CIBECS

PROTECTING USER DATA

CIBECS / IDG CONNECT

2012 BUSINESS DATA LOSS SURVEY

The latest statistics around enterprise endpoint data security.

IDG CONNECT

REPORT

www.cibecs.com

Table of Contents

2012 Data Loss Survey Results:
The State of Business Data Protection 2012

Executive Summary

Data Protection and the Endpoint Imperative

"Enterprise organizations are beginning to become aware of the inadequate protection of important data on corporate laptops and mobile devices. Mobile workers are integral to the success of many businesses and carry data that would be nearly impossible to reconstruct if their corporate devices were damaged or stolen." - Sheila Childs, Vice President of Research at Gartner on backing up business data

The Enterprise IT landscape has seen several significant shifts in recent years due to the fast-paced changes taking place, specifically in the way we **create, access, share and store business data.**

This evolution of macro level trends has been swift, and has resulted in complex IT Data Protection processes, procedures and solutions needing to be procured or created, tested and made scalable.

Data creation is growing at a rapid pace, with a single business's daily data growth reaching Terabytes and being accessed and edited on various devices. Our **exposure to social channels and new technologies has resulted in a cultural shift.** It means that Users manage and share their data differently, leaving business critical information increasingly vulnerable to loss, theft and corruption.

Business stakeholders often recognize the value of (and begin using) new technologies in the workplace before IT departments can harness and implement controls, **resulting in multi-device proliferation and increasingly mobilized and shared data.**

The massive increase in mobile workers *(60% of those surveyed this year use laptops as their primary device)* has meant that **IT can't assume that user-managed, server-focused data protection is a secure data protection strategy.**

It's become absolutely paramount to **begin data protection with endpoint devices, and to completely remove users from the data backup process.**

The effects on IT environments are outlined in what Gartner calls, "the emergence of the nexus of four forces" - the convergence of cloud, information growth, mobile and social into a unified group of forces that are undoubtedly **influencing almost every IT-related decision.**

IT organizations must **respond to the demands resultant of these four forces, while balancing security against access** and continuing to plan for and meet the requirements of users who are more technology-savvy than ever before.

Data protection becomes more demanding with an intricately complicated environment. The **consequences of data loss have also become increasingly legislated and costly**, and the business benefits of employing a simple, effective and secure solution are now more tangible than ever before.

However, for a surprisingly large number of companies with between 10 and 1000 employees, the perception from IT Departments is that **C-level Executives don't experience enough of a sense of urgency around protecting their endpoint business data.**

Multiple industry-offered reasons for this relaxed approach were submitted to us, including:

- *'Our CEO does not recognize the consequences of Data Loss'*
- *'Our C-level Executives don't believe that an automated data backup solution is necessary'*
- *' Executives don't see the value, and IT is left resolving the issues around lost data'*

What should however be obvious to all decision makers is that **any technology decisions heavily impact the business,** and can either positively initiate business success, or lack of adoption can result in slower processes, negatively affected productivity and costly and damaging data loss disasters.

It is widely agreed that with increasingly legislated consequences to ineffective data risk management, **all business decision makers and C-level executives will need to ensure that their organization is employing the right measures to protect their business data.**

This 2012 Data Loss Survey (results) white paper serves to examine the current effects on business data protection and management, as well as forming an analysis of Data Protection strategies of companies globally.
We further explore how perceptions on the importance of data protection are changing, and what business data protection challenges are in 2012.

The survey has been sponsored by Cibecs in partnership with the IDG Connect. The results analysis has been compiled by Cibecs. Cibecs develops an automated, centrally managed endpoint data protection solution built for enterprise environments.

01

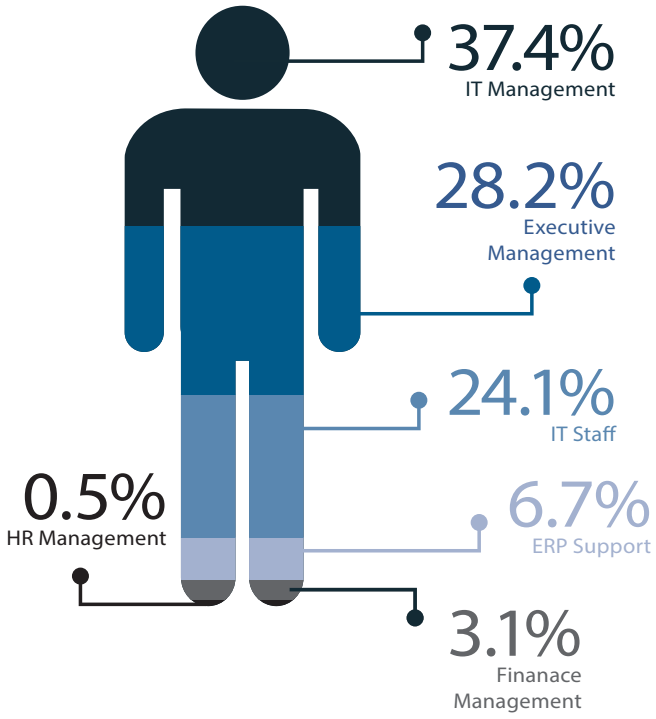
Who Participated in the Survey?

The Cibecs 2012 Data Loss Survey participants mostly consist of IT management and IT staff, with over 50% of participants working in IT.

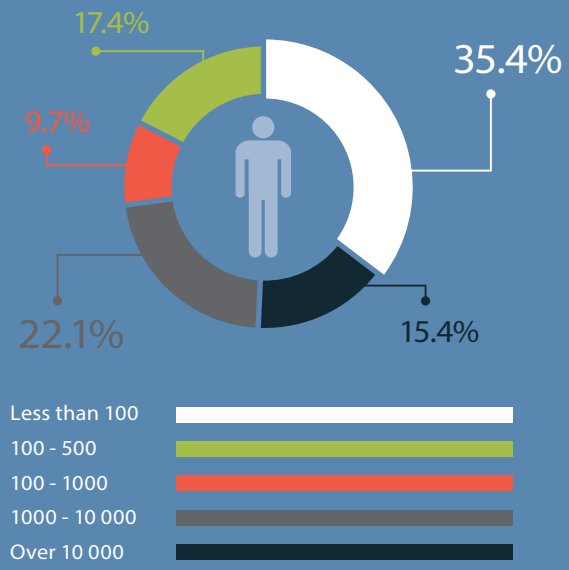
The participants of the 2012 Data Loss Survey are mostly employed by companies with over 100 users, **37% of respondents work for enterprise organizations of over 1000 users.**

In total, over 200 (mostly enterprise) organizations were represented, with respondents' geographical locations split as follows: **27.2% North American, 18% EU and 48.7% African, with 5.6% of respondents Asia based.**

WHAT IS YOUR ROLE IN YOUR ORGANISATION?



HOW MANY PEOPLE DOES YOUR COMPANY EMPLOY?



02

The Effects of Data Mobility on Business Data Protection

User Mobility and Data Protection

Last year, **around 50% of users employed a laptop as their primary work device. In 2012 that percentage has risen to 60%** - illustrating the fast and definite trend towards increasingly mobile users.

Mobilized data **increases business vulnerability to data loss, data theft and data corruption,** as companies have less centralized control over their business information. Increased mobile workers can also mean **increased data costs and certainly more complicated endpoint data protection requirements.**

20% of our survey respondents stated that their biggest data protection challenge is that increased data mobility has required specialized endpoint data protection.

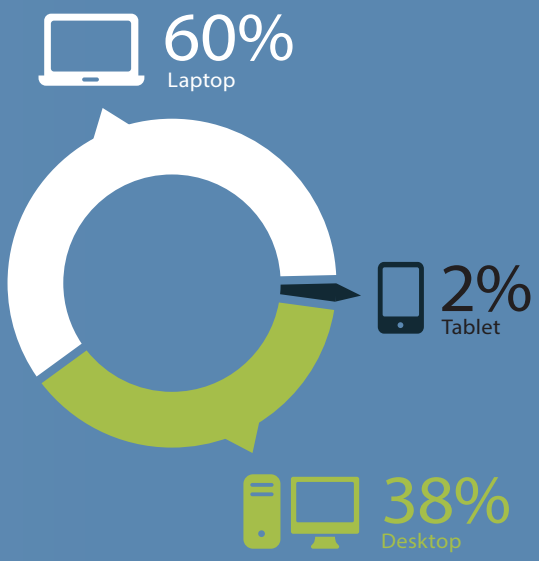
With more than half of executives utilizing laptops as their primary device – we have seen the IT mindset change from server data protection to an outside, inwards approach – **looking at endpoint devices as the start of an organizations data protection strategy.**

Organizations that are effectively protecting their data understand the importance of ensuring that data protection is focused on the endpoint- **automating laptop & desktop data backup and simplifying the recovery of any lost files**.

Mobile users also lead to an **increasing lack of company control.** Expecting that users will follow a data backup policy where they are required to backup their own files to a central server, or external hard drive, is **putting business data at severe risk.**

Surprisingly, almost *36% of companies are still utilizing antiquated data protection strategies* where they expect User's to follow policy and manually backup to either a central server or an external hard drive.

WHAT DO YOU USE AS YOUR PRIMARY ENDPOINT DEVICE



02

Bring Your Own Device (BYOD)

Only 3% of those surveyed feel that BYOD is their biggest data protection chellenge

Bring your own device has had an obvious impact on the responsibilities of IT Management. The relatively recent (and virtually unstoppable) trend of allowing the use of personal devices to access company resources has resulted in the necessity for **improved control and security.**

Today, BYOD has become a commonplace business IT challenge as **more companies need to cater for a large number of users, including C-level execs, who want to access email and other company data on the device of their choice.**

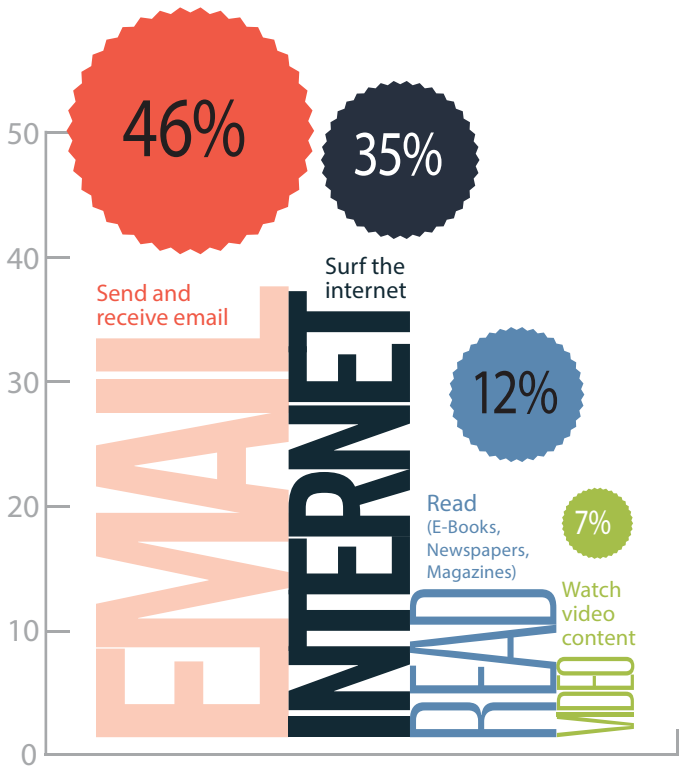
40% of respondents reported that their companies allow BYOD – and another 8% are planning to. Which still leaves the majority of 52% who do not allow BYOD in the workplace.

When it comes to BYOD we've seen how the iPad has started to infiltrate the corporate space – but it seems that **only a small percentage (2%) of professionals are using their iPad as a primary work device.**

Instead, the majority of professionals use their iPads to send and receive mail, browse the web, read and present to clients – making it largely a data consumption device.

Although it was expected that the iPad would have a more significant impact on this year's results, the majority of **Executives use their iPads as a secondary, consumption device.**

MOST FREQUENT USE OF TABLETS AMONG MOBILE WORKERS



02

Should Users be Given Control?

We've seen a **significant increase in user mobility and technology independence**. This in turn increases company risk of data loss **if backups are not automated and centrally managed**. Every year we report the same result – companies who employ user-managed data backup end up losing their data.

Almost every single survey respondent (who stated that their company expects users to follow a data backup policy) reported *users not following policy as their biggest data protection challenge.*

- Of the companies expecting users to backup their data to an external hard drive or central server, according to company policy – 94% said users do not follow policy.
- An automated and centrally managed data protection solution is vital to ensure effective company data protection.

03

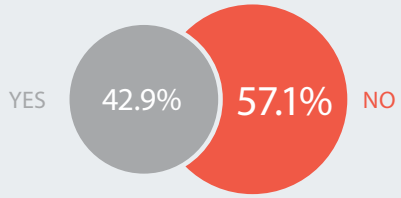
Do you believe that your Business Data is effectively protected?

How companies are securing their data

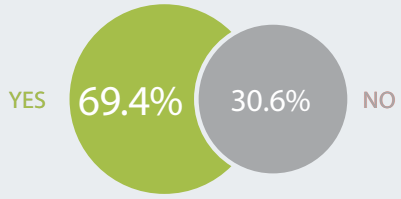
Only 43% of those surveyed feel secure that their data is completely protected from data loss and data breaches. This should clearly be a warning sign to organizations and IT management as **users do not generally feel that they are being effectively protected.**

- **37% have no real protection against unauthorized access to their data** if they had to lose their laptop, meaning that their companies are not compliant with Corporate Governance and that **company and customer data is severely at risk.**
- If these Executives were to lose their business data **only 69% could recover their files.**

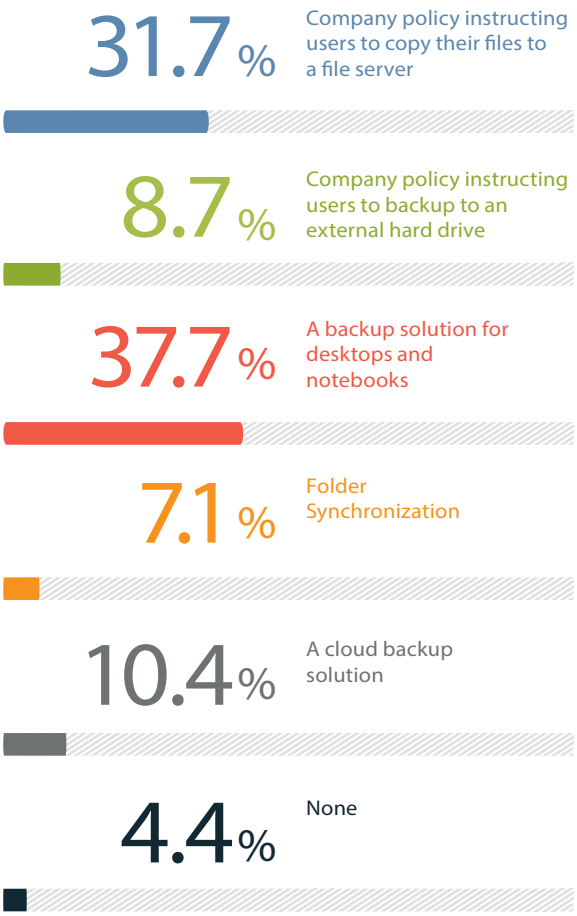
Do you feel secure in the knowledge that your endpoint data is 100% protected from data theft, data loss and data breaches?



Can your company recover all your critical data for any and all users, the next time there is an incident?



HOW DOES YOUR COMPANY CURRENTLY PROTECT BUSINESS DATA?



04

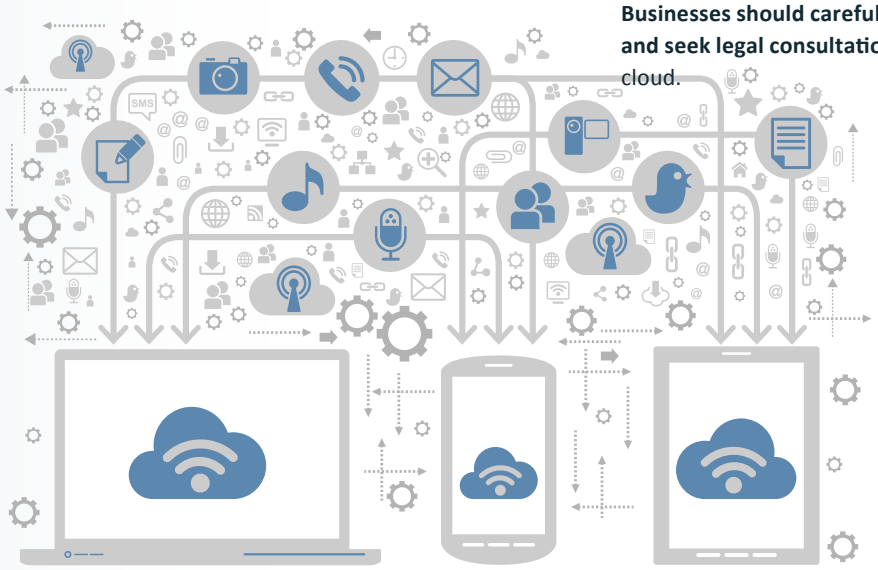
The Cloud Movement

Of our participants in 2012, 10% are employing a cloud backup solution.
> The majority of these are SMB's of less than 100 users.

Often businesses move their non-critical functions or data into the cloud first **to test the environment and their appetite for cloud.** They might then begin to migrate more business critical data.

However, due diligence is required, as Cyber Criminals are often actually looking for the data we may consider 'non-critical' such as our ***processes, our marketing plans and templates, and our company strategies.*** Attacks on Public Sector, the Health Industry and Government departments are specifically common.

- The RSA (Security division of EMC) data breach reportedly cost the company around $43M, sending a clear reminder to organizations of the importance of ensuring they **consider the possible security concerns associated with Cloud backup.**
- Another consideration is the **jurisdiction in which the 'cloud' sits.** Businesses need to ensure they understand **where their data is being stored geographically, and what the Legislature around Data Protection and Cross Border Data Transfer is in that country.**
- It is further important that organizations **understand how to mitigate their risk and ensure that they have a full understanding of all the Service Provider's contracts**. This is vital as, in many territories, there is a complete lack of legislation pertaining to Cloud Service Providers. The result is that **the company is constrained by the Service Provider's Terms and Conditions and thus vulnerable if the correct due diligence doesn't take place.**



Businesses should carefully assess the Provider's liability and seek legal consultation before moving data to the cloud.

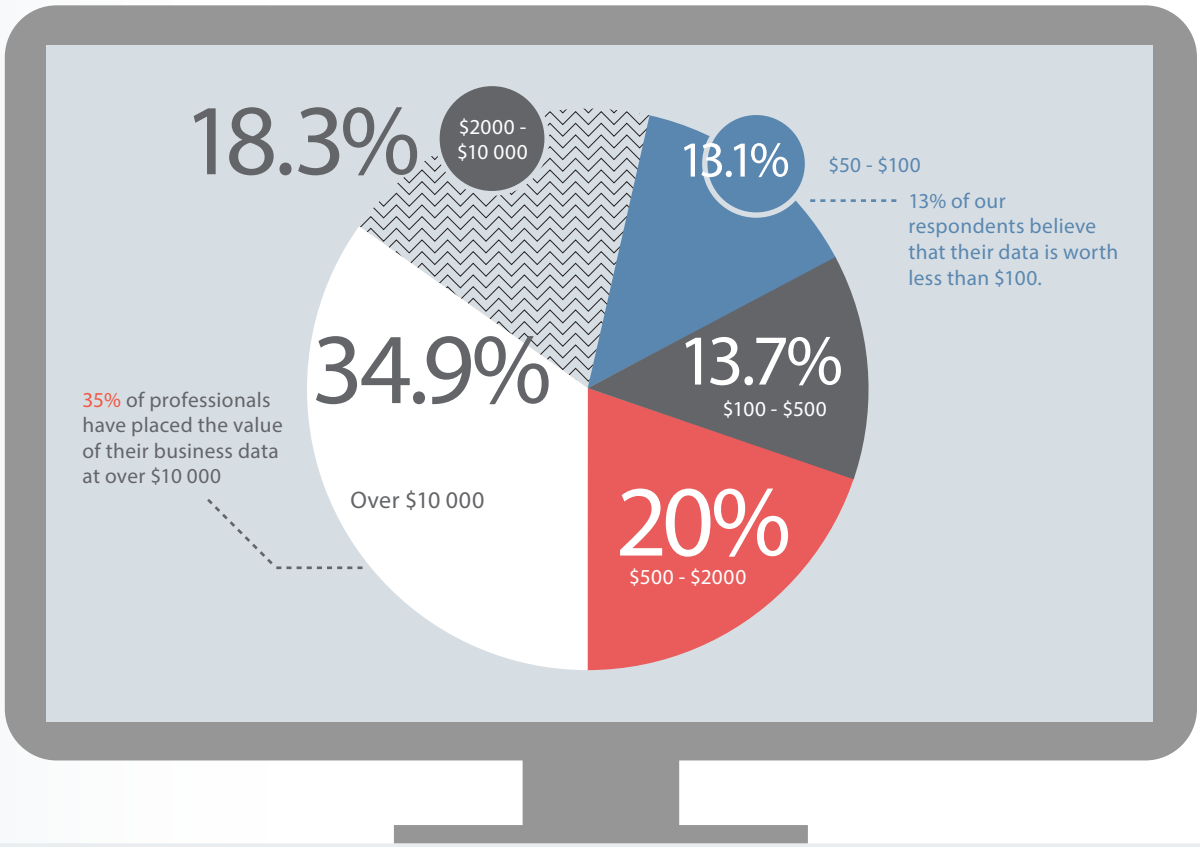
05

The Perceived Value of your Data

With 30% of businesses having *no way of recovering lost user data*, do organizations and executives fail to see their business data as valuable?

35% of professionals have placed the value of their business data at over $10 000 – and only 17% of our respondents believe that their data is worth less than $2 000.

WHAT DO YOU ESTIMATE IS THE VALUE OF THE BUSINESS DATA ON YOUR LAPTOP OR DESKTOP?



06

Data Loss 2012

Of those surveyed, 22% have already lost data this year – and another 14% lost data last in 2011.

The majority of those who can recover their data if lost say it takes them **between 1 and 5 hours to get their data back.**

29% of respondents will take about a day to restore lost files and 10% say it takes them about a week to get their data back.

The Consequences of Data Loss

We have already established that around 30% of professionals can't recover lost data. **What are the business consequences to data loss – other than the obvious costs and the value of business information?**

Governance, Risk and Compliance (GRC)

A vital consideration when estimating the value of your data is the **associated consequences of ineffective data protection.**

Compliance and Risk may have been an afterthought in previous years, but as the risks of data loss, theft and data breaches increase –alongside the importance of protecting personal data, customer information and company secrets – **the penalties of Non-Compliance have become severe.**

Legislation holds the board responsible for data security

Legislation around the world from the US, UK, EMEA and other regions are being aligned to guarantee the protection of critical information and hold company board members responsible for doing so. Notable legislation includes SOX and HIPAA in the USA and the incoming Protection of Personal Information Bill (PPI) in South Africa.

A recent US example of data loss consequences was the **HIPAA non-compliance penalty on BlueCross BlueShield of $1.5 million to the federal government** - a harsh warning to the Healthcare and Insurance industries to ensure effective data protection.[1]

The fine however is not the only expense of this Data Loss incident. Since the data was lost in 2009, the company has spent around **$17 million in costs on:**

- ✓ investigation
- ✓ analysis
- ✓ notification
- ✓ improved data protection efforts

This is a sure indication of the costs of HIPAA non-compliance, and how **severe the associated costs of data loss can be.**

[1] http://cibecs.com/blog/2012/03/15/over-17-million-the-cost-of-data-loss-and-hipaa-violation-for-blue-cross-blue-shield/

06

"This settlement sends an important message that the Office for Civil Rights (OCR) ***expects health plans and health care providers to have in place a carefully designed, delivered and monitored HIPAA compliance program,"*** said OCR Director Leon Rodriguez. [2] "The OCR will continue to vigorously protect patients' right to private and secure health information."

Whereas before the consequences of data loss may have been limited and perhaps considered unsubstantial enough to warrant procuring an automated and centrally managed solution – this has changed.

> Data is the new business currency.

Companies can't afford to be lackadaisical about data protection. **Organizations need to understand what legislation is relevant to them and the industry within which they operate, and then get expert advice to ensure compliance.**

- It is critical for organizations to take a **bold step away from generalized and vague approaches to Governance, Risk and Compliance.**

Financial Penalties, Legal Action and Incarceration

User laptops may contain data that **isn't perceived as a risk to the company if lost.** What we do not realize is that data such as email addresses, phone numbers, personal information, company strategy, staff details and any legal documentation is **exceptionally valuable and can create huge reputational damage if lost.**

Businesses are going to very soon face serious penalties if they don't carefully consider the risks of ineffective data security – these penalties include fines or even jail time, particularly if the company is found of guilty of gross negligence through **knowingly employing an ineffective data protection strategy.**

The increasing prevalence of APT Cyber Crimes (Advanced Persistent Threat) has meant that organizations need to ensure they invest in effective user data protection. These Cyber criminals are interested in exploiting company or individual 'secrets' as this has become some of the most valuable data on the Cyber Crime black market.

Rampant theft of Medical Records in the US

- Between September 2011 and November 2011, a government benefits program suffered the theft of EHRs of 4.9 million military personnel, the health information of 4 million patients of a reputable US West Coast healthcare system were stolen electronically and a major academic medical center inadvertently disclosed the EHRs of 20,000 of its patients.[3]

> Medical Records currently sell for about $50 per record on the black market.

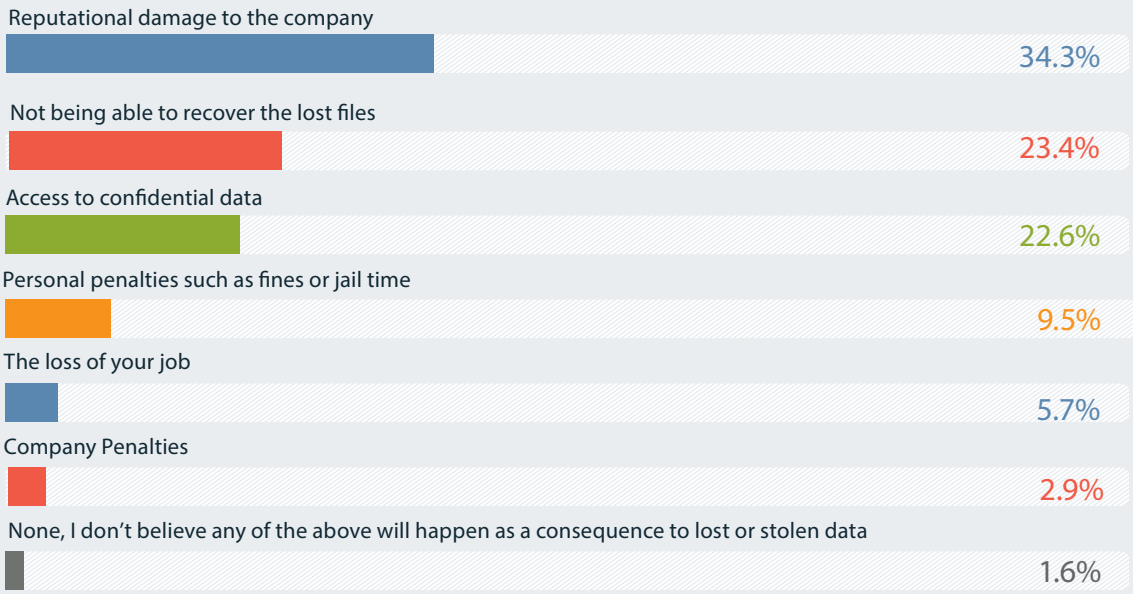
The loss of custodial data results in massive fines, legal consequences and financial penalties – however the theft of company Knowledge Bases has been overlooked and is proving to be exceptionally popular.

[2] http://www.hhs.gov/news/press/2012pres/03/20120313a.html
[3] http://www.cio.com/article/701492/Healthcare_Industry_CIOs_CSOs_Must_Improve_Security

06

The Most Concerning Data Loss Consequences

WHICH OF THE MOST COMMON CONSEQUENCES OF DATA LOSS CONCERNS YOU THE MOST?



When we asked our participants what they saw as the most concerning consequences of Data Loss, **the majority of executives listed reputational damage to the company.**

This is an exceptionally damaging repercussion which has resulted in **extremely serious consequences for organizations**. If customers believe that their data is at risk – they are much less likely to want to do business with that enterprise.

A recent survey revealed that 84% of consumers would no longer deal with a company if they were informed that the company had lost their Personal Information.

The second and third most concerning data loss consequences were not being able to recover files and access to confidential information.

Under 2% of professionals don't believe there are any consequences to losing business data.

Make.Believe? SONY counts the true cost of data loss.

The Ponemon Institute estimates that last year's data breach at SONY will cost the company an absolute minimum of $5.6 billion – with the majority of cost attributed to "expense outlays for detection, escalation, notification, and after-the-fact (ex-post) response" as well as the "economic impact of lost or diminished customer trust and confidence as measured by customer turnover, or churn, rates."[4]

[4] http://www.zdnet.com/blog/btl/sonys-data-breach-costs-likely-to-scream-higher/49161

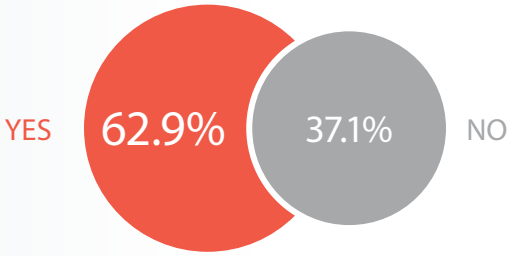
07

Who is Responsible for Data Loss?

With increased and legalized data protection requirements, and more severe penalties in place, who is responsible for lost data?

If a company has communicated their data protection policy to its employees and a **user loses Private Information** which results in a Law Suit– that user could be held **personally responsible.**

ARE YOU AWARE THAT YOU MAY BE HELD PERSONALLY LIABLE FOR LOST COMPANY DATA - WITH CONSEQUENCES VARYING FROM FINANCIAL PENALTIES TO JAIL TIME?



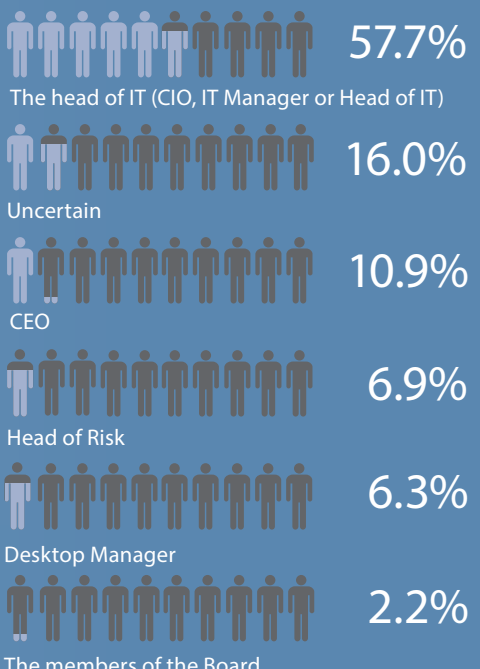
Only 63% of our respondents are aware of the personal liability attached to protecting their data, the other **37% did not know that they may be held personally responsible for lost confidential company data.**

Most companies have given ownership of data protection to a specific employee, who is then responsible for formulating a data protection strategy, for implementing the appropriate solutions and procedures – and understands the required Compliance regulations and legalities.

Of the companies we surveyed, it is most often (58%) the responsibility of the Head of IT to ensure effective business data protection.

- 11% stated that it is the CEO's responsibility, and 7% said the responsibility lies with the Head of Risk.
- 16% were unsure of who in their organization is responsible for protecting business data.

WHO IS RESPONSIBLE FOR ENSURING THAT YOUR COMPANY AND USER DATA IS EFFECTIVELY PROTECTED AND SECURE?



08

What do Companies want from a Data Protection Solution?

The requirement for effective data protection is obvious. Businesses need an automated, centrally controlled data backup and recovery solution that does not rely on users if they want to protect themselves from Data Loss and the associated risks and problems.

Considering the vast proliferation of solutions on offer – how do businesses select a Data Protection solution that will secure their data, while offering the required software features and benefits?

The professionals we surveyed said that protection from data loss is the most important consideration.

- ✓ 49% said that finding a solution that ensures complete protection against business data loss is paramount.
- ✓ 22% said that Corporate Governance Compliance is the most important benefit of effective data protection. Some data backup and recovery solutions are optimized to assist with GRC.
- ✓ 15% said that the associated operational cost savings are the most valuable benefit. While data backup and recovery software protects businesses from data loss – these solutions may also offer multiple features that support reduced overheads.
- ✓ 4% of professionals feel that reduced bandwidth & storage requirements are the most important benefit
- ✓ 3% believe that simplified Data Migration Projects would benefit their business most.

It's important that companies exploring data protection solutions understand the available benefits of advanced software solutions – and that the initial investment of Data Protection often results in huge cost savings in bandwidth and storage, reduced support requirements, simpler data migration projects and prevention of interrupted user productivity.

These solutions further protect companies from the massive cost of data loss.

This results white paper was compiled by Cibecs – providing enterprise organizations with the simplest and most secure laptop & desktop data protection.

If you are interested in a 30 minute WebEx presentation of our Enterprise Data Protection solution please Contact us: info@cibecs.com

09

ABOUT CIBECS

Cibecs is the simplest, most efficient solution for business endpoint data protection.

CIBECS LAPTOP & DESKTOP DATA PROTECTION OFFERS KEY BENEFITS, SUCH AS:

- Central control over user data backups – daily backups are automated, invisible and secure
- Protection against data loss and the consequences
- Faster, simpler data migration
- Reduced bandwidth & storage costs by up to 90%
- Quick and easy data recovery
- Ensure data protection Corporate Governance Compliance
- Intuitive reporting

> **Visit the Cibecs Website: http://cibecs.com**

> **Request more Information: info@cibecs.com**

Thousands of businesses across the globe trust Cibecs .
Cibecs customers include *Ingram Micro, GreenPeace, Unisys, Dimension Data, Absa, University of Witwatersrand, KPMG, Barloworld Automotive and the South African National Prosecuting Authority*

Visit www.cibecs.com for more information or contact Cibecs on +27(11) 791 0073.

CIBECS
PROTECTING USER DATA