KrollOntrack™
By KrolLDiscovery

Mitigating the risks of migration

Introduction

Upgrades and data migration are a routine element of the day-to-day IT workload, whether organisations are upgrading software or introducing new hardware, including mobiles, laptops, PCs or servers. However, as the company that is called in to help when data goes missing and has to be recovered, we see hundreds of cases when backups fail during the migration process. To understand when and why this happens, we carried out research[1] across the world to identify the biggest risks associated with data migration.

The alarming fact that emerged from our research is that organisations most often experience data loss because their backups fail for whatever reason—and even though these processes are carefully planned for beforehand, data loss can still occur. Upgrades and migration processes are equally risky whether they are being undertaken for mobiles, laptops, PCs or servers and whether they involve changes to the hardware or the operating system.

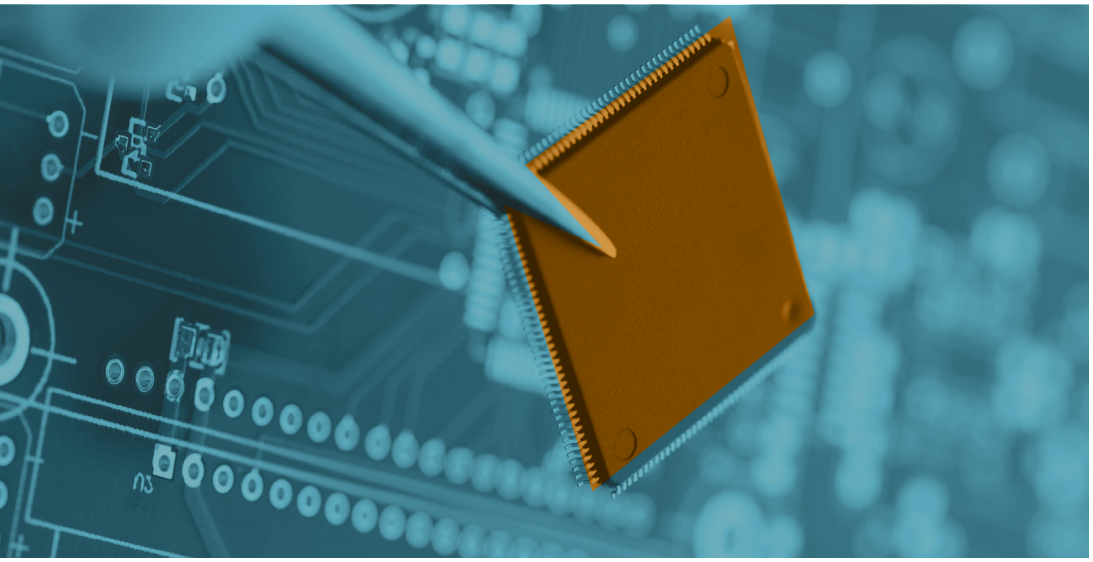
The problem is widespread: almost a third of respondents (32%) said that they had experienced data loss when migrating to new software from a server, while almost half (49%) lost data when upgrading software from a desktop or laptop.

As well as being endemic, the problem is ever-present. The results of this year's survey are consistent with research undertaken in the previous three years by Kroll Ontrack, where over half of consumers/businesses reported data loss even when backups were made.

What can organisations learn from these insights?

The biggest lesson to learn is that some data loss is unavoidable, so it's vital to ensure that a rigorous backup strategy including regular testing of backup and restore functions is in place. While organisations should check their capability to restore frequently, it's especially important to do so before a migration. The need to upgrade systems is not going to go away: indeed the increasingly fast pace of change in IT means that upgrades will need to be made even more regularly.

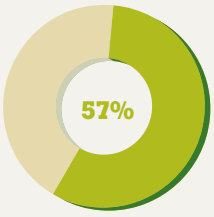
1—Kroll Ontrack surveyed 572 Ontrack Data Recovery customers in February 2016. Respondents were based across North America, Europe and Asia Pacific.



The data recovery gap

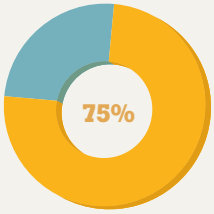
The global survey of nearly 600 IT administrators revealed that while over half (57%) of respondents had a backup solution in place when data was lost during migration processes, three quarters (75%) were not able to restore all of their lost data, with more than one-in-five (23%) unable to recover any data at all.

Did you have a backup in place at the time of the data loss?

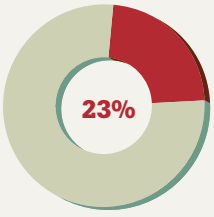


had a backup

Were you able to recover the data lost during the migration?

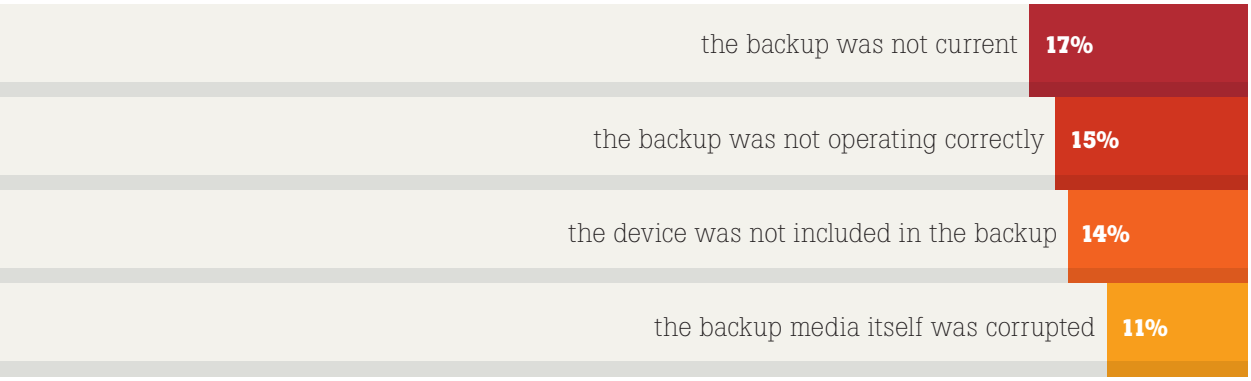


were not able to restore all of their lost data



unable to recover any data at all

Specific to data loss experienced while migrating or upgrading operating systems, respondents cited that the backup was not current (17%) or it was not operating correctly at the time of data loss (15%), the device was not included in the backup (14%), or that the backup media itself was corrupted (11%).



Why do organisations continue to fail to backup effectively? In a separate study undertaken by Kroll Ontrack with 528 respondents across North America, Europe and Asia, over half (54%) of people who did not have a backup solution in place cite time to research and administer as their primary reason for not seeking a backup solution (up 4% from 2015).

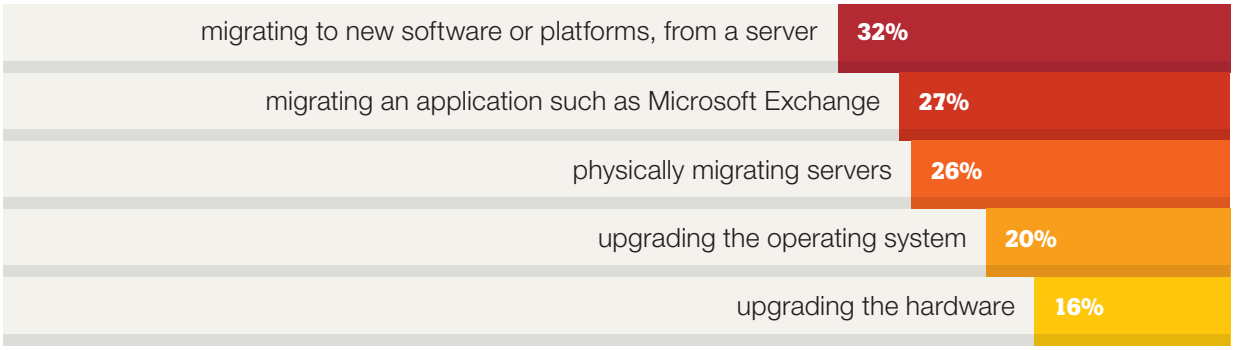
However, seven per cent fewer people in 2016 (24%) report the expense of a backup solution as their primary reason for not leveraging a backup. Other findings include a six per cent increase in the number of survey participants who report daily backups this year (48%).

Such findings are encouraging, but the incidence of data loss continues to alarm. While almost half (47%) of organisations that had lost data during a migration had only experienced this once, a further 45% had lost data during a migration between two and four times. The remaining 8% reported losing data during migration more than five times, representing a real risk to the business in terms of lost revenues or reputational damage.

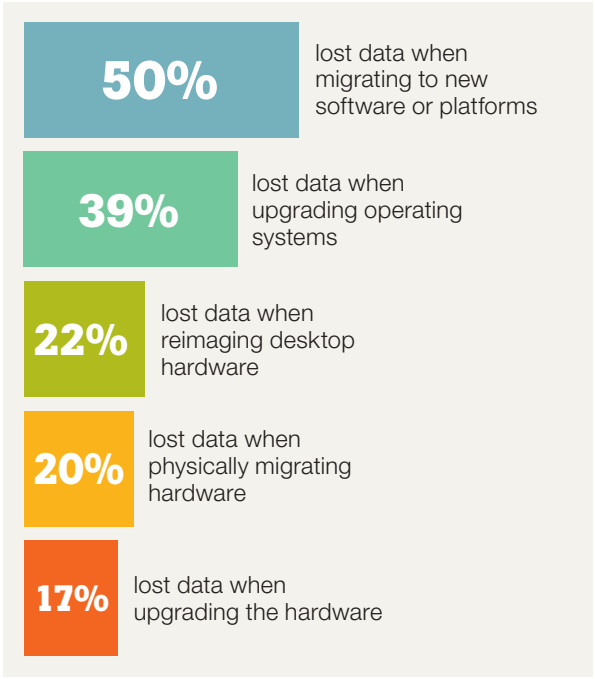
Organisations that reported losing data when migrating to new software or platforms were most likely to attempt to recover it by using a third party software tools (52%), their native system recovery program (24%) or a data recovery provider (24%).

Operating systems or hardware: what's riskiest?

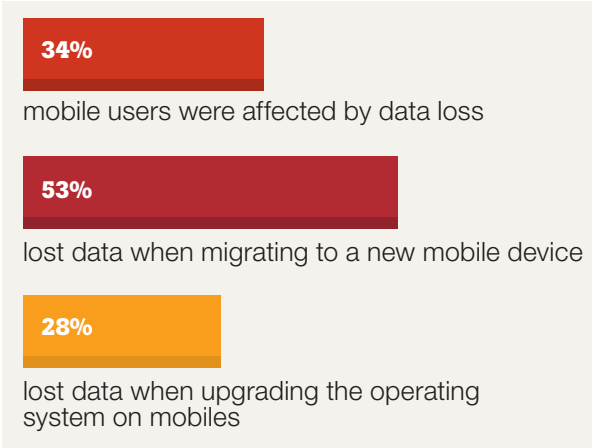
When asked whether they had experienced data loss when migrating to new software or platforms from a server, almost a third (32%) said that they had. The riskiest points of server migration were when migrating an application such as Microsoft Exchange (27%), when physically migrating servers (26%), when upgrading the operating system (20%) or when upgrading the hardware (16%).



The problem of data loss occurs as regularly on standalone devices as on servers, highlighting the fact that this is a challenge for individual users as well as businesses. In fact half (50%) of respondents said they had lost data when migrating to new software or platforms from a desktop or laptop. The riskiest upgrades in these cases were upgrading operating systems (39%), reimaging desktop hardware (22%), physically migrating hardware (20%), or upgrading the hardware (17%).



Data loss appears to be less of a problem for mobile users, but still affected more than a third (34%) of respondents. Despite the automated update processes available when upgrading mobiles, 53% of respondents said that they lost data when migrating users to a new mobile device. A further 28% said they had lost data when upgrading the operating system on mobiles.



Organisations should also be aware that data can be lost when organisations migrate to new software or platforms from back-up or archive applications: over a quarter (26%) reported that this had happened to them. This is most likely to occur when organisations are upgrading older software or infrastructure that encrypted data (38%), upgrading to a new release of the same software (29%) or migrating to a new back-up or archive (27%).

A global view of the risks that lie ahead

Interestingly, in looking ahead to what respondents believe will be the major causes of corporate data loss in the next 12 months, global respondents rank migration and upgrading systems low on the scale of concern, even though our research reveals one-third of respondents had lost data during such exercises. Instead, respondents believe that hardware failure (22%), user error (22%) and unforeseen and unexpected errors (21%) as the top-ranking risks to corporate data loss. Only 11% believe that poor internal controls and data governance will be a top three risk, despite the fact that so many backup systems fail and mean that data cannot be restored.

In the next 12 months, what do you believe is the top risk to corporate data loss?	
Hardware failure	**22%**
User error e.g. deleting data by accident	**22%**
Unforeseen and unexpected errors	**21%**
Poor internal controls and data governance	**11%**
The move to cloud-based storage	**7%**
Upgrades to critical customer-facing applications	**5%**
The move to mobile devices for employees	**5%**
The move to virtual drives	**4%**
The move to Microsoft Office 365	**3%**

How to safeguard your data during migration

It's clear that data loss is a problem that will not disappear, whether it happens during the migration process or for other reasons including hardware failure and user error. Kroll Ontrack advises that individuals and businesses regularly monitor and certify their chosen method of backup to ensure it is successfully operating and capturing all relevant data, in addition to the following tips:

- Take the time to invest in a backup solution and set a backup schedule
- Ensure all identified devices and media are included
- Ensure that backups are running regularly in accordance with the determined schedule
- Check backup reports for errors or failure
- Test backups and the restore process on a regular basis to validate that data has been accurately captured and files are intact

Kroll Ontrack further recommends that organisations include details of a third party data recovery partner in disaster recovery plans so that they can be consulted as quickly as possible in the event of serious data loss.

Further tips for de-risking the migration process

Before starting the migration process it is essential to run a backup of all computers and perform a restore test. The backup should not only include data files but also the entire system through a complete image. There are other safeguards organisations can put in place to de-risk the migration process. Depending on the size and scope of the migration, it makes sense to implement some or all of the below measures.

Test environment

A test environment is a simulation of the live production environment but without the risks. If something goes wrong, the damage will not affect data. It's a good idea to build an environment and test the migration process, install the drivers and software applications to make sure that everything is working properly. Updates and patches should first be deployed in a test environment and then applied to the production environment. Though we can't foresee all eventualities, this extra step can help minimise the risk of a loss and provide an opportunity to prepare corrective measures should any failures or loss occur.

Don't be the first to migrate

It may not be a good idea to deploy a new OS immediately but instead to wait for some months. A new version usually brings with it missing or not yet optimised drivers and also some new bugs. It's advisable to wait for some time and in order to access compatible and stable drivers, install patches for bugs discovered after the launch and upgrade to applications software in a fully compatible state. It will also be possible to find new forums dedicated to the new OS or platform and therefore easier to seek and obtain support from the online community.

Use appropriate tools for the deployment

The risk of data loss or that something is not working properly in a migration process can be further mitigated by using ad-hoc deployment tools. IT administrators can use tools that can backup data and settings, but also to manage the entire migration process in a centralised console.

Conclusion

Software and hardware upgrades are a necessary part of scheduled IT maintenance. Whether it's migrating to a new version of Microsoft Windows, adopting Windows 365, replacing desktops with tablets or updating backup and recovery platforms, constant change is the norm for all organisations as well as individuals and micro businesses.

Given this fact, together with the findings from our study that show the high and regular incidence of data loss during migration, it is clear that something has to change. The place to start is with backup planning, scheduling and quality checking so that if the worst happens during a migration process, organisations have done as much as they possibly can to prepare for this and mitigate against irrevocable data loss.

About Kroll Ontrack

Kroll Ontrack provides technology-driven services and software to help legal, corporate and government entities as well as consumers manage, recover, search, analyse, and produce data efficiently and cost-effectively. In addition to its award-winning suite of software, Kroll Ontrack provides data recovery, data destruction, electronic discovery and document review services. For more information about Kroll Ontrack and its offerings please visit: www.krollontrack.it or subscribe to the Kroll Ontrack Data Blog.

CONTATTI

Kroll Ontrack Srl | Via Marsala 34/A | 21013 Gallarate (VA)
Tel. **+39 0331 1835 811** | Numero Verde **800 44 00 33**
info@krollontrack.it

www.krollontrack.it