



# Quantifying the ROI of IT Security

Becrypt Whitepaper  
January 2010

## Introduction

With the majority of banks and other financial institutions maintaining a very tight grip on their lending purse strings, most corporates are having to justify each additional request for IT expenditure they make.

At the same time, corporate IT managers are under significant pressure - either from their boards or other senior management, including investor sources - to justify their current security expenditures in the face of continuing shareholder scrutiny on all expenses.

Whilst historical evidence suggests that IT security has been an essential part of the necessary investment aspect of business for a number of years, there are signs that IT budgets generally are being cut in the face of the current economic situation.

Data leaks and losses – the main result of poor IT security - have, unfortunately, been with us since the earliest days of PCs in the 1980s.

But the good news is that solutions to data leaks and losses have been available to PC users since the mid-1980s - as leakage and loss risks were discovered, so the industry developed an increasing range of sophisticated solutions.

The arrival of the Internet as a mass communications medium in the late 1990 changed the ballgame significantly, however and even the best security technologies of the period - and security best practices - could not prevent a raft of data leaks and losses occurring.

The net result of these losses was the development of a number of laws designed to penalise those organisations that failed to implement best practices and policies on data leaks and losses, as well as enforcing those policies using relevant security technologies.

The plethora of legislation that seeks to prevent data leaks and losses in UK organisations include the Data Protection Act and, of course, where the company is trading with the US organisation, there is the Sarbanes Oxley Act.

But are organisations adhering to the requirements of this legislation?

## **Understanding the need for IT security**

Unfortunately for the audit and IT security function, Moores Law - the assertion by Intel's co-founder Gordon Moore in 1965 that the power of technology would double every two years - has meant that, as fast as auditors and IT security managers create their own control systems, they quickly became outmoded.

A classic example of this is the Internet, which, despite popular folklore, actually evolved in the 1980s, but took until the late 1990s before mass-market acceptance of the technology meant that information sharing became a technology concept.

This meant that auditors and early IT security managers of the 1980s were frequently hit by security leaks as a result of new technology being introduced to the office mix before they had a chance to analyse the technology and evolve protective systems.

Even at the turn of the century, IT security managers were caught flatfooted - in the nicest possible sense - when the first USB sticks, known as DiskOnKeys, were imported by IBM from the Far East in early 2000.

Although the media has a habit of pigeon-holding IT security incidents into distinct categories when reporting on them, it is important to understand they all fall into the main topic of security events.

These events can be divided up into a number of categories, including:

### ***Intentional actions***

- the intentional deletion of a file or program

### ***Unintentional actions***

- the accidental deletion of a file or program
- the misplacement of DVDs, CDs or floppy disks
- administration errors
- the inability to read unknown file format

### ***Failure***

- Power failure, resulting in data in not being saved
- Hardware failure, such as disk crash.
- Software crash or freeze, resulting in data not being saved
- Software bugs or poor command systems
- Data corruption - file or database corruption

### ***Disaster***

- Natural disaster, earthquake, flood, tornado, etc.
- Fire

## ***Crime***

- Theft, hacking, sabotage, etc.
- A malicious act, such as a virus or theft of physical media.

Studies have consistently shown hardware failure and human error to be two most common causes of data loss, accounting for roughly three quarters of all incidents (Source: <http://bit.ly/2qQ5wA>)

A commonly overlooked cause involving IT systems is a natural disaster. Although the probability is small, the only way to recover from data loss due to a natural disaster is to store backup data in a physically separate location.

## **Understanding the need for risk analysis**

Whilst there are a good number of IT security solutions available in the marketplace, preparing the way for selecting and purchasing a solution requires the use of risk analysis procedures.

The good news is that our belief here at Becrypt is that the process is far from complex. All that is required is to break down the process into a series of stages and, as a result, implementing the process is more about good planning than the high degree of IT security knowledge that many in the industry claim.

Good research in almost any organisation will reveal that the main threat to data integrity comes from insider in that organisation, and typically from employees who will relay data outside their business environment for either accidental or malicious reasons.

Companies need to be protected in all instances to ensure their information does not walk out the door.

The first step to ensure that corporate data is protected is to make sure laptops are encrypted.

Our observations suggest that failing to encrypt employee notebooks is a potentially fatal mistake, but it is not the only step to protection. Organisations need to make sure the encryption can be revoked when an employee leaves the business.

This requires having an encryption policy that is centrally managed by reliable IT systems. This type of policy will keep data protected while enabling IT to lock it from unauthorized employee access at any time.

The next step is ensuring employees cannot transfer information to a USB, MP3 player or other portable device.

Implementing device control allows the IT department to monitor and restrict data copied to removable storage devices to prevent it from leaving the business's control.

Having control over devices on the network also allows IT to understand how internal compliance is working and block any attempts to violate IT security policies.

The final step in protecting data on your network is to ensure employees cannot send information outside to personal email accounts or through instant messaging.

## **Implementing the required pre-purchase procedures**

Largely as a result of the economic down cycle - and, ironically, the increased use of IT in workplace - a growing number of organisations are employing staff on minimum wages - or slightly above this level.

Because of the trend towards less skilled employees and a requirement to cut costs at the staffing level, there is much greater strain being placed on the supervisory function in most organisations.

And just to make matters worse, the constant impetus to cut staffing costs means that many businesses are actually reducing the level of supervision that they use.

The bad news is that the consequent reduced supervisory function means there is a greater risk of an employee making an error or, perhaps worse, actively defrauding their employer.

These frauds can involve collusion between the staff within an organisation outsourcing the work concerned, and staff at the business supplying the outsourced facilities.

To counter these - and allied - problems, it is necessary to employ a carefully defined analysis of data security systems and procedures before a decision on which security technology is the best option for your organisation.

***The four main stages in this analysis are as follows:***

- ID management - who is authorised to do what and when
- Regulatory requirements
- Data handling processes - where is the company's data located?
- Staff change management - when someone leaves, what happens?

Cloud computing - the process of storing, sharing and accessing business data on the Internet, rather than on private servers owned or operated by the organisation - changes the ballgame significantly.

Provided, however, the IT security technology that is being employed - or planned - by the organisation can handle cloud, as well as conventional IT data storage systems, the gap between network and cloud-based security analyses is, again, not as great as some experts report it to be.

Becrypt's observations with clients, in fact, suggests that implementing effective IT security technology can help to reduce the operational risk profile of cloud computing.

It is, however, important to understand that we are still at the pre-contract stage at this point, so traditional steps such as service level agreements, remediation procedures and penalty clauses are not relevant considerations.

What is required is an assessment of the expectations that management have for the cloud outsourcing contract - what precise functions are required to be completed by the outsourcing company?

This is actually a multi-step process as steps one and two (of the four detailed above) can help to reduce the risk profile of the outsourcing project and, in turn, require steps one and two to be revisited until the outsourcing risk profile is at its lowest possible point.

## **The role of KPIs in measuring security effectiveness**

Key Performance Indicators (KPI) are now a primary means of calculating the effectiveness of almost any IT and business solution.

As a result, the best approach with security technology is to align the KPIs with your organisation's overall data protection strategy.

It's also important to note that linking performance and operational KPIs to your security strategy will allow your organisation to more effectively measure its performance.

This will ultimately enable you to make more informed business decisions.

Commonly used KPIs that can be used in your security strategy plan should include:

- the number of security incidents
- the percentage of network coverage,
- the percentage of application coverage.

To make this process as seamless as possible, you should seek to eliminate analysis and reporting activities that are not directly aligned with the KPIs or security strategy.

## **Measuring productivity gains from IT security**

Measuring gains in productivity from improved levels of IT security is all about measuring the increase in the effectiveness of the resource in question.

To better execute the measurement process, it is necessary to assign roles and responsibilities in your organisation.

A detailed Responsible, Accountable, Consulted, Informed (RACI) matrix and staffing model will help you determine how the various functional areas within your organisation factor into the planning, design, implementation, and operation of the overall security solution.

In addition, a well-researched and effective RACI clearly defines each stakeholder's role and helps facilitate stakeholder buy-in.

It's also important to understand the organisational culture within your business operation and other directly connected companies and agencies.

Depending on the vendor, end users may consider the security products you plan to deploy as being intrusive.

A sound understanding of organisational culture will help you establish which features are important to your organisation and how much impact users are willing to bear.

This will help you achieve a smooth, complete, and successful implementation. It also helps to identify the owners of the data.

Data owners understand the importance of their data in relation to the business and should be the primary decision makers involved in remediation efforts.

You should immediately identify the data owners; establish relationships with them; and engage them in effective, ongoing, two-way communications with those owners.

Analysing the existing technology and process controls will help you identify control gaps. You should base your security assessment on an established risk management framework and detailed classification scheme.

You should also ensure that you cover all areas of the organisation, catalogue the location of sensitive data, estimate the amount of exposure the organisation faces, and measure the potential magnitude of the loss of sensitive data.

## **Quantifying ROI from your IT security**

Measuring Return on Investment (ROI) from your security solution is not that different from measuring the ROI from your entire IT system

You should consider obtaining stakeholder buy-in to the security solution from across the entire organisation.

While deploying your security solution, be sure to involve the stakeholders from the beginning. This helps to ensure that the parties fully understand the business requirements and the impact they may have on operations, employee behaviour, and corporate culture generally.

Stakeholders will generally include representatives from the following groups: privacy, IT, security, investigations, human resources, legal, compliance, audit, and the direct lines of business.

To help you measure the ROI from your security investment, you should ideally use technology solutions to detect and prevent data loss in your organisation.

It's also important to remember that deploying IT solutions typically occurs modularly.

Using a modular approach allows your organisation to continue to provide the greatest coverage with the least amount of internal disruption.

This approach will make it possible for your organisation to seamlessly implement more robust data protection solutions down the line, as technologies mature and your business needs dictate.

## Conclusions

Security technologies are designed to address three distinct scenarios: data at rest, data in motion, and data at the endpoint.

Protection techniques aimed at each of these scenarios offer distinct benefits and mitigate different types of risk.

Data at rest typically resides within stationary repositories, such as file systems, databases, desktops, and groupware.

Common risks associated with this type of data include the lack of visibility into where sensitive data is stored, the lack of understanding around who has access to the sensitive data, and the lack of secure storage for sensitive data to prevent theft and loss.

Using effective IT security technology to address these issues will allow your organisation to reduce the proliferation of sensitive data and so enable your business operation to improve its data protection controls.

Data in motion usually consists of information that is electronically transmitted outside an organisation's network via e-mail, online chat rooms, and other methods.

Common risks associated with this type of data include the loss of sensitive data through various communication mediums, the harvesting of sensitive data by malware, and broken business processes that expose sensitive data.

With effective security technology, you can stop sensitive data loss through electronic means, and help enforce compliance with local and federal regulations, as well as corporate standards and policies. You can also identify broken business processes.

Finally, data at the endpoint relates to information stored on laptops and portable storage devices. Stolen laptops and portable storage devices provide unauthorised individuals with portals into your data storage and transport endpoints, and give them immediate access to offline data.

You should also continuously refine your security policies in order to maximise shareholder value from your IT security solution.

IT security is far from being a 'set it and forget it' technology - as the technology is deployed and starts to embed itself in your organisation, you can refine your policies to be more accurate.

And in this way maximise your ROI from your IT security system, and so generate the best return for your bottom line and, of course, your shareholders.

# #becrypt

All product names referenced within this document are trademarks or registered trademarks of their respective companies.

Becrypt Ltd disclaims interest in the marks or names of others. While every effort has been made to ensure technical accuracy, information within this document is subject to change without notice and does not represent a commitment on the part of Becrypt Ltd. No part of this document may be reproduced or transmitted in any form, electronic or otherwise, without the expressed consent verbal or written of Becrypt Ltd.

For more information please call 0845 838 2050 or +44 (0) 20 3145 1050; fax 08458382060  
Becrypt Limited, 90 Long Acre, Covent Garden, London WC2E 9RA. [info@becrypt.com](mailto:info@becrypt.com) [www.becrypt.com](http://www.becrypt.com)

© Copyright 2010 by Becrypt Limited. All Rights Reserved. The Becrypt logo and trademarks are owned by Becrypt Limited. No material may be reproduced for any purpose, private or commercial, without prior written permission from Becrypt Limited.