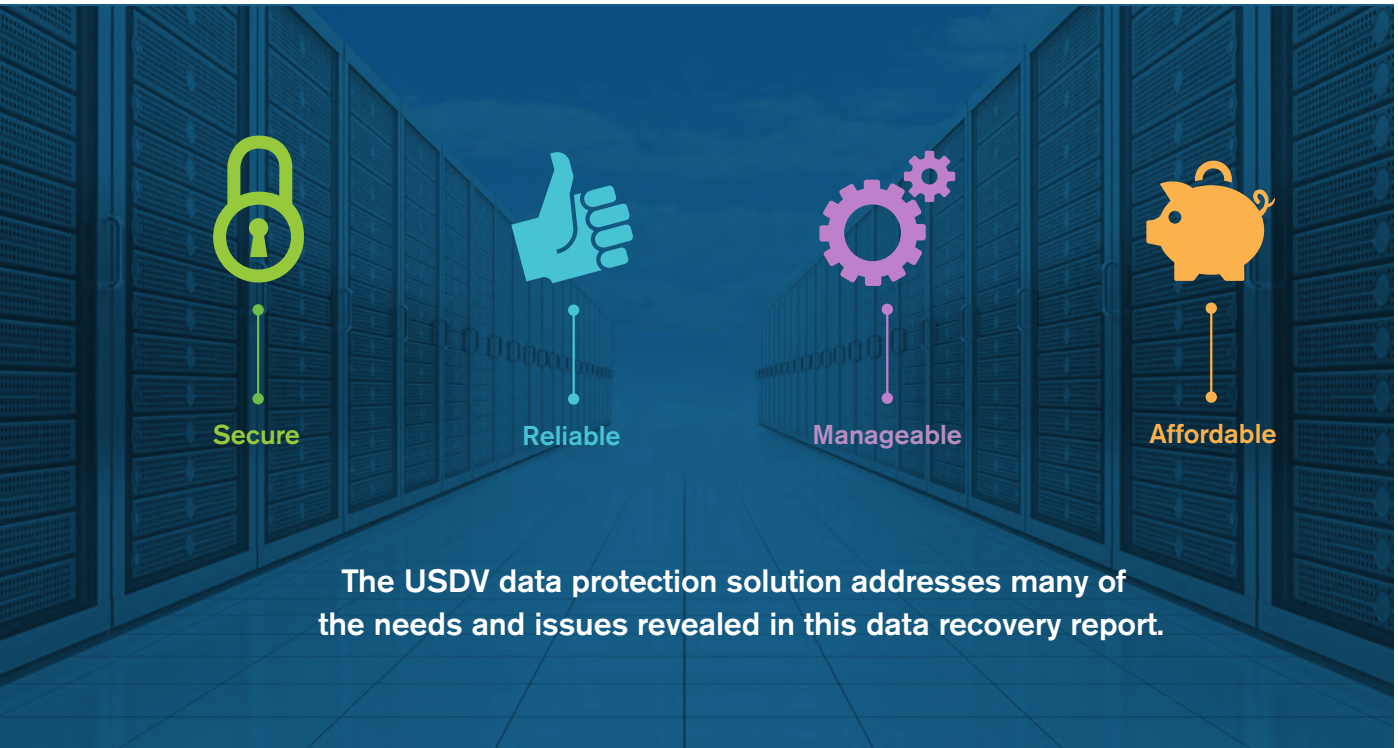
Protection from **Hardware Failure or Missing Equipment**

Also, USDV software includes the ability to access missing devices as they come online and remote wipe data from them. In addition, to address data loss from sources such as hardware failure, USDV offers features such as "Healing" which verifies the logical and physical integrity of data written to storage systems by constantly monitoring whether the backup data it captures is the same as the backup data stored on the disk.

In Conclusion

This recovery report demonstrates the critical importance of robust data recovery capabilities as a key feature of an organization's data protection strategy.

USDV's enterprise backup and recovery software provides secure, reliable, manageable and affordable comprehensive data protection for all of an organization's data, from virtually any data source including laptops, servers, data centers, and SaaS platforms and Infrastructure-as-a-Service clouds.



How much time & money would you loose if all your data was gone!

To contact a US DataVault Backup Specialist, call **1-615-933-USDV** or **615-933-8738.**

FOLLOW US DATAVAULT ON SOCIAL MEDIA