3 Critical Steps to IT Data Management Success

It's been just over a year since the General Data Protection Regulations (GDPR) were introduced, yet companies are still putting themselves at risk by not managing their data.

If there is one dominant theme which defines corporate life during the early years of this century it is data. Not so long ago, data was something which was gathered for governmental, scientific or medical research, and not by companies whether large or small.

Yet the digitisation of our lives has radically altered this. Data is being gathered and stored in ways and amounts which were unthinkable thirty years' ago: from smartphones to photocopiers, PCs to laptops, cloud-based systems to on-premise servers, and not to mention the many ways in which data can be shared.

While all this data helps to run our companies with great productivity, it also comes with great responsibility. Failure to understand your duty concerning the storing, and ultimately the destruction of data has become a serious offence.

First American Financial Corp, one of the largest title insurers in the US, was sued by a client who claims that the company's lax security measures put him at risk of identity theft, along with millions of others whose personal information could be accessed through its website.

Treating this data with its due respect prompted authorities in Europe to usher in GDPR and during its first year, 206,326 cases were reported across the 31 countries in the European Economic Area. Furthermore, a total of €56m in fines have been levied at those found in breach .

As for the worse offenders, the Netherlands with 15,400 data breaches tops the list, Germany is in second with 12,600, while the UK is in third place with 10,000 breaches .

Managing data has always been a part of the IT lifecycle. However, with the advent of GDPR, data breaches mean, not only a possible loss of corporate reputation and financial loss, but hefty fines too. Therefore, it's essential to have robust processes in place to manage your data and mitigate against the associated risks.

THE MAIN CONSIDERATIONS:

This whitepaper explores these themes, they are:

1. THE THREE TYPES OF DATA BREACHES
2. DATA AUDIT
3. DATA DESTRUCTION

1. Three Types of Data Breaches

GDPR defines three types of data breaches – it's vital to be aware of them.

When data breaches are reported in the media, they are usually the preserve of large corporations who have leaked millions of personal records and are now facing serious legal action. While such stories grab the headlines, data breaches can – and do – affect companies of any size that hold other people's data.

To ensure that you are not subject to a data breach, it's important to understand what one actually is. In general, GDPR is concerned with data breaches governing personal data which reveals 'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored, or otherwise processed. '

In other words, any information which is clearly about a person and may include their ID number, online identifier, location data, or specific information relating to the physical, physiological, genetic, mental, economic, cultural or social identity, of that person.

According to GDPR, there are three types of data breaches:

– CONFIDENTIALITY BREACH
A breach of confidentiality is when data or private information is disclosed to a third party without the data owner's consent. Whether an intentional breach, accidental error or theft, the data owner is entitled to take legal action for potential losses or damage that comes as a result of the breach of confidentiality .

– INTEGRITY BREACH
This is when there is an unauthorised or accidental alteration of personal data. For example, hackers could target a company database in order to erase files or disrupt processes.

– AVAILABILITY BREACH
This occurs when there is an accidental or unauthorised loss of access to, or destruction of, personal data.

While these three categories are enshrined in GDPR legislation, they are often known as the CIA triad, and are the building blocks of information security . Understanding such threats is the first step in their prevention.

2. Audit Trail

Knowing the location of your data is the key to keeping it safe.

While we are all benefiting from the many devices which we use for work, the proliferation of such devices – and the mobile way we work today – means that data may be more easily compromised.

While PCs, CDs, USB sticks, tablets and company smartphones are an obvious location, data also sits on desktop phones, scanners, and printers.

If your company allows employees to receive company email on their personal devices such as their smartphones, you are responsible for this data too. Therefore, a full inventory of where data sits in your organisation is vital.

A proper IT audit has many benefits, including::

– PREVENTING THEFT
Regular auditing will deter and reduce theft of IT assets and the possible selling of such items with confidential data on them.

– IDENTIFYING OLDER ASSETS
Older assets are more vulnerable to cyber attack. Identifying and disposing of such assets will reduce the risk that they pose.

– COMPLIANCE
There is a legal obligation on certain financial institutions to detail where client data is being held and who has access to it .

– LEGACY SYSTEMS
Identifying legacy processes and/or systems in need of upgrading/replacement which are a data risk.

– LEASED EQUIPMENT
Leased equipment must be properly identified and sanitised before it is returned.

– INSURANCE COSTS
IT assets must be accurately insured in case of a data breach.

– WARRANTY
Checking what assets are under warranty will reduce maintenance and compliance costs.

Only a full, physical audit on all your IT assets will ensure full GDPR compliance.

3. Data Destruction

The destruction of data is part of its lifecycle and a key part of data protection.

When you have identified IT assets – and the data which they hold – in need of destruction, it's important to dispose of such data in a compliant manner.

In an infamous case, Canadian computer and electronics retailer Netlink Computer Inc. simply abandoned some of their equipment which included 20 Dell PowerEdge and Supermicro servers, 300 desktop PCs, 109 hard drives, and another 400–500 drives.

The equipment turned up for sale on Craigslist, and then it was discovered that it contained 13 terabytes of data, including 385,000 database records containing names, email addresses, phone numbers and account passwords, 258,000 of which included full credit card payment details.

According to a report by Stellar who conducted the world's largest study of old devices, 71% of the 311 devices analysed contained personally identifiable information, personal data and business information; while 222 of the devices studied were disposed of in secondary markets without using proper data erasure tools.

When it comes to data destruction, there are three important steps:

1. DATA DESTRUCTION STRATEGY

Once an IT Asset Disposition (ITAD) program has been established and lists the data and/or assets to be destroyed, you should decide on strategy, namely: data destruction or asset recycling.

- Data destruction
  - This involves data erasure and degaussing services; and
  - The destruction of data carrying devices
- Asset Recycling
  - The repurposing of used IT parts
  - Donation of IT assets to charity

2. DATA DESTRUCTION LOCATION

Typically, data can be destroyed in two places, either on or off-site.

- On-site
  - On-site data destruction is preferable for companies with compliance concerns
- Off-site
  - Secure shipment for small media quantities / boxed materials for off-site destruction

3. FULL ACCOUNTABILITY

When your data has been destroyed, it must be ensured that all data has been removed from the devices. Such accountability should include:

- Certificate of erasure of data for each hard drive
- Evidential video file of device destruction for each hard drive
- Date and time-stamped of the destruction process
- Full chain of custody tracking and reporting of all redundant/obsolete assets

4. Conclusion

GDPR and data management is a process which will be with us for the foreseeable future.

According to Gartner Research , the average lifespan of a desktop PC is 43 months, and 36 months for mobile PCs. The consequence of this is that every three to five years, you will, not only be replacing such computers, but have to manage the data and assets too.

With this in mind, it's vital to develop an ongoing strategy when disposing of your IT assets. This will ensure that your old assets are disposed of in line with data regulations and help to prevent against certain types of data breaches.

A certified and professional ITAD strategy incorporated into your IT Asset Management process will typically achieve a 30% cost savings in the first year, and at least 5% cost savings in each of the following five years .

Lastly, you must ensure that your strategy keeps apace with technology. GDPR is not like the Millennium bug, it cannot be 'solved' by adapting certain processes and then forgotten about. Instead it's an ongoing approach to data which, as more and more data is produced everyday, will become embedded in all your IT processes.

References

https://www.datacenterknowledge.com/security/first-american-financial-sued-over-alleged-data-breach

http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

https://tech.newstatesman.com/gdpr/data-breaches-gdpr

http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm

https://www.hiscox.co.uk/business-insurance/professional-indemnity-insurance/faq/what-is-breach-of-confidentiality

https://www.testingexcellence.com/confidentiality-integrity-availability/

https://www.fenergo.com/assets/files/industry-knowledge/whitepapers/GDPR-Key-Challenges.pdf

https://nakedsecurity.sophos.com/2018/09/24/bankrupt-ncix-customer-data-resold-on-craigslist/

https://www.stellarinfo.com/ResidualDataStudy.php

https://www.vbsitservices.com/2016/02/how-often-should-your-company-replace-computers/

https://www.gartner.com/imagesrv/media-products/pdf/provance/provance_issue1.pdf