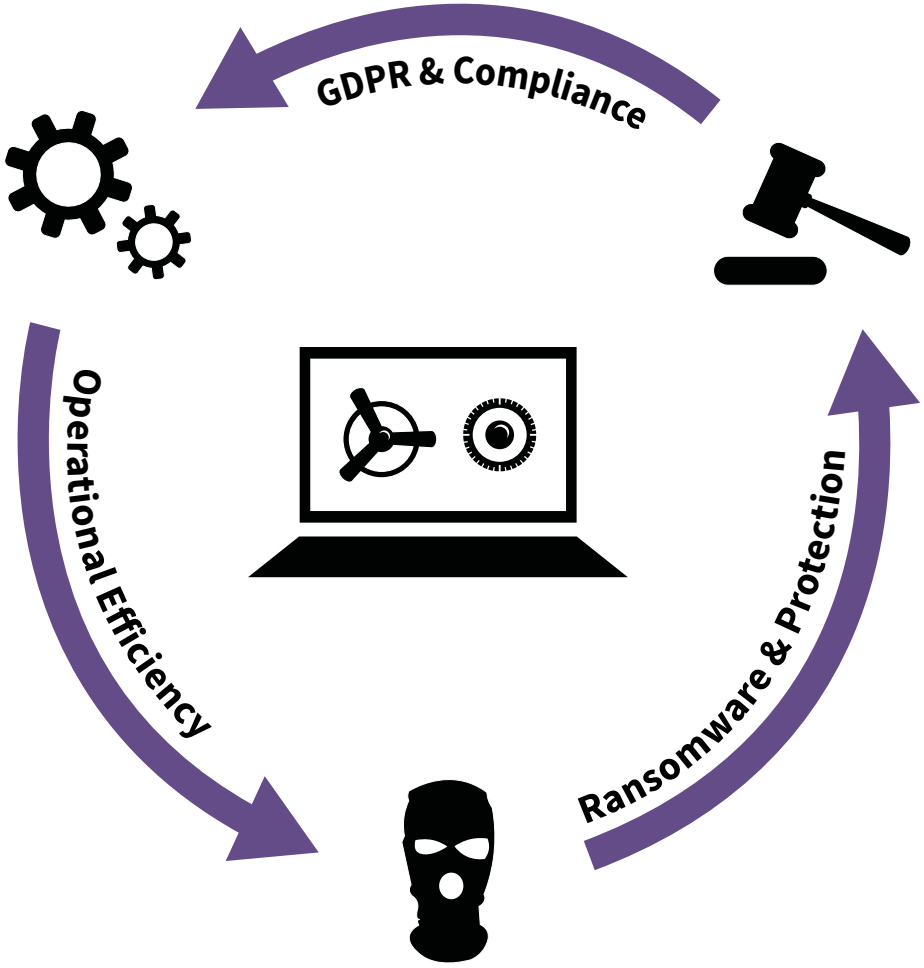
FREEFORM DYNAMICS

IN ASSOCIATION WITH

FUJITSU



DATA PROTECTION REVISITED

A RISK REVIEW AND INVESTMENT GUIDE FOR IT PROFESSIONALS

FREEFORM DYNAMICS, JANUARY 2018

DATA PROTECTION IMPERATIVES AND OPPORTUNITIES

As business – and indeed the wider world – becomes digitally-driven, the pressure is on IT professionals to ensure that their organisation's electronic data is effectively managed and protected to minimise operational and business risk. A corollary to this, though, is that the growing dependence on data also brings the opportunity to do data management and protection better, especially as the threats of ransomware and the GDPR require budget holders to pay increasing attention to actively managing data. Let's look at the key requirements facing any data-using organisation.

Established requirements

Business operations perspective

Security and access

Ensure that sensitive data is only accessed by those who are authorised to do so.

Prevention of data loss

Take steps to avoid data being lost due to human error, technology failure, or malicious activity.

Business continuity

Make sure critical IT systems are resilient to data-related incidents and failures, i.e. keep running.

Disaster recovery

Minimise the time to recover and get systems working again if a major incident causes a major failure.

Established requirements

Legal & compliance perspective

Record integrity

Maintain accurate and complete records to meet statutory reporting requirements.

Data governance

Define/implement policies to deal with data collection, security, storage, access, use, retention and disposal.

Information discovery

Ensure all data relevant to a customer, incident, case, etc can be quickly located and retrieved.

Auditing and tracking

Track relevant activities in relation to key data, e.g. creation, access, change and deletion.

Emerging imperative

Ransomware protection

An infection with one of these data-encrypting viruses can be both hugely disruptive and tough to remediate. Modern examples are network-aware, so they can also damage servers, cloud storage and can even encrypt backup media. Ransomware defence must be layered, including user training, anti-virus software, network behaviour analysis and more, but if infection occurs then paying up is not the answer. The only reliable solution is an offline or otherwise air-gapped protected backup.

Emerging imperative

GDPR compliance

The EU's new rules for the protection and privacy of personal data, called GDPR, take effect in May 2018. In most organisations they should bring significant changes to how you manage data. In particular, they demand a higher degree of transparency and accountability from the business, and your data protection systems may well have to change significantly in order to support that. In many cases, this could and should become a catalyst for a wholesale rethink of the data protection strategy.

From risk management to incremental business value

What matters first and foremost in data protection is whether the data is there to support your business. You can take as many backups as you like, on any format or several formats, and none of it will matter if you cannot return damaged, lost or archived data within an appropriate timeframe.

Beyond that, though, are both business risks and business opportunities. Data protection systems can now become key to both mitigating risk and opening up new opportunities, because they are the hub where all the organisation's data can be found. That in turn offers an opportunity to place IT and data protection at the very centre of the business.

In particular, once we get beyond risks and requirements there are notable opportunities for IT to identify incremental uses for the data protection system. It might for instance be consolidating data for business analytics, generating synthetic backups from an archive, discovering and protecting dark data (data which would normally be invisible to the organisation even though it has significant business value, perhaps because it exists only on a user's device) or one of several other possibilities. These incremental uses are the 'value-add' that can make the data protection system ever more cost-effective and efficient.

MODERN DATA PROTECTION SOLUTIONS

Data protection is more than just backup, or even backup and archiving. It covers a broad range of information management and security needs, and modern solutions therefore integrate many capabilities that were not part of traditional backup solutions and in the past had to be implemented separately.

The ideal here is an integrated system that can cover the wide range of data protection risks and requirements. Acquiring and implementing this needs time and money, however, commodities that are typically in short supply. The short term pressures of ransomware and GDPR are changing this, freeing up budget in many organisations – the challenge is to prevent this from being wasted on yet another point solution that adds yet more long-term complexity and operational cost in return for what's merely a short-term fix.

Fortunately, there is a high degree of commonality between organisations and their needs and expectations, even if their actual implementation details may vary considerably. Not everything will be appropriate in every case, but when specifying or acquiring such a system, here are some requirements and major topics to consider – and of course to ask potential suppliers about.

Data protection requirements

Business operations

Security and access, prevention of data loss, business continuity, disaster recovery, ransomware protection

Legal and compliance

Record integrity, data governance, information discovery, auditing and tracking, GDPR compliance

Key questions and considerations

Data discovery
Can it find all your data? Where is it? How fast does it change? How is it protected?

Data classification
What is it? Is it sensitive? Does that vary with time? Is it adequately protected?

Recovery
Can it be tested, at multiple granularities (record, file, VM, etc)? Can it be self-service?

Auditing & Reporting
Can it track access to sensitive data? Can it warn of failed backups? Do you need chargeback?

Policy management
How simple is it to define and change protection levels?

Data security/integrity
Can it encrypt specific backups? How are the keys managed?

Hybrid recovery
Can it recover to different platforms, e.g. on-premise to cloud or vice versa?

Metadata re-use
Will it enable data protection metadata to be reused for added business value, e.g. analytics?

Acquisition options
DIY installation, build-to-order, appliance or managed service?

Don't forget the essentials: security, access, automation and auditing

Stand back, review and plan

As we have discussed, the whole area of data protection covers multiple requirements, services and processes, and while they can be very different, they can also be interdependent and intertwined. For example, a backup is not an archive, but it is possible for a modern data protection system to serve as an archive, a backup, a secure compliant store, and several other things besides. Of course you can instead implement all those many services as separate solutions. Indeed, you probably have had to do so already, in response to requirements that arose bit by bit. That means considerable duplication of both effort and storage needs though, with different systems storing multiple copies of the same data for different purposes.

Normally, the holistic all-in-one view is something of a luxury, with each incremental demand for a new service or a new degree of protection being insufficient by itself to warrant significant change. However, new demands such as GDPR and ransomware protection are anything but incremental. GDPR in particular requires a major response, so it is little surprise that many organisations are (or should be) allocating significant amounts of funding here.

The real opportunity lies in using that funding to reduce overall complexity and solve other problems too, by proposing and implementing a modern data protection system that will almost certainly have wider capabilities than your current systems. Its sophisticated data management can, for example, allow you to look for incremental business opportunities – new ways to use your organisation's data (within the bounds set by legal and regulatory compliance, of course). It makes sense therefore to carry out a full review, planning for any new system to cover as much ground as possible.

Allocate resources, implement solutions

While it is crucial for IT to be deeply involved in specifying, acquiring and implementing data protection systems, many of the risks and requirements are very much business issues. IT therefore needs to ensure that the business is fully involved in, for example, defining risk profiles and desired protection levels (RTO/RPO), understanding the needs of compliance and governance, and of course determining the organisation's appetite for risk overall.

IT also needs to be closely involved in building the processes that underpin all of this: without the right systems and processes in place, an investment in data protection technology may well become worthless.

In addition, the business must acknowledge and accept that it is legally responsible for its data. Yes, it will be IT that implements and maintains the foundations of data protection. However, rules such as the GDPR make it clear that failures in data privacy, for example, are the board's responsibility, and that the data protection officer should have the authority to match their responsibility.

The last question to consider is how much time and effort you will expend on physically acquiring and implementing the necessary hardware and software. Many IT departments are up-skilling from primarily being technologists to become experts in using technology to solve complex business problems. In this context, the potential advantages of doing your own hardware/software build and integration, such as greater control over the process and configuration, need to be weighed against the potential speed and simplicity of buying a complete system, either built-to-order or as an appliance.

ABOUT FREEFORM DYNAMICS

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better-informed investment decisions.

For more information, and access to our library of free research, visit www.freeformdynamics.com.

ABOUT FUJITSU

Fujitsu is the leading Japanese information and communication technology (ICT) company offering a full range of technology products, solutions and services. Approximately 162,000 Fujitsu people support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers.

This includes a strong portfolio of data protection solutions helping customers to backup, recover and archive data in a simple and efficient way.

For more information, please visit www.fujitsu.com/fts/products/computing/storage/data-protection/.