Ontrack®

Protecting data through its lifecycle

Data is crucial to an organisation’s success. But the more information an organisation manages, the more risk it carries. An organisation may hoard corporate data assuming that it’s better to keep it for litigation purposes or that it’s cheaper and easier to store it than destroy it. More than often, this is not the case. Most corporate data outlives its use quickly. Only a few industries need to retain data indefinitely. Once data is no longer deemed valuable, it becomes a liability, one that could expose an organisation to extreme risks.

Data today

The Radicati Group estimates that in 2021, we will be sending 320 billion emails a day. An incomprehensible amount of data. We are producing more big data than ever before and at an increasingly fast volume. Organisations should, therefore, be more aware than ever of the risks of managing data.

Digital transformation is taking hold. According to New Vantage's 2019 Big Data and AI Executive Survey, 91.6% of organisations are investing in big data and AI. Businesses today not only have tape backups and hard drives to contend with, but they also have mobile devices, memory cards and now, more than ever, virtual environments. No matter what data a company produces, managing data through its entire lifecycle is vital to ensure an organisations security and compliance.

Below are a few recent examples of organisations failing to manage their data effectively:

In 2019, a significant privacy breach occurred in Japan where 18 hard drives used by the Kanagawa Prefectural Government to store taxpayers' data were auctioned online instead of being destroyed. Sold online by an employee of a Tokyo-based recycling company, the hard drives were meant to be securely destroyed. The data on the sold devices totalled 27 terabytes and included individuals' names, addresses, and tax payment records.

Credit card company, Capital One was also hit in 2019. In this case, a hacker exposed more than 106 million credit card applications and customer accounts. The perpetrator was quickly arrested, but not before the damage was done with investigations revealing that some of the records dated back as long as 14 years.

The results were staggering finding sensitive residual data on **42%** of the drives

A study commissioned by Ontrack in partnership with data erasure specialist, Blancco analysed 159 second-hand drives bought from eBay. The results were staggering finding sensitive residual data on 42% of the drives, with 15% containing personally identifiable information including passport information, birth certificates, university papers, financial records, and photos.

The dangers of data

There are three main types of data that an organisation may store:

Customer data – This will include personally identifiable information (PII) that could help to identify a specific person, e.g. name, address, bank details, health records.

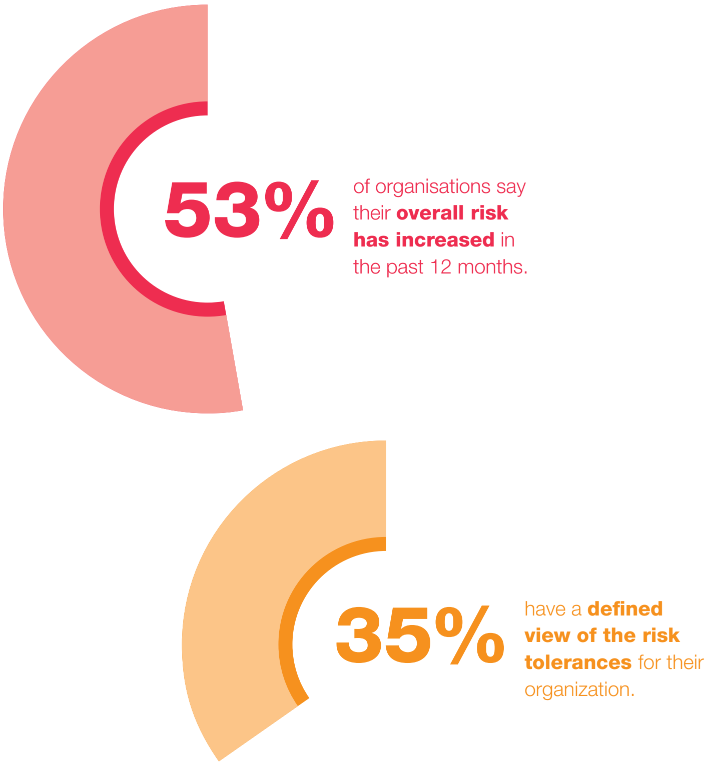
Employee data – This includes personally identifiable information regarding employees but also includes information regarding salary, performance reviews and any disciplinary records.

Corporate data – This may include sensitive information such as research and development data, merger and acquisition communications, customer lists, financial records, supply chain deals and trade secrets.

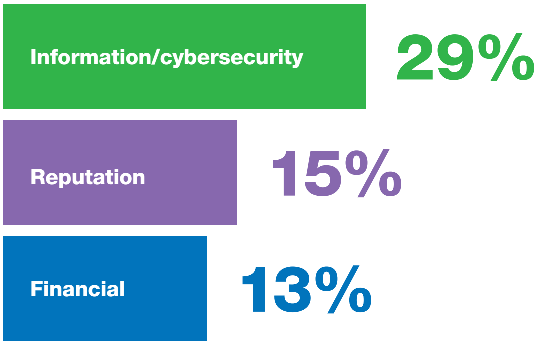
As already mentioned, the more data an organisation manages, the more risk it carries. The last few years have seen a substantial increase in cyber attacks, with the main purpose to steal corporate data and set a ransom for its "safe" return. In fact, the latest report by McAfee states that in the first quarter of 2019, ransomware attacks grew by 118%. And not only was there a significant rise in the number of attacks, but there were also several new ransomware families appearing – showing that cybercriminals are using more innovative techniques to cause chaos.

Organisations should consider not only the risks of data exposure but also the cost of protecting the data in the first place. The more data you have on servers, backups tapes, and mobile devices, the more investment you need to make to ensure it's secure. Cybersecurity needs to be a top priority for businesses of any size to protect itself again the ever-evolving threat network. According to ISACA, CMMI and Infosecurity Group's "State of Enterprise Risk Management 2020" study, 53% of respondents stated that they had seen increased risk to their organisation over the last 12 months. Additionally, 29% of respondents found that cybersecurity is the most critical risk category facing enterprises today and 33% believe that information/cybersecurity risk will be the most crucial category of risk facing their organisation in the next 18-24 months.

INCREASING RISK



TOP 3 most critial risk categories facing organisations today:



Source - ISACA, CMMI and Infosecurity Group's "State of Enterprise Risk Management 2020

It’s not just data security that costs

An organisation should not only be wary of the cost of cybersecurity and the potential risk of data breaches. There are also less measurable elements an organisation should consider. These include:

- The cost of procuring and maintaining data storage and backup equipment
- The cost of preserving personnel processes and software to manage short-term data storage, near-term onsite backup and long-term offsite data archiving
- The time and resources of workers who have to sift through unnecessary data to find relevant information – reduction in productivity of a workforce can cost organisations hundreds of thousands of pounds each year.

Lifecycle data management – from cradle to grave

To effectively mitigate the risk of data exposure and avoid the costs of storing and handling unnecessary information, an organisation should implement an end-to-end process for managing its information from creation to disposal. Data lifecycle management comprises of a strategy, process, and technology to effectively manage information, improving the control over an organisation’s critical data.

A lifecycle management programme can bring significant benefits to an organisation through the simplification and consolidation of IT resources and systems.

Specific benefits include:

- **Reduced risk:** Reducing the storage of unnecessary or expired information and making your data easier to manage. Reducing the volume of unneeded information will lessen the risk of a data breach. Knowing where specific data is stored will reduce the chance of missing critical information when searching.
- **Cost savings:** Storing data costs money. The more data you have, the more it costs to store. Legal and eDiscovery costs can also be reduced with better management of information.
- **Improved service:** Data management can become less of a drain on IT and legal resources, allowing them to focus more on business-critical/customer-focused tasks.

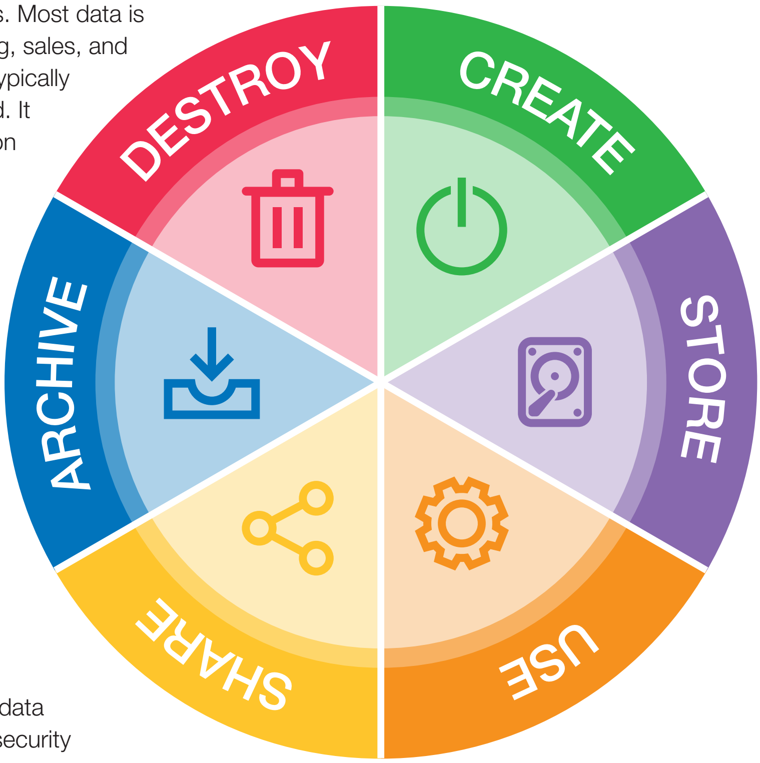
	Hard £	Soft £	
Reduce Cost	Application Decommissioning	eDiscovery	**Enhance Productivity**
	Data Storage	Findability	
	eDiscovery	Reuse / Repurposing	
		Personal Records Administration	

Additional Soft £ Benefits

	Benefits Drivers	
Mitigate Risk	Control	
	Quality	
Enhance Productivity	Collaboration	
	Process Efficiency	
Drive Opportunity	Decision Making	
	Information Delivery	

Source: Deloitte

The data lifecycle includes six phases:



Create – Data creation occurs throughout organisations. Most data is created by business functions such as finance, marketing, sales, and human resources rather than the IT department whose typically responsible for managing the data once it's been created. It can take place on-premise either in your data centre or on employees' devices or externally in the cloud. Protecting your data during this phase will include access controls such as passwords, threat scanning for antivirus, and data classification that will specify the data type, its location, how it should be protected, and who has access to it.

Store – Once data has been created, it is typically stored on a computer hard drive or in a data centre. Certain types of transaction or analytics data might be generated in transit or in memory but not permanently stored to disk. Storage also involves near-term backups that must also remain protected. Once data is stored, responsibility for its management typically falls to the IT or security team.

Storage protections include access control around who can read and overwrite the data, device control such as data encryption, backups to protect the data from loss, plus security measures to protect the backups themselves.

Use – During the 'use' phase, data is accessed, viewed or processed. Protecting data during this phase will usually fall equally between the lines of business and the IT department.

Protections during data usage include access control, encryption, data rights management for copyrighted information and data loss prevention, which involves software and business rules to prevent unauthorised access to sensitive information.

Share – Data is often shared amongst internal employees and to corporate partners outside of the organisation. Data sharing can occur through the network, via removable media, or across the internet via transfer sites or email. When data is shared, it is subject to new risks.

Data sharing safeguards involve access control, encryption, network security (firewalls/intrusion detection) and data loss prevention. When organisations are dealing with third-party vendors, they should have clear measures in place for data removal and verification after services have ceased.

Archive – For short-term data protection, all data must be backed up regularly, either onsite or offsite. When an organisation needs to retain data for the long term, it can be archived to tape or disk media and placed in remote, secure locations.

An organisation's operations team would usually take responsibility for archiving as opposed to IT or the lines of business. Protecting archived data include access control and encryption.

Destroy – When an organisation's data reaches the end of its life, it must be permanently erased. Determining which data is erased, how it's erased and how that erasure is verified depends on several factors, such as content type, usage needs and regulatory requirements.

When it's considered at all, the "Destroy" phase is most often addressed by the operations team. But when managed properly, end-of-life data destruction is truly the responsibility of all stakeholders, from IT to the lines of business.

Lifecycle management in your organisation

The management of data across its lifecycle is not a consideration for many organisations. But without a data lifecycle strategy in place, an organisation is leaving itself exposed to serious security risks and costs.

Lifecycle management shouldn't be the responsibility of just one department; there needs to be a collaborative approach that involves all the stakeholders of the business.

Organisation's that rely heavily on data for their success should consider establishing a Chief Data Officer (CDO) whose main role is to ensure the prioritisation of data protection. Once a CDO is in place, you then need an information governance team that involves the lines of business, legal, IT and operations team.

Each department has its own role to play in the data lifecycle. The lines of business heavily depend on data, but they should not just assume that someone else is managing it. They should work closely with legal and IT to ensure they're in compliance with regulations and that they have the right policies, tools and processes in place to protect critical information. IT departments must work with the lines of business to ensure they fully understand the requirements and challenges of protecting data at every stage. And legal must ensure that every employee understands the potential risks that not complying can have on the organisation.

In the end, the policies and procedures that govern the management of the data lifecycle may reside in the IT department, but an organisation must remember that all stakeholders must be actively involved to ensure that all data is protected from the moment it is created until its end-of-life.

Today, the cost of ineffectively safeguarding data comes with 'too high a price.' Data breaches, damaged reputation, lost customers, downtime, and large fines are all potential risks for an organisation that doesn't effectively manage its data's lifecycle. Those organisations that take the time to invest the necessary efforts and resources in data lifecycle management can minimise the risks and costs of their business-critical data at all stages.

Ontrack®

Global House, 1 Ashley Avenue
Epsom | Surrey KT18 5AD

24/7 +44 (0)1372 741 999
www.ontrack.com/uk