

A CIB ECS REPORT 2011

Business Data Loss Survey

Table of Contents

- 01 EXECUTIVE SUMMARY
Who took part?
- 02 THE ENTERPRISE ENDPOINT
How user data is being protected
- 03 INCREASED INTEREST IN ENDPOINT BACKUP
Has endpoint data backup become top of mind?
- 04 ENTERPRISE BACKUP REQUIREMENTS
Features / Benefits that matter
- 05 DATA MIGRATION
Common company challenges
- 06 BUSINESS DATA LOSS
Data loss risks & factors
- 07 CLOSING COMMENTS
Reality vs Belief

01

EXECUTIVE SUMMARY

WHO TOOK PART?

Over 250 companies took part in this year's Cibecs Endpoint Data Loss Survey.

As shown (in Chart 1) **29.9% of participants are enterprises comprising of 1 000 – 10 000 employees**, while just less than 50% are SMB's with a staff of less than 500. 7% of the survey respondent companies employ more than 10 000 people.

Chart 2 illustrates the market sectors of our survey participants. Again this year the IT industry has lead the way at 23.7%, with Retail or Wholesale coming in as the second highest representation.

Over 40% of our survey participants are IT Managers or Executives in their respective industries. A further 17.8% are in either development or technical departments.

CHART 1

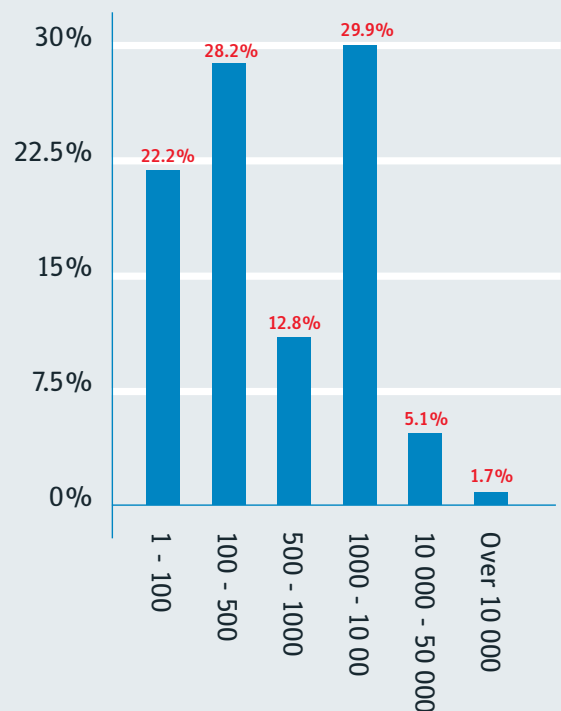


CHART 2 | INDUSTRY SECTOR REPRESENTATION



Marketing / Public Relations	1.0%
Business Services / Consulting (non-ICT related)	3.4%
Construction / Architecture / Engineering	4.1%
Education	1.7%
Finance / Banking / Insurance / Accounting	11.0%
Government	10.2%
Information Technology	23.7%
Parastatals / Utilities	2.5%
Manufacturing (non-computer related)	9.3%
Medical / Dental / Healthcare / Pharmaceutical	0.8%
Mining / Petrochemical	1.7%
Retail / Wholesale	14.4%
Telecommunications / Cellular providers	3.4%
Other	12.7%

02

THE ENTERPRISE ENDPOINT

HOW USER DATA IS BEING STORED & PROTECTED

This year's results have revealed a workforce mobilization shift, with **over 50% of respondents using laptops as their primary system.**

This indicates an increase in data mobility and, in turn, a significantly higher risk of business data loss.

Concurrent to the requirement for mobile user data protection is **growth in company bandwidth costs** and an increased need for solutions that address bandwidth & storage optimization.

67% of companies have reported significantly higher bandwidth & storage costs this year.

BACKUP POLICIES

The large majority of companies (47%) rely on a **backup policy instructing user's to backup their data to a file server or external hard drive**, similar to the 46% last year. The number of companies implementing an endpoint backup solution has grown by 3%

As we found last year, user's not following policy was once again listed as the most significant challenge when protecting business data – 34% reported that user's do not consistently follow policy. 6% of companies stated that they have no user data backup solution in place.

FCOM, a trade group composed of 4,000 datacenter managers, conducted a survey in which CIOs and high-level IT directors responded saying **more than 15 percent of data centers have nothing yet in place for data backup and recovery.**

Another interesting result of our 2011 Endpoint Data Loss Survey was the increasing prevalence in

frustration over user data migration projects such as hardware refreshes. If endpoint data is incorrectly backed up, these projects take significantly longer and become more costly. **17% of businesses listed the time it takes to upgrade user's laptops and desktops as a major frustration, resulting from ineffective data backup.**

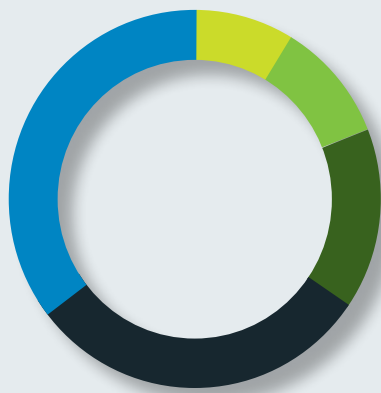
WHICH OF THE FOLLOWING ISSUES ASSOCIATED WITH USER DATA BACKUP DOES YOUR COMPANY EXPERIENCE?



- Users do not consistently follow our policies **34%**
- The infrastructure (bandwidth and storage) cannot cope with large backup volumes **12%**
- Security concerns (users dont want sensitive information on our servers) **11%**
- Upgrading users desktops and laptops takes a lot of time **17%**
- There are no issues **13%**
- High impact on user computers **13%**

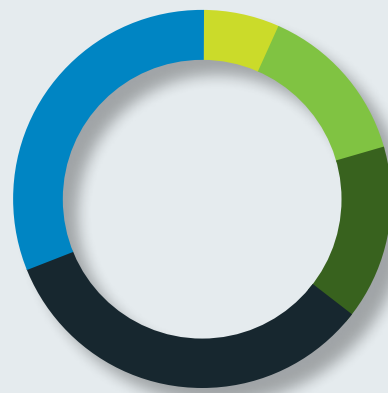
02

HOW DO COMPANIES PROTECT USER DATA? (2010)



- A backup solution for desktops and notebooks **30%**
- Company policy instructing users to backup to an external hard drive **10%**
- Company policy instructing users to copy their files to a file server **36%**
- Folder synchronisation **16%**
- We have no user data backup solution in place **8%**

HOW DO COMPANIES PROTECT USER DATA? (2011)



- A backup solution for desktops and notebooks **33%**
- Company policy instructing users to backup to an external hard drive **16%**
- Company policy instructing users to copy their files to a file server **31%**
- Folder synchronisation **14%**
- We have no user data backup solution in place **6%**

WHAT ABOUT CLOUD?

A new Forrester Research survey of 1,200 IT decision makers found that only 8% of businesses (small, medium, and enterprise) have any current plans to utilize cloud storage and only 3% are using it now. These results suggest that, while there is a lot of potential for cloud storage (43% claimed some interest), concerns about privacy, security, and

pricing are keeping most companies from moving data out of their data centers, at least as a primary storage option.

11% of companies are taking the plunge - these are the **early adopters** and **innovators**. The **early majority** (43%) is interested, and watching. The **late majority** is not in the game, yet.

02

EFFECTIVE ENDPOINT DATA PROTECTION

Reality is that user's do not follow backup policies.

So how does IT take users out of the equation & ensure effective endpoint protection?

To ensure reliable and effective endpoint data protection, companies require a data backup & recovery solution that provides:

- ✓ Centralized data backup policy setting and control
- ✓ Automated endpoint data backup
- ✓ Multiple user management
- ✓ Data recovery simplification and control
- ✓ Consolidated and intuitive reporting.

THE IMPORTANCE OF AN EFFECTIVE ENDPOINT SOLUTION

Most companies are experiencing at least 30% data growth annually.

The SEPATON annual survey of large enterprises with at least 1000 employees and at least 50 TB of primary data states that Data growth continues unabated with more than one third of respondents reporting that their data **was growing by more than thirty percent annually.**

Add to that the ever increasing mobility of vast amounts of data by way of much improved laptop storage, and the requirement for an effective corporate data backup solution becomes paramount.

“30% of companies feel their current data backup solution is moderately to highly ineffective”

HOW EFFECTIVE IS YOUR COMPANY'S CURRENT SOLUTION IN PROTECTING USER'S BUSINESS DATA?



Highly effective	25%
Highly ineffective	8%
Moderately effective	45%
Moderately ineffective	22%

The problem of unreliable and ineffective business data protection is clearly prevalent in corporate enterprises, and the improvement of solutions and strategies is increasingly becoming 'top of mind' for IT.

Ranked as the No. 3 IT priority by more than 500 respondents to ESG's 2011 IT Spending Intentions Survey, **“improving data backup and recovery” takes priority over a number of other IT initiatives** and was edged out only by “increasing the use of server virtualization” and “information security initiatives.”

03

INCREASED ENTERPRISE INTEREST IN ENDPOINT BACKUP

HAS ENDPOINT DATA BACKUP INCREASED IN IMPORTANCE FOR ENTERPRISES?

THE ENDPOINT IMPERITIVE

One of the key challenges acknowledged by Gartner in storage planning for 2012 is that IT tends to look at user data protection in the traditional sense, meaning from the centre out, instead of from the edge, inward – **with the main areas of risk and exposure residing on endpoint user devices such as laptops and desktops.**

Increased user mobility and the requirement for an effective user data protection solution that addresses operational efficiencies as well as reducing required resources and controlling bandwidth and storage spend have resulted in **enterprises placing Improved Disaster Recovery and Business Continuity Planning as their No. 2 spending priority**, according to a recent survey of IT decision-makers conducted by Forrester Research.

“Organizations are waking up to the fact that they have important data resident on endpoint devices that is not adequately protected, but should be.”

(Gartner ID #: G00211731)

HAS YOUR COMPANY CONSIDERED AN AUTOMATED DATA BACKUP AND RECOVERY SOLUTION FOR ITS LAPTOPS & DESKTOPS



- We currently have a system in place **36%**
- We are currently investigating a solution **37%**
- We have considered it, but have not yet investigated the matter **22%**
- We are not considering backing up the data on user laptops & desktops **5%**

03

HAS YOUR COMPANY EVER CONSIDERED AN AUTOMATED DATA BACKUP AND RECOVERY SOLUTION FOR ITS DESKTOPS AND LAPTOPS?



● We are currently investigating a solution	37%
● We currently have a system in place	36%
● We have considered it, but have not yet investigated the matter	22%
● We are not considering backing up the data on user laptops & desktops	5%

Only 5% are not considering automated endpoint data backup and recovery in 2011, down significantly from the 11% last year.

Judging by our survey findings, it appears that a large percentage of companies are realizing the importance of an automated laptop and desktop backup solution. 37% of respondents are currently investigating a solution, in comparison to 15% in 2010.



04

ENTERPRISE BACKUP REQUIREMENTS

WHAT FEATURES / BENEFITS ARE IMPORTANT TO BUSINESSES

The majority of companies listed **reliability as a primary requirement** of a data backup solution. 25% answered that reliable endpoint data backup is their most important priority.

19% of those surveyed answered that simple, fast data recovery is the most important feature, while 23% listed centralized backup policy setting and control as their most important requirement in a data backup and recovery solution.

When comparing different features against each other, the ability to **quickly and effectively recover lost data** was listed most often as 'very important' – with only 2% of companies feeling that speed and reliability of data recovery is not important.

The ability to centrally select the appropriate data for backup, so control over data backup policies, is very important to 70% of enterprises- again highlighting the need for a **solution that provides centralized control and does not rely on users**.

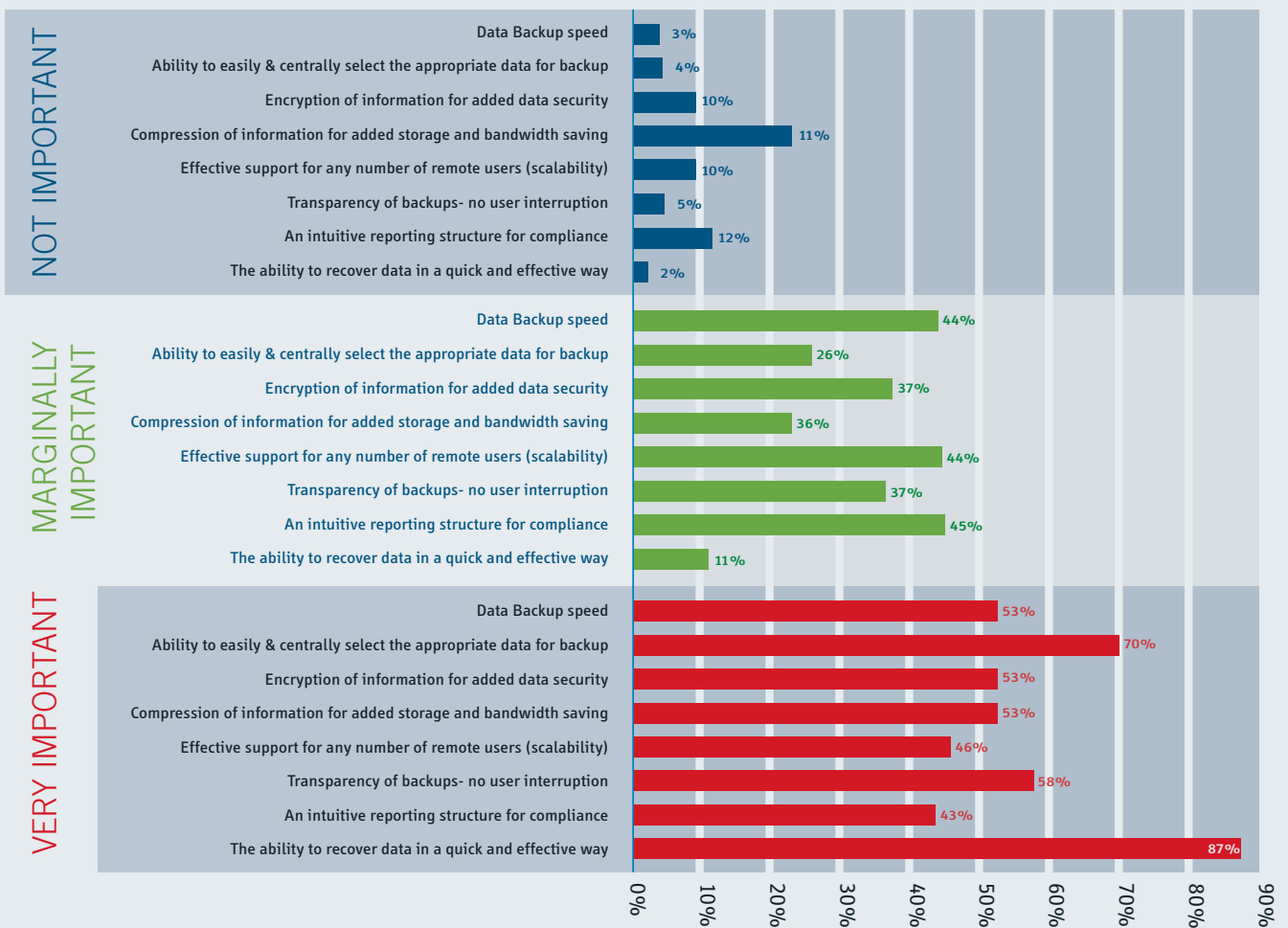
WHAT IS YOUR MOST IMPORTANT PRIORITY WHEN SELECTING A USER DATA BACKUP SOLUTION?



● Reliable endpoint data backup	25%
● Centralized backup policy setting & control	23%
● Non-intrusive end-user experience	15%
● Reduced bandwidth & storage requirements	6%
● Easy install configuration	5%
● Simplified user data migration	3%
● Easier corporate governance and reporting to prove legal compliance	4%
● Simple, fast data recovery	19%

04

RATE THE IMPORTANCE OF THE FOLLOWING IN A USER DATA BACKUP SOLUTION



05

DATA MIGRATION

COMMON COMPANY CHALLENGES

According to independent IT research analysts, Bloor, companies spend over \$5 billion every year on data migration. Add to that a 60% failure rate and the result is a (difficult to ignore) financial incentive to ensure the successful migration of your business data.

SOME OF THE COMMON PROBLEMS ASSOCIATED WITH DATA MIGRATION:

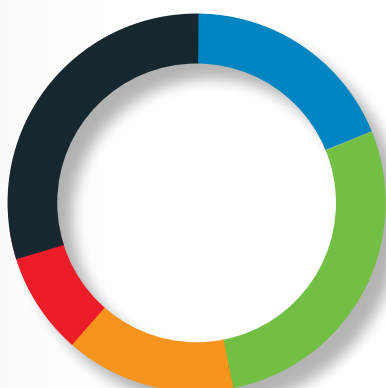
- Data corruption, missing data or data loss
- Extended or unexpected downtime
- Application performance issues

- Technical compatibility problems
- Data isn't restored to original location on a new OS

Our 2011 User Data Loss survey has revealed that the biggest challenge when migrating user data is the user downtime and interrupted productivity experienced with 30% of respondents listing this at their biggest problem experienced when migrating user data.

Locating business data stored in non-standard locations was the biggest issue of 28% of companies, while data loss was listed by 18% of businesses.

WHAT ARE SOME OF THE BIGGEST PROBLEMS YOU EXPERIENCE WHEN MIGRATING USER DATA?



● Data Loss	18%
● Locating business data stored in non-standard locations	28%
● Data confidentiality is threatened	14%
● Inflated bandwidth & storage costs	10%
● Extended user downtime	30%

HAS YOUR ORGANIZATION CONSIDERED A SOLUTION THAT SIMPLIFIES ENDPOINT DATA MIGRATION?



● We currently have a system in place	18%
● We have considered it, but have not yet investigated the matter	28%
● We are currently investigating a solution	25%
● We have not considered this	19%
● Unsure	10%

05

HOW AN ENDPOINT DATA BACKUP SOLUTION ADDRESSES DATA MIGRATION CHALLENGES

01/

REDUCE DATA MIGRATION RISKS

- ✓ IT can easily locate and backup critical data stored in non-standard locations on laptops and desktops, reducing the risk of not migrating all business critical data.
- ✓ Data can be restored on new hardware in the original location- saving time and avoiding increased IT support requests and interrupted productivity.
- ✓ Overcome incompatibilities between operating systems when migrating shortcuts such as My Documents and the user's Desktop.
- ✓ Ensure that Microsoft Outlook archived email stored on user computers is easily migrated.

02/

REDUCE EXTENDED USER DOWNTIME

- ✓ Business data on laptops & desktops is automatically backed up and available for recovery, simplifying company PC refresh processes.
- ✓ Faster recovery to new computers, reduces time required by technical resources.

03/

MINIMIZE IMPACT ON INFRASTRUCTURE DURING DATA MIGRATION

- ✓ Central control over backup policies prevents unnecessary bandwidth and storage wastage caused
- ✓ Data is compressed, preventing inflated operational costs and lowering impact on the network by reducing bandwidth usage.

04/

CORPORATE GOVERNANCE AND REPORTING

- ✓ Abiding by compliance and corporate governance regulation is vital during company PC refresh projects.
- ✓ User data is encrypted, aiding with corporate governance compliance and ensuring confidentiality of business data during migration.
- ✓ Centralized reporting provides an audit trail of the migration process.



06

BUSINESS DATA LOSS

DATA LOSS RISKS & FACTORS

Lost business data is a leading pain-point for businesses, accompanied by an undeniable financial incentive.

When you consider that **the average cost of a lost or stolen business laptop is \$50 000**, (Ponemon Institute Report) with worst-case scenarios reaching close to \$1,000,000- this due to the increasing value of enterprise data and the obvious costs associated with attempting to recover or replace lost files- organizations have a difficult to ignore financial incentive to protect their endpoint data.

This paired with corporate governance requirements, and failure to comply with Governance, Risk and Compliance (GRC) regulations resulting in financial penalties, legal action and reputational damages, a backup and recovery solution for the data residing on endpoint devices is no longer a 'nice to have'.

DO WE UNDERESTIMATE THE VALUE OF OUR BUSINESS DATA?

When asked to estimate the average value of the business data on their laptop or desktop, 90% undervalued their business data. Only 10% of those surveyed believed the cost of replacing this data to be around the \$50 000 mark. This is often because we forget the associated costs of data loss.

COMMON ASSOCIATED DATA LOSS COSTS & RISKS

- Interrupted productivity & extended user downtime
- IT support costs
- Replacement of legal documents
- Recreating business reports and documents
- Managing reputational damage

Data loss can result in huge corporate governance and

compliance ramifications.

To avoid these costs, a company requires effective endpoint data protection that provides simple, fast data recovery.

WHAT ESTIMATE VALUE WOULD YOU PLACE ON ALL THE BUSINESS DATA THAT RESIDES ON YOUR LAPTOP OR DESKTOP?



● \$500 - \$1000	11%
● \$1000 - \$2500	11%
● \$2500 - \$5000	20%
● \$5000 - \$10 000	18%
● \$10 000 - \$25 000	10%
● \$25 000 - \$50 000	20%
● \$50 000 +	10%

06

MAJOR DATA LOSS FACTORS

Companies are constantly at risk of data loss, according to our survey:

- > 36% of data loss is ascribed to hardware failure
- > 29% of data loss is attributed to negligence
- > 18% of company data loss is caused by theft

LEADING CAUSES OF ENTERPRISE DATA LOSS



● Theft	18%
● Negligence	29%
● Hardware failure	36%
● Viruses	9%
● Failed data migration	8%

These statistics highlight the massive risk companies are exposed to daily. A scary thought, especially considering that 11% of businesses have no backup solution in place.

As we've said before: staggering financial, legal and productivity ramifications are just one unlucky day away.

RECOVERING LOST DATA

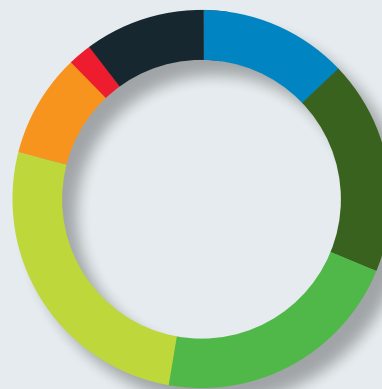
Often organizations aren't interested in an endpoint data backup solution as they wrongly believe that this data is being effectively backed up already, or that the frequency of data loss won't be significant enough to cause any real damage.

Of the companies we surveyed

- **OVER 50% HAVE LOST DATA IN THE LAST 12 MONTHS**

The ability to quickly and simply recover lost data is vitally important for companies, yet 10% of companies surveyed said they would not be able to recover lost data and 27% of respondents said it would take around 24 hours to recover data.

APPROXIMATELY HOW LONG WOULD IT TAKE YOUR ORGANIZATION TO RECOVER LOST DATA?



● Less than an hour	12%
● 1 - 2 hours	19%
● 2 - 5 hours	22%
● 1 day	27%
● 1 week	8%
● 1 month	2%
● We would not be able to recover lost data	10%

07

CLOSING COMMENTS

Data loss is an unavoidable reality for businesses. In the past, this problem was remedied by legacy solutions and most often, the enforcement of a data backup policy.

Enterprise CIO's and IT managers know that relying on the user doesn't work.

- ✓ 34% of businesses listed user's not following policy as the biggest challenge associated with data backup.
- ✓ However, 47% of companies still implement backup policies instructing user's to backup their data to a file server or external hard drive.

This reveals an obvious requirement for companies to move away from this ineffective, high-risk strategy and to find an automated and centralized data backup solution:

59% of respondents are currently investigating or considering an automated endpoint data backup solution.

The increasing mobilization of today's workforce, with around 50% of companies using laptops as their primary system, and the introduction of tablets to the corporate space has meant that business data is often mobile-amplifying the risk of data loss.

With over 50% of those surveyed having lost data in the last 12 months, and 20% saying it would take longer than a week to recover this data, it is obvious that a massive requirement for more effective data backup and recovery exists.

35% of companies have said that data loss is one of their most significant threats but that substantial solutions have not yet been implemented.

Other than reputable analysts representing big names such as Gartner and Forrester pinpointing endpoint data protection as an increasingly imperative enterprise consideration, it is apparent that companies are realising the importance of a built from the ground up endpoint solution that effectively protects endpoint data while providing real operational benefits.

This survey was sponsored by Cibecs - the simplest and most reliable way to backup and recover your enterprise endpoint data. Find out more about Cibecs user data backup and recovery.