FREEFORM DYNAMICS

IN ASSOCIATION WITH

FUJITSU

DATA PROTECTION REVISITED

A RISK REVIEW AND INVESTMENT GUIDE FOR BUSINESS EXECUTIVES

FREEFORM DYNAMICS, JANUARY 2018

DATA PROTECTION IMPERATIVES AND OPPORTUNITIES

In today's digitally-driven world, the effective management and protection of electronic data is vital to minimising your exposure to risk in a number of key areas. The risks are increasing in severity too: organisations are storing ever more data and becoming ever more reliant on their software and other business technology, regulators are requiring ever greater levels of regulatory compliance, and criminals are becoming ever more devious in their assaults.

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, storage, 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

Businesses are now routinely targeted with the data-encrypting and network-aware viruses known as ransomware. Having your data encrypted can be more damaging than simply losing it, due in part to the viral nature of the attack. Ransomware defence needs to be multi-layered, including for example, user training, anti-virus software and network behaviour analysis, but if infection occurs the only reliable solution is an offline or otherwise protected backup.

Emerging imperative

GDPR compliance

New EU rules for the protection and privacy of personal data take effect in May 2018, and will affect almost any organisation that deals with EU residents. Called GDPR, the new rules require you to audit and record your use of personal data, ensure you have a lawful permission to process it, allow data subjects to check and amend it and request its erasure, and report data breaches. Penalties available for non-compliance include fines of up to €20m or 4% of your annual turnover.

From risk management to incremental business value

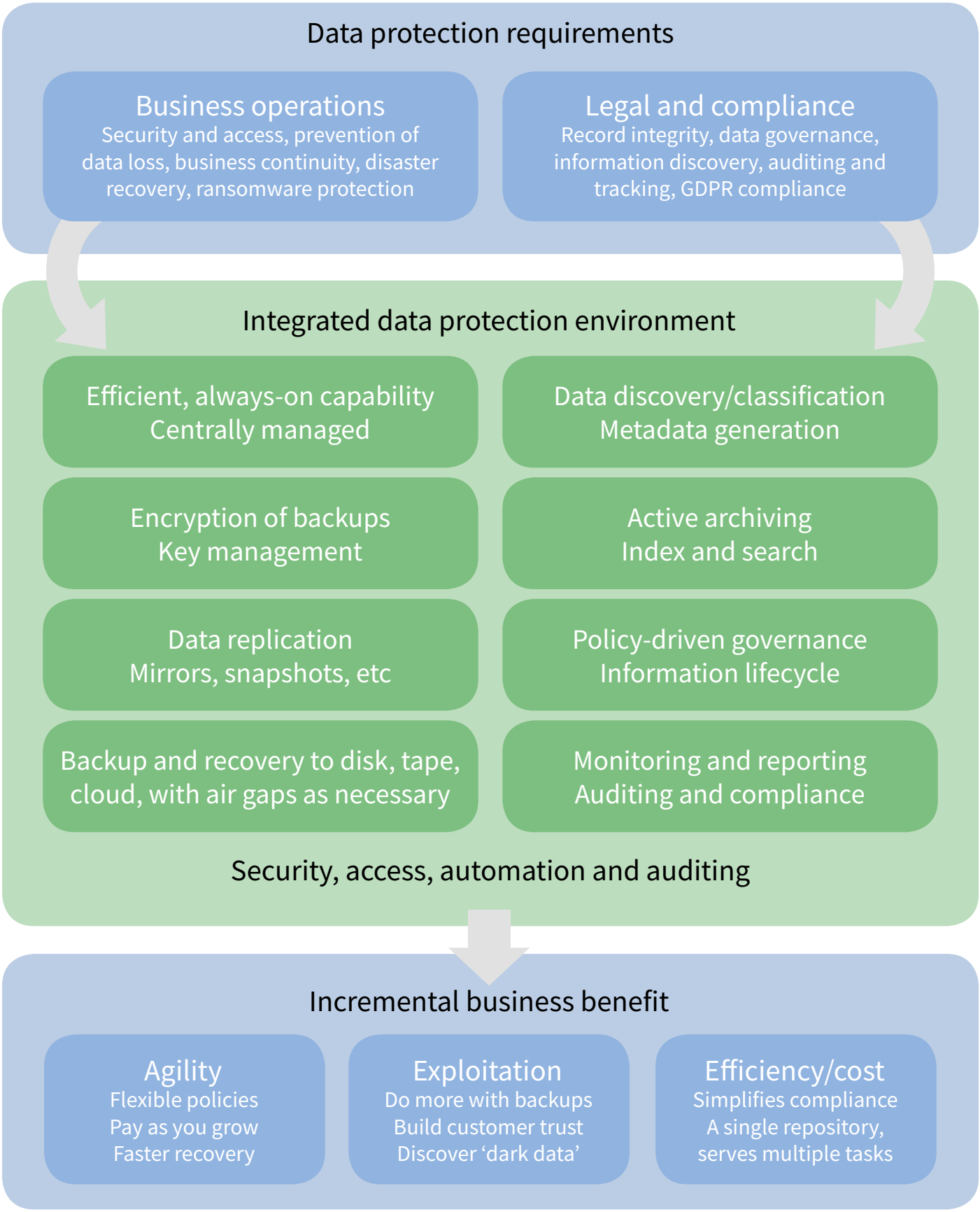
Fortunately, a large part of what is needed in order to mitigate business and legal risk is merely good data governance and management. The problem is that many organisations do not yet have good data management structures in place. The opportunity is that addressing these risks in a planned and holistic way will also equip the organisation with data management tools that it can potentially use to generate incremental business value.

The key here is the 'planned and holistic' aspect. Most of these risks could also be addressed using point solutions, but this will result in unnecessary complexity and is likely to be considerably more expensive overall than implementing a single modern data protection system to take care of it all, or at least most of it.

The downside is of course the need for a single, relatively large, purchase and implementation, versus lots of smaller, bite-size, solutions. However, the long-term operating cost of the single system should be lower and its operational benefits considerably greater.

MODERN DATA PROTECTION SOLUTIONS

Today, data protection is more than just backup, or even backup and archiving. It addresses a broad range of information management and security needs, and modern solutions acknowledge this. They can therefore integrate many capabilities that in the past were not part of traditional backup solutions and had to be implemented separately. Bringing them all together can yield considerable cost and operational efficiencies.



Stand back, review and plan

The severity of the challenges currently facing data protection offer that rare thing: an opportunity to step back, take a look at the bigger picture, and plan for meaningful change. The aim should be a holistic approach – that is, treating the whole area of data protection as interdependent and intertwined. Yes, you can implement all these services – disaster recovery, archiving, compliance and governance, etc – as separate solutions. Indeed, you probably have already done so in response to requirements that arose bit by bit over time. That often means considerable duplication of effort though, and unnecessary multiplication of your storage needs too, with different systems storing multiple copies of the same data for different purposes.

Normally, the holistic 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, today's new demands – in particular, GDPR and ransomware protection – are anything but incremental. They require major responses, so it makes sense to carry out a full review, planning for any new system to cover as much ground as possible. Key elements that you may need to include in your review include:

- Understand the implications of GDPR and the associated business requirements
- Assess your sensitivity to risk, including to emerging threats like ransomware
- Determine how will you handle the discovery and classification of sensitive data
- Decide who will take responsibility for data protection and policy definition
- Explore the incremental business opportunities offered by sophisticated data management
- Construct a balanced business case for a modern and holistic data protection solution
- Test and model alternative new solutions

Allocate resources, implement solutions

While it is absolutely necessary for IT to be deeply involved, data management – and by extension, the modern data protection system – is very much a business concern. Only the business can answer many of the questions around risk and data classification, for example, and of course it is the business that must bear the responsibility for any failures in this area, not just in terms of compliance and governance, but also any financial damage. And of course it is the business that must allocate the necessary resources, both financial and organisational, to implement solutions.

A vital part of the latter is process: without the right systems and processes in place within the business, an investment in data protection technology can easily become worthless. This in turn may well require operational and cultural changes (and of course user education) within the organisation, in particular to make data privacy an integral part of how the organisation stores, manages and uses information. In effect, privacy must be baked into your business's entire process of software development, deployment and operation.

Yet it will normally be IT that must implement and operate the necessary technology, ensuring that it satisfies the needs of the business and risk mitigation, enables data privacy, and supports those systems and processes. Modern data protection is therefore a classic example of the need for a fully-integrated project team spanning all the relevant stakeholder groupings.

One last point to be aware of is that some of the skills and resources required are sophisticated and specialist. You may well need therefore to bring them in from outside, either in the form of consultancy or via your hardware and software supplier. On the plus side, the basic requirements are common to all organisations, even if each organisation then has its own specific needs so their actual implementation may vary. This makes it feasible to consider buying a 'customisable package' from a suitably adept supplier; this is a very useful option given the GDPR time pressures, and the fact that ransomware variants continue to evolve and could strike at any time.

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/.