The Data Protection Imperative

Time to take notice, time to become proactive

Freeform Dynamics Ltd, July 2013

Sponsored by:

commvault

Introduction

As a business manager or executive, the detail of how information is stored and administered in your organisation's computer systems may not be something you spend a lot of time thinking about. However, the chances are that at some point in your career you will have suffered from or witnessed some kind of systems failure or security incident, in which important data was lost or ended up in the wrong hands. It's at times like this that your attention is often drawn to the need for some improvement so it doesn't happen again.

Beyond this kind of catastrophe, there is usually only one other situation in which electronic information handling makes it onto the senior management agenda. This is when additional regulation appears that mandates a new or different way of tracking and reporting the organisation's activities.

If any of this sounds familiar, and/or if your IT team is pressing for more investment so they can do a better job in this area, then we would encourage you to read on. In the remainder of this short paper, we are going to spell out why the time has come to adopt a more proactive approach to what IT people call 'data protection', and how the discussion should be about cost and value, as well as risk.

What, specifically, is included in this discussion?

Unfortunately, like so much of the other jargon in IT, the term 'data protection' is ambiguous. If you operate in the EU, there is then further confusion because of the existence of the 'Data Protection Directive', along with national equivalents such as the 'UK Data Protection Act'. While such legislation is about information management in one sense, its scope is limited to the assurance of citizen privacy when personal data is held by a business entity. IT professionals tend to apply the term differently.

In line with this, for the purposes of our discussion here, we will be using 'data protection' as a collective term to refer to the following activities:

- Securing sensitive business information so it doesn't end up in the wrong hands
- Taking measures to prevent important information from being permanently lost or corrupted
- Maintaining high availability of information that's critical to business operations
- Ensuring that critical information is brought back online quickly in the event of a systems failure
- Archiving historical data in an efficient, tamper-proof and easily accessible manner

In order to facilitate these activities, a combination of policy, process and technology is required. From a technology perspective, you may already be aware of the existence of security software, backup and recovery solutions, and archiving systems, and these all have a role to play. Modern solutions in these areas, though, are extremely comprehensive and flexible, so working through the various options and implementing them in a way that suits your business is important.

Furthermore, a range of other technologies and techniques that you may not have heard of are also available to provide data protection on a more continuous basis. Included here we have everything from simple mirroring of the disks used to hold business data, through to extremely clever solutions that can take a ‘snapshot’ of an entire system every few hours or even minutes. Gone are the days of having to rely on nightly backups, with the risk of losing up to a day’s worth of data following a failure.

It’s beyond the scope of this paper to go into detail on any of these technologies; we just wanted to convey the nature of data protection at a high level, and the fact that there is quite a lot to consider from a requirements and capabilities perspective. And that’s even before we take on board some of the trends and developments that are changing the goal posts in terms of requirements.

How well are you keeping up with the pace of growth and change?

If your organisation is anything like its peers, the chances are that trends and changes driving the rate at which business information is growing and diversifying are impacting the way you operate. Whether it’s mobile computing, home working, workforce collaboration, electronic commerce, social networking, automated B2B trading, or simply the way in which multi-media content is proliferating, the reality is that the volume and variety of data now being accumulated is putting stress on existing data storage and protection measures.

Even if you haven’t thought about this or realised it explicitly, you may have picked up clues from business users complaining of system downtime, lost data, difficulties finding information, and so on. If not, then all credit to your IT team for keeping on top of things. But regardless of how well they are coping, we would be extremely surprised if you haven’t heard an escalating level of requests from IT to approve spending on additional storage capacity and data management tools. All such complaints and requests are symptoms of reactive investment, in which money is spent and effort is expended, but no one ever gets things fully under control against the backdrop of rapid growth and change.

If you have read this far then we assume that you can relate to the kinds of challenges we have outlined. Our simple message to you is therefore that it’s time to consider information management and protection more explicitly. Unless you put it on the senior business agenda proactively, it will find its way there for all the wrong reasons – i.e. via the inevitable disasters and distress calls.

So what are the right reasons for senior management to pay attention to data protection?

Extend your thinking to consider cost, as well as risk

Data protection is often viewed in a similar way to insurance. The mind-set is that you need adequate protection, but at the end of the day the money you spend doesn’t actually generate a return – it’s simply part of the cost of doing business. This is understandable as both insurance and data protection are obviously about dealing with risk, but the view is flawed because the rationale and objectives behind each are quite different.

Insurance, for example, doesn’t prevent problems occurring, it just compensates you for your losses when something bad happens. Data protection, on the other hand, is there to actually prevent losses in the first place. Furthermore, while insurance is typically about dealing with unusual situations that you hope will never come to pass, data protection is concerned with minimising the damage and disruption caused by frequently occurring incidents that inevitably arise during the course of operating a business. This includes everything from users accidentally deleting or overwriting important files, through loss of mobile devices or the failure of PC hard drives, to more serious failures that could, and often do, bring down key computer systems for a period of time.

In many ways, when thinking of the rationale for data protection, it therefore makes sense to focus at least as much on cost as risk. From a business user perspective, for example, the kind of problems we have mentioned have a direct impact on productivity, as all of the interruptions can add up to a considerable amount of wasted time. There is then the distraction factor as users work around data-related challenges and attempt to resolve their own problems in their own way.

From an IT perspective, considerable cost and overhead frequently stems from time spent troubleshooting, recovering data, and otherwise helping users out of the jams they get themselves into through well-intentioned but ill-fated attempts at self-support. In addition to this, if the tools being used by the IT team for even basic operations like backup, recovery and archiving are out of date or otherwise inadequate, this translates to a further hit on costs. There is the time spent executing manual processes that really should be automated, and related to this, the effort required to resolve problems arising from human error. Again, if you add up the hours spent on activities that are not actually adding value to the business, the opportunity-cost is considerable.

Data protection as an enabler of business value

Mentioning opportunity-cost brings us to another perspective on data protection. Just think about how both users and IT people could better spend the wasted time we have highlighted on activities that actually create useful output. It's a short step from here to beginning to think of good data management and protection as an enabler of business value.

This view is strengthened when we consider some of the spin-off benefits. A pre-requisite for effective data protection, for example, is generating a good understanding of the business data you have and how it is stored. You might think there is someone in the IT department that already has a good handle on this, but you'd be surprised how sketchy the picture probably is in reality. This will be especially true if some departments manage their own IT systems, or your employees make significant use of laptops, smart mobile devices and internet (cloud) services that can all be used to store copies of data. It is not uncommon for business data to be spread across many locations in a fairly uncontrolled manner.

The output from data classification activity and the inventory of 'information assets' that stems from any proactive data protection initiative can also be used as a foundation to enhance user access. This can make it easier for employees to find the data they need, which can in turn lead to better decision-making and provide the intelligence needed to drive business innovation. We are starting to blur the lines here between data protection, more generic information management, and business analytics, but all of these are predicated on knowing your data and having it properly organised, which often starts with the basic need for protection and availability.

Netting it all out

Information is critical to the operation of the business, and better protection of it obviously helps to manage risks in a world in which the volume and diversity of data are growing relentlessly. Taking a more proactive approach to data management and protection, however, can also reduce operational costs and enable employees to contribute more in the way of business value and innovation. A relatively modest investment in data protection capability can therefore pay dividends in a short space of time, as well as removing a lot of distractions and headaches for those involved in running the business.

Given this, we would therefore encourage business managers and executives with any level of involvement in the way information is used in their organisation to take a serious interest in the areas we have been discussing. And as a call to action, we suggest working with your IT team to develop a more proactive and inclusive approach to data protection and management if you are not already doing so. Without this, cost escalation is inevitable, and nasty surprises are pretty much guaranteed.

Further reading

For additional insights into this important and fast moving area, and some ideas on how to move forward with a coherent plan of action, we suggest reading "Data Protection as a Business Enabler", a companion paper to this one which is available from www.freeformdynamics.com.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.

About CommVault

CommVault provides companies with a better way to protect, manage, and gain business value from their data. Today, with more than 17,000 customers and counting, CommVault is liberating companies worldwide from chaos, excessive costs and complexity.

CommVault is a publicly traded data and information management software company headquartered in Oceanport, New Jersey. It made its mark with the industry's leading backup product, Simpana software. Customers choose CommVault because of its Solving Forward® philosophy and ability to deliver complete solutions with infinite scalability and unprecedented control over data and costs.

Leading technology companies worldwide have formed strategic partnerships with CommVault, including Dell, Hitachi Data Systems, Microsoft, NetApp, VMware, Novell, HP, Oracle and Bull.

To learn more about CommVault, please visit our website at www.commvault.com.

Terms of Use

This report is provided for your general information and use only. Neither Freeform Dynamics Ltd nor any third parties provide any warranty or guarantee as to the suitability of the information provided within it for any particular purpose.