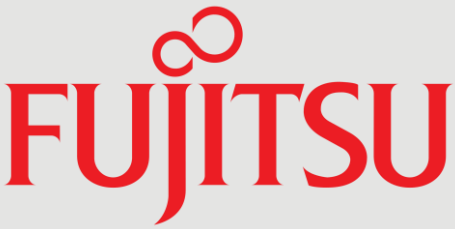
Inside Track Research Note

In association with



Data Management for a Digital World

Turn GDPR compliance and ransomware defence to your advantage

November 2017

In a nutshell

About this Inside Track

The insights presented in this document are derived from independent research conducted by Freeform Dynamics. Inputs into this include in-depth discussions with IT vendors and service providers on the latest technology developments, along with intelligence gathered from mainstream enterprises during broader market studies.

Has your organisation considered updating and enhancing its data protection capabilities but postponed the decision, perhaps due to time and cost constraints, or because of more pressing business needs? If so, then now may be a good time to revisit that decision. Two major risk-related business imperatives – ransomware protection and GDPR compliance – have recently emerged and need to be properly addressed. At the same time, as data continues to accumulate and fragment, it's becoming harder to keep track of what you have, let alone to manage it effectively.

You could approach these challenges in a reactive way, dealing with one requirement at a time in a piecemeal manner, through costly yet limited point solutions. Taking a more joined-up, proactive approach, however, using a modern data protection environment, could allow you to simultaneously deal with the risks, and generate incremental business value – even turning some threats into business opportunities.

This paper discusses how, with the right mindset and approach, GDPR compliance and ransomware protection can work as catalysts for positive change.

New data challenges, legal and criminal

Business risks come in many forms, but in today's digital environment, effective management and protection of electronic data is central to minimising your exposure in a number of key areas. While this principle is well appreciated, and most organisations have some level of data-related risk management in place (no matter how informal), two recent developments are creating a new set of challenges.

The rise of ransomware

Ransomware can be deadlier than a system crash.

Let us start with the emerging risk that is arguably the easier one to understand: ransomware. To begin with, these data-encrypting viruses were mainly a threat to home users, but in recent years criminals have increasingly targeted businesses and other organisations, using clever social engineering to fool users into accepting the virus, e.g. through spoof links and malicious attachments.

Ransomware has grown more sophisticated too, for example some versions can encrypt or delete the shadow volume copies created by Windows, or the Mac's Time Machine backups. Business-grade ransomware is also network-aware, meaning that it can infect other computers on your network. It can even reach out and encrypt network storage servers and cloud storage.

Having your data encrypted by someone else is potentially even more damaging to the business than losing it in a system crash. And while these viruses are called ransomware because the criminals offer to supply the decryption key in return for a payment, there is no guarantee that paying the ransom will get your data back. In some cases the virus only pretends to encrypt but is actually deleting your data, and the criminals simply "take the money and run". In others, the authorities may already have shut down the payment mechanisms.

Ransomware defence requires training, network protection, and an offline or protected backup.

Ransomware defence encompasses staff training to defeat social engineering attacks, and network analysis to detect and prevent the virus's attempts to spread and cause damage across your network. However, if you do get infected then the only real

solution is to restore from an offline backup or a well-protected one, for example one stored on a non-erasable write-once medium.

GDPR fast approaching

GDPR applies to any organisation that keeps data on EU residents, not just EU-based organisations.

Dealing with the EU's General Data Protection Regulation is rather more complex – unless of course you can entirely exclude EU residents and their personal data from your organisation's data processing activities. If you can't, then whether you are EU-based or not, it will be mandatory from May 2018.

Before we go on, it's worth clearing up a potential source of confusion that often arises when IT professionals start to explore GDPR and its implications. To anyone looking through a traditional IT lens, the term 'data protection' means ensuring the security and availability of data, via techniques such as backup, access control, encryption and replication. However, to the national Information Commissioners and Data Protection Agencies who supervise GDPR compliance, 'data protection' means regulating access to, and the use of, people's personal data, i.e. it is primarily about respecting customer privacy.

Modern data protection must also cover the privacy of personal data.

The good news is that these different definitions are actually two faces of the same coin, which opens up opportunities to leverage the same investments across both from a technology perspective. More of that in a minute.

Back to GDPR, despite our mention of technology, one of the challenges is that you can't just buy a solution, turn it on, and then assume you are good to go. Compliance requires the right behaviours to become an embedded part of the way you work.

It starts when you acquire the data and any related consents, continues as you establish quality controls and audit and track data access and use, and extends to how you assure accountability and transparency and life-expectancy and ultimate erasure.

Design for privacy to be the norm, not the exception.

A useful concept here is 'privacy by design', making privacy the default rather than an optional extra. As an example, you can mask or obfuscate customer and employee data as standard when it is accessed outside of rigorously controlled transaction or engagement systems. Even better, don't collect data that you don't need in the first place. And whatever approach you take to anonymisation, always consider how much work and extra data it would take to re-identify your data subjects, because combining or cross-referencing data sets could easily bring the data back within GDPR coverage.

The principles of privacy by design are well established and are recommended by regulators and others around the world. Of itself, it is not a complete solution to the challenges of personal data protection; it is an important step along the road, however. For example, baking it into your software delivery processes to build a privacy mindset among your developers can reduce the likelihood of inadvertent compliance breaches.

Turning risk to advantage

An information audit is good practice for data management and governance overall, not just a tool for demonstrating GDPR compliance.

Much of what is required both for GDPR compliance and ransomware protection can also bring significant benefits to an organisation in other ways, if implemented with that in mind.

For example, the UK regulator's self-assessment plan for GDPR recommends an information audit that maps your organisation's data flows, detailing how you will deal

with subject access requests and the right to erasure, and having procedures to detect, report and investigate personal data breaches and misuse.

Good data management is useful for a lot more than just regulatory compliance.

All those are just aspects of good data management, and you don't have to think very hard to come up with ways that the same audit data and the resulting data management structures could also be used in more mainstream business processes.

The fact is that many organisations do not have good data management structures in place. Data may be held in silos, not cleansed or secured properly, and used for purposes it wasn't supplied for and which the organisation is not aware of. Fixing all that, even if it's done because GDPR insists on it, will result in data that is easier to find and make use of.

Similarly, in this world of exponential data growth we need metadata and data lifecycle tools to help us realise the full business value of the information held, in data archives as well as primary storage systems and databases. In the past, data usually became less valuable as it aged, but the ability to gain insights through analytics now means that the more data you have, the more valuable it can be – if you have those GDPR-driven data management capabilities in place.

The ability to gain insight through analytics means more data can mean more value.

Other defences can be turned to your advantage too. Data recovery after a ransomware infection requires a layered data protection scheme with the ability to roll back changes if possible, and the existence of a protected or air-gapped backup, such as tapes stored offline or non-erasable media, as the final line of defence.

If this drives organisations to make it easy to restore damaged systems, that can also pay off in other ways. Thorough backups of desktop PCs might reveal valuable 'dark data', such as locally stored customer lists or correspondence, which can now be leveraged for business value. Or the same protection systems could also provide self-service access for users to recover files that they accidentally deleted or over-wrote.

Adhering to the GDPR's values of fairness, accuracy and transparency can help build customer trust.

And there are reputational advantages to be won. From a risk perspective, failing to protect users' personal data, or abusing their privacy, even if inadvertently is likely to damage your reputation and brand, weaken your customer relationships, and could ultimately cost you money, not just in fines but in lost business. Turning this around, from an incremental business value perspective, GDPR compliance helps to demonstrate that customers can trust your organisation with their personal data. If you can build trusted relationships, there's then an opportunity to extend your use of that data and derive more value from it, with the appropriate consents where needed.

Taking action on GDPR and ransomware

For ransomware defence it is crucial to assess whether your data protection systems are fit to withstand an attack. If an infection gets in, can it reach and attack your backups? How readily can you restore a system, once it has been disinfected?

It is crucial to assess your data protection systems' resilience to ransomware attacks.

While there is no 'one size fits all' solution to GDPR, the requirements are the same for every commercial or professional organisation, with the proviso that those with fewer than 250 staff are exempt from some of the record-keeping provisions. We have provided some other GDPR related specifics in Appendix A, including comment on some of the common myths you might come across.

In the meantime, it is worth noting that to help with some of the practicalities, several advisory groups have developed structured methods or processes for self-assessment

Organisations need to discover what personal data they hold, and determine its compliance status.

and achieving compliance. As an absolute minimum, organisations need to discover what personal data they hold, determine its compliance status, and if necessary, implement the controls needed to demonstrate GDPR compliance. Fortunately, modern backup software does more than just backup and restore: increasingly it provides a range of additional information management functions.

Solutions, not just strategies

There is no shortage of would-be advisers who will help you assess your GDPR readiness and formulate a strategy for achieving and maintaining compliance. Time is short, though, and the last thing most organisations need is another point solution.

A better approach therefore is to use ransomware and the GDPR as catalysts, and do the job properly by moving to a modern, compliant and all-embracing data protection platform. That's because your backup platform covers all your data – or it should do – so it is the most logical place to start building information management and governance strategies, leveraging the core metadata that it already gathers on files.

Turn the threats of ransomware and the GDPR into catalysts for positive change.

If you lack the necessary in-house skills and resources for this, look for a partner who can not only provide that advice, but who also has the blueprints or plans necessary to design a suitable data protection and governance system. You may also want a partner with access to the hardware, software and support skills needed to build, commission and maintain that system for you.

Technology alone is not enough

A modern data management and protection system can bring significant benefits, not least because it gives you the technical foundation that you need in order to handle information risks better. However, technology alone can't solve all the challenges of ongoing information management. Most organisations will need assistance both at the assessment stage, and when it comes to making governance and operational process recommendations based on those assessments.

Most organisations will need practical help with data governance and mapping, as well as compliant data protection systems.

Developing new data management and information governance capabilities may also require operational and cultural changes within the organisation, as will the adoption of privacy by design. Top-level commitment within the organisation is of course essential, and most organisations will need expert advice and assistance here too.

The bottom line

Few organisations, and certainly none in Europe, can afford to ignore GDPR compliance, and none can ignore the threat of ransomware. Yet we keep hearing of organisations struck by the latter, and woefully under-prepared for the former.

The threats are real and existential, but not insurmountable.

The doomsayers who liken them to onrushing trains are overly negative, however. Yes, the time is short, but there are suppliers who can provide both advice and complete hardware/software solutions (though of course complete safety can never be guaranteed).

Fortunately, facing these challenges brings opportunity as well as risk. Yes, organisations absolutely must make a firm commitment to the necessary technical, operational and cultural changes – and these can be significant. But they should also look at them as opportunities to improve the business and how it serves its customers, not just as costs and bureaucracy.

Appendix A: GDPR truths and myths

Knowing what you legally can and can't do with the data you hold is essential.

It can sometimes be hard to sort fact from fiction where the GDPR is concerned. As an example, one of the myths about the GDPR is that it is all about explicit consent. However, while the subject's explicit consent is necessary for processing sensitive personal data, it is not the only lawful basis for processing personal information. Others could include banks sharing data for fraud prevention, say, or insurance companies processing policy claims, and individuals handling data for non-commercial personal or household purposes.

However, it is true that data can only lawfully be processed for the reason it was collected, unless you have consent to use it for anything else. This guiding principle means the bank or insurance company would still need consent to also use it for marketing or big data analytics.

Transparency is a key GDPR principle, so if you get it wrong, report it fast and report it truthfully.

Also true is that the regulators can levy significant fines – up to €20 million or 4% of an organisation's world-wide turnover, whichever is higher – for non-compliance. The idea that regulators will start issuing €20m fines from May 2018 is largely a myth, though: the GDPR requires fines to be proportionate to "the nature, gravity and duration of the infringement", and allows reprimands to be issued instead where appropriate. The regulator is expected to take into account your prompt and honest notification and the efforts that you took to prevent or mitigate harm, for instance.

Another GDPR truth is the importance of record keeping. It is essential to note which categories of personal data were processed and for what purposes, plus details of transfers to third parties or other countries, security measures in place, and so on (there are exemptions for smaller organisations). Your data protection officer – who is legally required to have expertise in data protection law – should be able to advise here.

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, please 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/.

Terms of Use