

# Data Loss: A Mounting, But Not Insurmountable, Problem

How to respond to the changing threat landscape



Over the past few years, data loss has rocketed to the top of IT chiefs' agenda. This hardly represents an unfamiliar new challenge for IT – rather it's a recognisable business concern that has been given added impetus. And the reason data loss has become such a hot button topic is because of the corrosive impact that data loss is having on firms. Previously, data loss incidents were frowned upon, then quickly forgotten.

Today, the threat of criminals stealing corporate secrets, or customers having their identities stolen means that the financial cost of data loss has risen sharply. And organisations' reputations – painstakingly crafted over the years – are trashed in an instant.

There is not an organisation today that doesn't need to be alive to the risks of data loss. High profile incidents, such as the release of millions of top-secret documents to whistle-blowing website WikiLeaks, have demonstrated that even government, military and diplomatic secrets can quickly be siphoned off.

So what are IT chiefs doing in response? There are some technologies – such as data loss prevention (DLP) tools, which promise to help keep the corporate crown jewels firmly locked away. Indeed a recent survey of IT decision makers in the UK showed that nearly half admitted that the WikiLeaks incidents have made them take a closer look at DLP.

But technology alone is not sufficient. For DLP to be effective, IT leaders need to understand the value of the data they hold, where that data is stored and who needs legitimate access to it. Without some sort of risk assessment, even the most powerful DLP technology cannot hope to provide a workable solution.

There is **not an organisation today** that doesn't need to be alive to the **risks of data loss**.

## The grave new world of data on the move

Protecting business-critical data is, unfortunately, harder today than it has ever been. Traditionally, IT departments could adopt a castle-defence strategy to secure the enterprise network: preventing any outsiders from gaining entry. A strong network perimeter was regarded as the best defence against hackers, viruses and data leakage.

But it is not a model suited to today's business environment. On any given work day, mobile workers, hot deskers, part timers, contractors and the like flit through company premises, or want to access the network from external locations. Lock the network down and you may as well shut up shop – nobody will be getting any work done.

Alongside increasing complexity of the user base, the variety of devices seeking access to the network has grown exponentially. That has been fuelled by the rapid adoption of consumer technology for business use. These days it's common for staff to bring their iPads and smartphones in to the office and expect to be able to connect to the network.

## Bring your own insecurity

According to independent research undertaken on behalf of Dimension Data, more than half (see fig. 1) of UK businesses sanction the use of employee-owned devices. That underlines the shift in thinking over access to the corporate network, but more worryingly, further analysis has shown that this relaxation of the access rules has been accompanied by a weakening of IT security.

Figure 1

### The use of employee-owned devices at work

**51% of organisations allow the use of employee-owned devices at work**

**49% don't**

Of those businesses that allow employees to use their own devices to access corporate systems, 39% do not use encryption to protect corporate data.

It's a similar tale when it comes to remote working. Around one in five firms let staff access the organisation's network without

insisting they have anti-virus software installed on their gadget; a third are similarly lenient when it comes to anti-spam software.

It should come as no surprise then, that when polled, the UK's IT leaders report that the biggest cause of data loss is via accidental data loss by employees. Today's must-have gadgets are the equivalent of fully-functioning computers, in terms of processing power and storage, says Chris Jenkins, line of business director – security at Dimension Data, the global ICT solutions and services provider. They are packed with features designed to give maximum mobile connectivity, he adds.

"If you allow these devices to connect to the corporate network, you have to accept that company data will be stored on them when the user leaves the premises. Unless you have plans to protect that data, you're risking accidental or even malicious losses,"

says Jenkins.

High-value smartphones, laptops and tablets are prime targets for thieves and can potentially be compromised by malware – so the acceptance of employee-owned devices on the network represents a clear risk. They potentially make it easier for attackers to snaffle logon credentials, account details or commercially sensitive information.

## The key challenge: balancing productivity vs. security

Too often, mobile devices are inadequately secured, says Jenkins. IT needs to strike a balance between the productivity benefits of allowing employee-owned devices onto its networks and the security risks, he says:

"If staff want to use their own devices, they should first agree to having battle-hardened data protection technology installed on those devices", he adds.

As a matter of course, businesses need to know that any sensitive data stored on an employee-owned device is encrypted and that the device can be remotely wiped, if necessary, says Jenkins.

"If staff aren't willing to agree to having the necessary security software on their devices, then their access to the corporate network should be restricted. It's about striking a balance,"

says Jenkins.

## Revealing the very real threat of damaging data loss

Of course, employee-owned devices are far from the only threat to the integrity of corporate security policies. High profile cases, such as the attacks on electronics giant Sony's online gaming networks and at email marketing firm Epsilon have hammered home the reality that even the largest tech-savvy firms are at risk.

Dimension Data's poll of 200 senior IT executives at large UK enterprises revealed that one in ten (see fig. 2) had been impacted by a data loss incident. Tellingly over half of those polled reported that they believed their business had suffered data loss – but they had yet to confirm it. The research also showed that internal fraud and hacking were the chief causes of data loss, after accidental loss (see fig. 3).

So what is the impact of such losses? According to those that have suffered data loss the damage varies (see fig. 4): 91% of victims report that their organisation's reputation has been tarnished; 27% report a loss of competitive edge; 18% lost suppliers or partners; 9% even lost customers; and finally 9% also report being handed fines by regulators.

In Sony's case, it offered insurance policies worth \$1m for its customers affected by the attack on its gaming network, to indemnify them in the event that the stolen information was used in identity fraud. Elsewhere, analysis by the Ponemon Institute suggests that the average data loss incident costs UK firms £1.9 million or the equivalent of £71 per record.

But the long term impact and damage to hard-won reputations can potentially be far more severe.

"When Sony's customer databases were breached, much of the focus surrounded the potential for credit card fraud," says Jenkins. "However, the more pernicious risk is that the hackers

Figure 2

Likelihood of experiencing a serious data leakage incident in the foreseeable future	
It's already happened	10%
It hasn't happened yet, but it's inevitable that it will	17%
Very likely	13%
Likely	24%
Unlikely	24%
Very unlikely	9%
Will never happen	1%
Don't know	2%

Figure 3

Causes of data leakage incidents	
Accidental data loss by employees	50%
Internal fraud or intentional data theft by employees	30%
External hacking	15%
Accidental data loss by suppliers/organisation partners	5%
Other, please specify	0%
Don't know	0%

Figure 4

Damage from data leakage incidents	
Reputation damage	91%
Loss of competitive edge	27%
Loss of suppliers/organisation partners	18%
Loss of customers	9%
Fines for non-compliance with regulations	9%
Loss of my job	0%
Other, please specify	0%
Don't know	0%

Today's enterprises will already be doing something – the big question for the IT chief is **whether their organisation is doing enough**, or indeed **doing the right things**.

## Too often, mobile devices are **inadequately secured.**

will have obtained personal information that makes many other forms of identity fraud possible.

“As the general public becomes more alive to that danger, the impact of data loss will inevitably become that much greater,” Jenkins adds.

Already, regulators appear to be taking tougher sanctions against those firms that protect sensitive data unsatisfactorily. There are, of course, many pieces of existing regulation that govern data security – Sarbanes-Oxley, Basel II, PCI DSS, MiFID and the Data Protection Act, as well as standards such as ISO/IEC 27000.

These play a vital role in setting the baseline for good practice, but they also give power to regulators to enforce good practice. Recent fines handed out by the UK Information Commissioner seem to indicate that a harder line is being taken. For example, two local councils, Ealing and Hounslow were fined a total of £150,000 having had laptops contained personal information stolen.

With regulators’ patience wearing thin and given the ever-changing threat landscape, the imperative for companies to take decisive action to protect their data has never been stronger.

### Responding to a changing threat landscape

For the most part, today’s enterprises will already be doing something – the big question for the IT chief is whether their organisation is doing enough, or indeed doing the right things.

The awareness and response to risks differs massively across different industries. But consistently, IT’s response to risks are driven by board-level questions about high profile incidents. As a result, they do not always focus on the risks that are most pertinent to the enterprise.

Understanding what data an organisation holds, where it holds it and what security is

in place around that is ultimately the key to assessing the risks it faces, says Jenkins.

Achieving that may entail some form of data classification project, to map out what data is where – and many IT leaders are wary of undertaking such seemingly Sisyphean tasks, says Jenkins.

“It can seem like a huge project, but the trick is to identify an approach that will fit your organisation,” he adds.

For many, the process of classifying the morass of data swirling around the enterprise has proven too daunting a task to contemplate. Research has shown that around a quarter of firms do not attempt to classify data at all. When asked why, nearly two-thirds fear that the results of such classification will require a level of investment that the management board is unlikely to sign off.

That can be an uncomfortable position for the IT chief: torn between the nagging notion that data is at risk and the need to keep a tight rein on spending. But a precisely constructed risk assessment can help IT leaders determine where that balance is best struck, says Jenkins.

By analysing their exposure to risk, considering threats to their data and the organisation’s appetite for risk, CIOs and CISOs can define an apposite security posture, he adds. For some that will dictate that every step is taken to minimise the chance of data loss; others may balance risk against cost.

The firm’s security posture will also dictate what level of data classification project is suitable. Some DLP tools use crawler programs to scour the networks, identifying files that match certain criteria. They can seek out specific data, perhaps credit card numbers or data whose format suggests a physical address.

Alternatively, firms can look to classify data at the server level.

“You may find a server where 99% of the data on it relates to internal business documents that are not commercially sensitive. But if the remaining 1% relates to trade secrets or may be governed by data regulations then automatically that asset becomes a high-value one,” says Jenkins.

IT chiefs may also go as far as considering how they treat virtual machines.

“How granular you get is entirely up to you,” adds Jenkins.

### Accept that data loss is inevitable, assign responsibility, and train staff

Whatever the decision on the organisation’s security posture, incident response planning will inevitably have to be part of the data protection planning, says Jenkins.

When it comes to reducing the organisation’s exposure to data risks IT chiefs would be better served by accepting that some form of data loss is inevitable, says Jenkins. Once you’ve made that mental leap, you’re much better placed to think about what your response should be, he adds.

A well-crafted incident response policy can be the difference between a high-profile event and an unfortunate but swiftly resolved one, says Jenkins. Such policies aim to outline the steps to be taken when a data loss incident comes to light. Critical components include classifying the incident – for example, firms may want to follow one procedure when an employee inadvertently downloads a virus, while a different one covers the loss of a mobile device.

The procedures should also identify who should manage the incident, how information pertaining to the incident is captured, how the escalation procedures should operate and even how and when to engage with law enforcement or the media, says Jenkins.

Without some sort  
of **risk assessment**,  
even the most  
powerful data  
loss prevention  
technology **cannot  
hope** to provide a  
**workable solution.**

According to Dimension Data's research, there is little clarity in most organisations over who should be responsible for incidents of data loss. Only a quarter of firms have a single person responsible for DLP, while 60% have multiple people (see fig. 5). Worryingly, nearly one in ten report that "no one in particular" has responsibility.

"There's an argument that data protection is everybody's responsibility," says Jenkins. "But if firms are serious about protecting their data, someone has to take charge."

You also need to train staff on the policies, so that in the event the policies need to be enacted, employees instinctively know what to do. This can be one of the hardest elements of all, admits Jenkins.

"Delivering effective security training is a hard nut to crack. Too often people believe that they inherently work in a security-conscious manner, so when it comes to training courses, they don't really engage," he says. "Sometimes you have to set out to shock them to get their attention."

### The true costs of DLP

Once firms are confident in their ability to deal with an incident of data loss – no matter how potentially serious – they are in a much better position to look at effective ways of minimising the likelihood their incident policy will be tested.

"By thinking through what you'd do in the event of losing data, you've already taken the first steps towards classifying the vast oceans of data within your organisation – and risk assessment is the foundation for a security posture that fits with the ethos of your organisation," says Jenkins.

Allied to making that decision is a good understanding of the true costs of implementing DLP technology. Alongside the upfront costs of purchasing DLP tools and the on-going maintenance charges, firms need to consider the cultural impact of implementing the tools – and this is something IT cannot do in isolation.

Figure 5

Who is responsible for data leakage protection in the business?	
A number of people	60%
A single person	27%
No one in particular	7%
No one at all	2%
Don't know	4%

DLP can affect how employees in non-IT business units work when it comes to sharing information, so it's beholden on IT to ensure that they have board-level support in deploying the technology.

It's a tough job, but someone's got to do it

Technologies other than DLP may also promise to cure the data loss headache for IT, but IT needs to take a dispassionate assessment of their promises, says Jenkins.

It may be tempting for some firms to believe that in future, new approaches to enterprise IT will offer a degree of shelter from cyber threats. If much of the enterprise estate moves into the cloud, does data security become someone else's problem?

"Hardly," says Jenkins. "From a customer's perspective, they won't differentiate between firms that use different models of IT delivery. They just expect their data to be safeguarded."

Impeccable data governance does not depend on models of computing delivery, argues Jenkins. Instead it is predicated on understanding what data resides within the enterprise – or on devices employees use – and what the risks are to that data. Only then can IT leaders decide on appropriate levels of protection.

And while it may seem that the data loss epidemic means all firms will be equally impacted, the sobering reality is that data security will become a source of competitive advantage – or perhaps more accurately a competitive disadvantage for those that fail to get it right.

Understanding **what data** an organisation holds, **where it holds it** and **what security is in place around** that is ultimately the key to assessing the risks it faces.

Whatever the decision on the organisation's **security posture**, incident response planning will inevitably have to be part of the **data protection planning**.

**MIDDLE EAST & AFRICA**

ALGERIA • ANGOLA  
BOTSWANA • CONGO  
DEMOCRATIC REPUBLIC OF THE CONGO  
GABON • GHANA • KENYA  
MADAGASCAR • MALAWI  
MAURITIUS • MOROCCO • NAMIBIA  
NIGERIA • SAUDI ARABIA  
SOUTH AFRICA • TANZANIA • UGANDA  
UNITED ARAB EMIRATES • ZAMBIA

**ASIA**

CHINA • HONG KONG  
INDIA • INDONESIA • JAPAN  
KOREA • MALAYSIA  
NEW ZEALAND • PHILIPPINES  
SINGAPORE • TAIWAN  
THAILAND • VIETNAM

**AUSTRALIA**

AUSTRALIAN CAPITAL TERRITORY  
NEW SOUTH WALES • QUEENSLAND  
SOUTH AUSTRALIA • VICTORIA  
WESTERN AUSTRALIA

**EUROPE**

BELGIUM • CZECH REPUBLIC  
FRANCE • GERMANY  
ITALY • LUXEMBOURG  
NETHERLANDS • SPAIN  
SWITZERLAND • UNITED KINGDOM

**AMERICAS**

BRAZIL • CANADA • CHILE  
MEXICO • UNITED STATES