

White Paper

Understanding and Addressing Data Issues within the Financial Sector

Fujitsu understands the business pressures that the Financial Sector (FS) is currently experiencing, from the drive to capture a greater market share and increase profitability by providing the services that customers are demanding, to continually trying to lower their costs and improve efficiencies. We also appreciate that FS organisations are striving to drive through the digital transformations, introduction of new technologies and the implementation of operational changes required to compete within a continually evolving and increasingly competitive marketplace. While at all times having to maintain the agility and flexibility required to address increased compliance and risk obligations.

Fujitsu recognises that at the core of all of these objectives, initiatives and obligations is an organisations data, the key for FS organisations to be able to successfully deliver against their business strategy while meeting legal and compliance obligations is their ability to fully understand, correctly align and manage their data in the most appropriate manner.

Global data volumes continue to grow at unprecedented rates and the FS sector is not immune to this trend, FS organisations are now creating, ingesting, storing, sharing, securing, protecting and analysing more data than ever before.

This White Paper examines some of the main data issues faced by the FS and outlines how Fujitsu and its strategic partners can work with FS organisations to give them a better understanding of their data, thereby making it easier for them to align it to their business strategy and maintain compliance, as well as allowing them to exploit the valuable business information that their data contains.



Introduction

Unlike other industries, the Financial Sector (FS) does not make or sell any physical products therefore the data that they generate and ingest is arguably their most important business asset. Over recent years there has been a seismic shift in value within the FS from the balance sheet to the data, and it is now recognised that the information the FS holds about its customers has significant business value. However, in order to extract and exploit that value, which is key in driving future revenue opportunities, FS organisations must first be in a position to fully understand and align their data.

Because of data value, organisations across all markets are now moving away from simply viewing data as a commodity and are beginning to view their data far more strategically and to treat it as a living and evolving business asset, one which, if understood and managed correctly is capable of unleashing significant new revenue generating opportunities.

However, the growth, origin and structure of that data is undergoing dramatic changes as customer bases diversify and place increasing demands on the FS to provide the capability to conduct business on the consumers terms as well as on a 24x 7x 365 basis.

In order for any FS organisation to be able to embark on a programme to monetarise and exploit the information contained within their data while also maintaining compliance, managing costs and resources as well as meeting the ever-increasing demands not only of their own business but also of their customers, there are a number of data issues whose origin and business impact must be fully understood before they can be properly addressed.

Data Growth and the Rate of Change

By its very nature the FS has for many years been a data driven industry and that data continues to grow at unprecedented rates. There are many sources predicting significant growth carrying on towards 2020 and beyond, with IDC estimating that in 2025, the world will create and replicate 163ZB of data (i.e. 1.63×10^{23} bytes – see Fig. 1), this represents a tenfold increase from the amount of data created in 2016. However, it is not just the volume of data that has to be contended with but also the rate of data change, for example there is every indication that the 'Data Cosmos' is doubling every two years, when you also factor in the social and behavioural changes that are taking place within the FS market and its customer base then it's easy to see why FS organisations now have far less time to react to the demands that their data places upon their business.

These issues are further compounded by rapidly increasing consumption of data as financial organisations strive for increased market share and more effective data exploitation in the face of increasing compliance legislation. For the highly data dependent organisations within the FS who are trying to understand their data and how best to exploit its full potential in the face of greater customer demands and increasing legislation while facing up to both established and emerging competition this growth and change present significant business challenges.

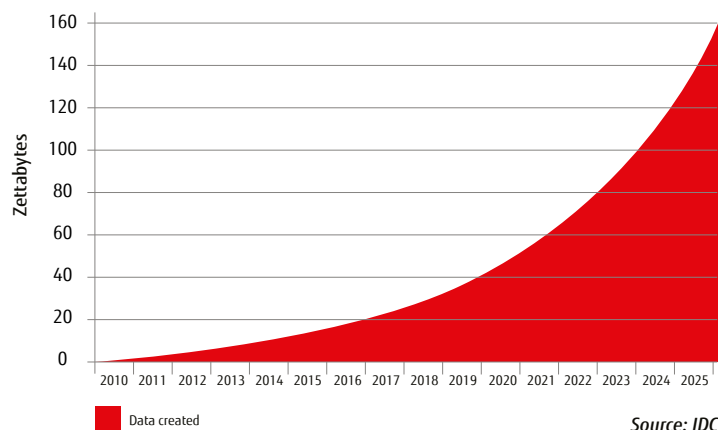


Fig. 1: Predicted increase in global data creation

Understanding Data Origin and Maintaining Quality

Both corporate and retail consumers now require an on-line, always available digital experience from their financial providers. This increased level of customer interaction means that data is now in many different formats as well as being ingested from multiple and diverse sources (see Fig. 2). Complications are further compounded by the changing state of the data once it comes under an organisations control, for example, not only can it have different attributes such as primary, secondary and archive, it can also move between these attributes in any direction and at any given time. There are multiple factors that can influence this ‘change of state’ such as the age of the data, current business requirements, external influences (such as changes in legislation) and even in the movement or sharing of the data between locations and organisations.

The challenge here for FS organisations is to understand their data flow and lifecycle in order to be able to confirm its validity, integrity, accuracy and consistency which must be verified, understood and maintained at all times.

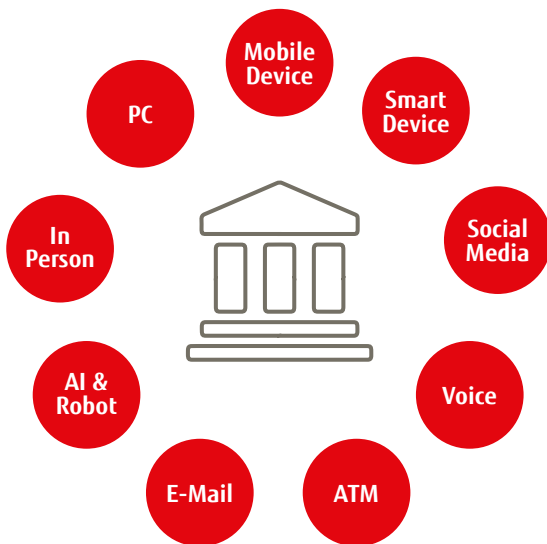


Fig. 2: The Financial Sector now has to cope with multiple data origins

Legacy Architectures and Data Sharing

As previously stated, global data volumes are growing at unprecedented rates. Within the FS this can be attributed in the most part not only to the moving away from traditional offerings to more information driven solutions that are required to meet customer expectations but also by changing business requirements and continued legislation.

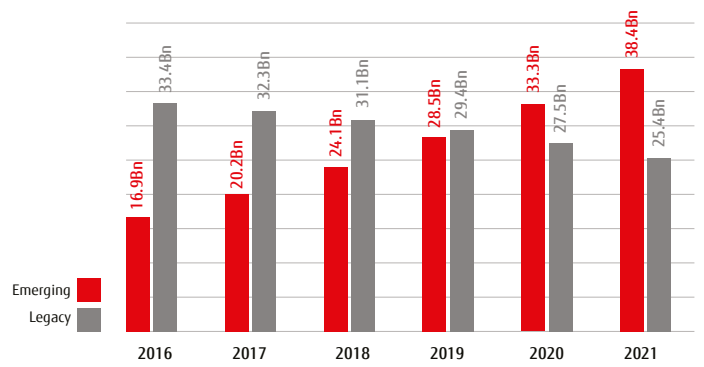
This seemingly unending increase in data coupled with the changes in business operations will highlight and significantly increase the complexities, inefficiencies, vulnerabilities and costs of the current legacy systems.

Simply increasing the complexity of traditional data solutions to meet changes in customer expectations and business requirements puts an increased strain upon the infrastructure. This increase in complexity can result in storage, backup, archive, disaster recovery, business continuity and compliance issues as well as negatively impacting customer service. As data is now created, shared and accessed across multiple business lines and organisations, the challenges over understanding, unifying, distributing and sharing data are now even more complex. A result of this is that FS organisations are now beginning to recognise the limitations that are being placed on their business by their legacy data systems.

The layering of new technologies from Fintech companies as well as artificial intelligence (AI), intelligent process automation (IPA) and robotic process automation (RPA) over the top of out-of-date core infrastructures is not the way forward and will only serve to create larger and more costly issues as demands on the business increase.

To address these issues will require more than just a technology change to existing infrastructure. In many cases a complete overhaul of the front and back-end systems as well as the supporting business processes and procedures will be required to effectively drive the digital business transformation needed to meet evolving demands placed upon the FS by their consumers, competitors and external obligations.

In a recent analysis for Fujitsu, PAC have concluded that by 2020 global spending on emerging technologies such as Cloud, IoT and Big Data analytics will outstrip that spent on legacy environments (see Fig. 3). However, the ability of FS organisations to understand and manage their data will be a key component in ensuring that any financial outlay on new technologies will be able to deliver against business expectations.



Source: PAC

Fig. 3: Projected Legacy and Emerging Technology Spend

Data Security and Privacy

The 2017 Internet Organised Crime Treat Assessment (IOCTA) conducted by the European Union Agency for Law Enforcement Cooperation (EUROPOL) categorised FS organisations as part of the ‘Critical Infrastructure’, i.e. an asset, system or part thereof located in member states which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of its people, (see Fig. 4). Any disruption or destruction of that infrastructure would have a significant negative impact both within the country affected as well as within a wider geographical context and result in their inability to maintain vital functions. The importance of the FS to the overall economy as well as the critically of their data to an individual organisation means that a high level of security is a core component of any FS organisation’s data management strategy.

Because of the very nature of their business, FS organisations will always be a target for criminals. Industry figures suggest that during 2017 cyber-attacks within the financial sector increased in excess of 140%, resulting in significant losses for those organisations affected, and a report by Cybersecurity Ventures estimates that by 2021 cybercrime damages across all industries will be in the order of \$6 trillion annually. However, it is not just the increase in the size, frequency and cost implications of these attacks that are a major cause for concern but the fact that criminals are becoming far more sophisticated in the targeting and execution of these crimes, making prevention, detection and remediation far more challenging and costly.

As a result of the increase and sophistication of attacks the barriers that organisations are now having to erect around their data to prohibit access are becoming increasingly complex making the necessary access and sharing of data far more difficult.

Unlike security which is the act of erecting barriers around data to restrict access, privacy is a collection of legal rules and guidelines that dictate how data can be used, shared, stored and transferred. While there have been laws in place protecting privacy for many years the increase in cybercrime, the rights of the individual and the value of information has seen the introduction of additional legislation that has major implications for organisations both inside and outside of the European Union (EU) when it comes to managing their data. This legislation has brought data security and privacy conversations to the forefront for FS organisations.

While the penalties for data breaches imposed by the various regulatory bodies can be significant, they can be relatively small when compared to any loss of consumer confidence. The rise in social media, the globally interconnected news networks and the increasing ease at which customers can change their financial service providers means that organisations need to be aware of the significant damage to their reputation, brand image and profitability that can be done should it emerge that they have experienced security and/or privacy issues involving customer data.

As FS organisations are built upon trust and security, and as data volumes increase and these organisations look to profit more from their data while maintaining compliance, security and privacy, any lack of data understanding could result in the introduction of increased vulnerabilities and risks into already highly complex environments.

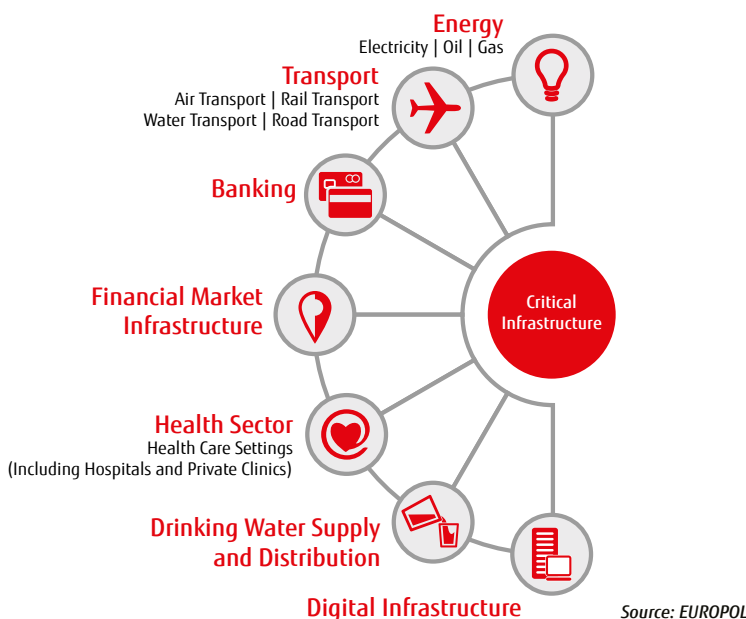


Fig. 4: Due to the key role played by FS organisations data security is a core requirement

Data Governance and Usage

When it comes to their data FS organisations are amongst the most heavily regulated within any industry. However, recent additional legislation in the form of updated versions of the Markets in Financial Instruments Directive (MiFID II), the Payment Services Directive (PSD2) and the new General Data Protection Regulation (GDPR) further increases the complexity around data governance and its usage.

MiFID II (3rd January 2018) builds on existing stock trading regulations and is aimed at bringing greater transparency to the financial markets. This will not only give investors increased visibility to ensure that they are being treated fairly but it will also give regulators greater insight into trading and sales activities allowing them to identify any anomalous activities earlier. For example, one of the ways that MiFID II is looking to increase the level of transparency is by enforcing that the trading of bonds (and some derivatives) will have to be conducted electronically and not over the phone. These measures will not only increase the volume of data that financial organisations have to manage but they will also increase the complexity of that management as the data will have to be stored, protected, shared, analysed, aligned as well as ensuring that it meets compliance requirements.

PSD2 (13th January 2018) is a broad and complex piece of legislation looking at a wide range of areas from technology and security to reporting and pricing. From a high-level perspective PSD2 can be broken down into three areas. Firstly, it relates to openness and conformity when it comes to pricing as well as firmer standards regarding reporting.

Secondly, it looks at security (e.g. strong customer authentication) and thirdly, PSD2 concerns itself with the access to accounts whereby financial institutions must allow other financial service providers to connect with their systems to access account information and initiate payments on behalf of customers.

As well as these three areas, under PSD2, organisations must also provide a testing capability whereby other financial service providers can develop and test new services that use their interface.

GDPR (25th May 2018) looks to protect the personal data of European Union (EU) citizens by standardising data privacy laws and processes across all industries and business sectors within the EU. While GDPR is a EU directive it is applicable to any organisation that has business operations with the EU or holds personal data on any EU citizens. As with both MiFID II and PSD2, GDPR is a complex piece of legislation comprising of eleven chapters and ninety-four articles (see Fig. 5) however, there are a number of key data areas for the financial sector.

GDPR Key Area #1 'right to be forgotten and data erasure', under GDPR individuals can request access to their own personal data or its removal without the need for any external authorisation. Some data may be retained to ensure compliance with other regulations, but if there is no valid justification the individual's right to be forgotten takes precedence.

GDPR Key Area #2 'consent', under GDPR customers retain the rights to their own data. Because of this there is no automatic opt-in regarding the collection of their personal data and customers have the right to know what personal data is being gathered, what it will be used for, and should there be a requirement to share the data with third-parties, additional consent will be required.

GDPR Key Area #3 'data flow', data is now not only collected from multiple sources it is also shared and transferred across multiple geographical locations and in many cases across multiple organisations (e.g. PSD2 access). GDPR imposes strict end-to-end accountability thereby ensuring that a customer's data is adequately protected by ensuring that not only the data owner is fully compliant but any organisation that may have access to that data is also fully compliant.

GDPR Key Area #4 'pseudonymisation', in order to ensure that personal data is maintained under a need-to-know basis GDPR aims to ensure that personal data, irrespective of whatever environment it resides within, must undergo a level of pseudonymisation (i.e. personal data must be processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional (separately held) information).

MiFID II, PSD2 and GDPR place additional strain on data management and further heighten the requirement that in order to effectively manage their business as well as meet their compliance and legal obligations, FS organisations must have a comprehensive understanding of their data because data that is not understood cannot be deemed compliant.



Fig. 5: The 11 Chapters of GDPR

Fintech

Traditional FS organisations have always proved to be highly resilient to any disruption of their business brought about by technology. However, this resilience is not as strong as it once was and the changes that are emerging will have a significant impact on data and how FS organisations go about understanding, aligning and managing that data.

In order to meet the ever-increasing demands not only of their consumers but also of their own internal business, established FS organisations are now embracing 'Fintech' (i.e. Financial Technologies brought about by new and emerging companies) at an accelerated rate.

Fintech now covers a broad spectrum across the financial landscape and according to McKinsey, Fintech activity within capital markets infrastructure has grown by almost 300% since 2010 (see Fig. 6). However, as with GDPR there are a number of key Fintech areas that many FS organisations are now focusing on that carry significant data management implications.

Fintech Key Area #1 – Distributed Ledger Technology (DLT), often referred to as 'Blockchain', this is a cryptographically encoded, highly detailed ledger of financial transactions which is distributed across either a public or private network. It promises to deliver significant cost savings through decreases in transaction times, increased security and increased process efficiency.

Fintech Key Area #2 – Analytics, Machine Learning (ML) and Artificial Intelligence (AI), these are helping FS organisations in areas such as Big Data information extraction, customer segmentation, personalisation and profiling, trading, improved decision making, fraud detection, risk management and operational effectiveness.

Fintech Key Area #3 – Increased automation and robotics, these are being used to drive an increase in efficiency and uniformity in areas such as fraud detection, risk management and compliance reporting.

Fintech Key Area #4 – Cloud, the changes in customer requirements and the need to control rising costs are driving many FS organisations towards looking at a utility IT model (as opposed to a more traditional in-house model) for parts of their infrastructure. This will help eliminate any constraints around physical locations, help to speed up deployment, transfer maintenance onto a service provider, free up resources for business development and also help drive down costs.

Open Banking

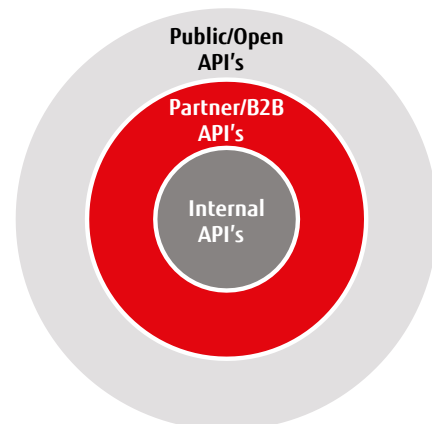
Open banking is a relatively new concept and it brings with it a significant number of considerations around how financial data is managed and shared.

Once customers have given their permission, open banking will allow them to share their financial data with other authorised FS organisations through shared APIs (see Fig. 7), which is one of the core principles of PSD2. It is hoped that open banking will help drive innovation within product offerings, improve customer interaction and provide improved services for customers.

However attractive this concept seems in principal, in practice things may be quite different. An open banking ecosystem provides an engagement platform for a multitude of participants from data owners and their customers to third-party suppliers and regulatory authorities. Even though data security is a vital component for all FS organisations, initiatives such as open banking (as well as their drive to increase their digital footprint) will only increase the risks associated with data loss, fraud, identity theft and other cybercrime activities.

FS organisations that embark down the open banking road will have to pay even closer attention to the management of their data as understanding how it is created, ingested, managed, shared and secured as well as ensuring full compliance to current regulations such as PSD2 and GDPR will be crucial for successful implementation.

Model Type	Attribute
Public/Open API's used by external partners and developers who build innovative applications and products.	Innovation through engaging the developer community Extended market reach
Partner/B2B API's used by business partners, including suppliers, providers, resellers and others for tighter partner integration.	Reduced partner costs API monetarisation Enhanced security
Internal API's are used by developers within organisation.	Cost reduction Operational efficiency Enhanced security



Source: McKinsey

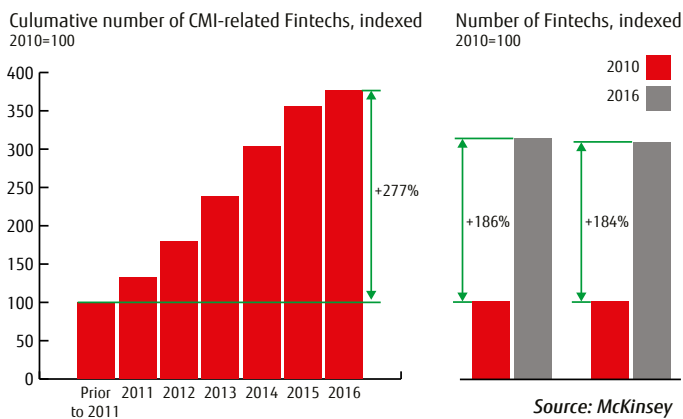


Fig. 6: Increased Fintech growth from 2010

Fig. 7: API Model

Cryptocurrencies

Cryptocurrencies have been seen as a disruptive innovation within the FS, as they allow digital transactions between two parties without the need for any third-party involvement. Unlike traditional currencies, whose circulation is tightly controlled by Central Banks, cryptocurrencies don't physically exist therefore there is no external control over them.

However, the fact that Bitcoin alone increased its value by more than 2,000% in 2017 and in January 2018 there were in excess of 1,380 cryptocurrencies available over the internet, gives a strong indication that they will be around for some considerable time. A recent report by Cambridge University's Centre for Alternative Finance shows that while cryptocurrencies still occupy a niche market the numbers involved were larger than industry expectations and are continuing to grow (see Fig. 8).

To ensure security, DLT is used, whereby every cryptocurrency transaction is digitally recorded in blocks which act like ledgers, all blocks are connected to each other in strict chronological sequence to form a blockchain (hence the name).

However, the information of the parties who are participating in the cryptocurrency transaction is not revealed and the money can only be tracked once it is converted into controlled physical currencies.

Initially many FS organisations questioned the credibility and long term viability of these cryptocurrencies, but those thoughts have now changed. FS organisations have now recognised that DLT was simply the engine used to drive and underpin cryptocurrencies and that its ability to increase transaction speeds, heighten transparency, tighten security and reduce costs can equally be applied to other areas of their business.

With this in mind six of the world's largest banks (UBS, Barclays, Credit Suisse, Canadian Imperial Bank of Commerce, HSBC and MUFG) have collaborated to create a new cryptocurrency, called Utility Settlement Coin (USC). They will use USC to settle securities transactions by paying each other in USC's for buying and selling securities without any waiting period for traditional money transfers. This project is seen as paving the way towards the introduction of cryptocurrencies created and controlled by the world's Central Banks.

But, as with all new technologies and innovations cryptocurrencies bring with them significant data management issues (e.g. data volumes, transparency, security and compliance) for FS organisations who are looking to go down this route.

The Internet of Things

Over the next five to ten years the connectivity and communication brought about by the Internet of Things (IoT) in order to share information, anticipate needs, solve problems and improve efficiency will have a significant impact on FS organisations and their data management.

Even though we are still in the relatively early stages of exploiting the potential that the IoT is promising to deliver, the impact has already been felt within FS organisations. But, with Gartner predicting that there will be in the order of 25 to 30 billion IoT devices by 2020 that impact is set for a major increase.

We have already seen today how FS organisations are using the IoT, for example, insurance companies applying the concept through telematics, which allow for the monitoring of driver behaviour for the purposes of car insurance. However, current IoT exploitation by the FS at the moment is only scratching the surface and the opportunities that the IoT could deliver are currently only bounded by how today's requirements are perceived. As the IoT matures and FS organisations begin to understand its potential in more detail those opportunities will grow at a significantly accelerated rate (see Fig. 9).

By its very nature the IoT generates vast amounts of data and like all data if it is to have any business value then FS organisations have to be in a position to understand, store, protect, share, analyse, align and maintain compliance around it.



Fig. 9: Some of the FS opportunities offered by the IoT

Significant rise in market capitalisation	~6,000,000 Active Wallet Users	~11,000,000 Active Wallet Users	~2,000 Full-time employees
Industry operates within both localised and globalised environments	~31% of companies operating across multiple sectors	Increased levels of fluidity within the industry	Issues around security and compliance will remain prevalent

Source: Cambridge University

Fig. 8: Key Cryptocurrency Industry Information

Resources

So far, this White Paper has concentrated on the business and technical side of FS data. But successful data management is also very much about the people. FS organisations have to also understand that to effectively manage their data and to fully exploit the information that it contains in order to deliver the services its customers are demanding, diversify into new markets, grow their business and maintain compliance they will also have to ensure that they have the ‘correct’ people in place.

One example of the negative business impact that can be brought about by not having the correct resources in place is U.S. Bancorp. In 2018 U.S. Bancorp the parent company of U.S. Bank was fined \$613M for having insufficient anti-money-laundering (AML) controls in place. The US Attorney’s Office said that U.S. Bancorp’s AML program was “highly inadequate” and could be attributed in part to a lack of appropriate staff and resources.

Data roles such as consultant, analyst, manager, architect, administrator or scientist are currently at a premium within the IT and FS industries and are set to remain so as even greater emphasis is continually placed on data, with IBM predicting that the industry demand for data scientists will increase 28% by 2020 in the US alone (see Fig. 10). Therefore, FS organisations will need to ensure that they have the correct recruitment plans, organisational structures, remuneration packages, career paths and retention plans in place for their employees if they are to deliver against their business strategy.

Data Professional	Number of 2015 Postings	Projected 5-Year Growth	Estimated 2020 Postings
All	2,352,681	15%	2,716,425
Data Decision Makers	812,099	14%	922,428
Functional Analysts	770,441	17%	901,743
Data Systems Developers	558,326	15%	641,635
Data Analysts	124,325	16%	143,926
Data Scientists	48,347	28%	61,799
Analytics Managers	39,143	15%	44,894

Source: IBM

Fig. 10: Table showing double digit rise for data professional jobs in the US

Summary

Many of the IT analysts are now talking about “Data being the new oil” while this may be a somewhat oversimplified statement, there can be no doubt that corporate data is growing at hugely accelerated rates and given that FS organisations hold massive volumes of data about their customers and their financial transactions, that data and the information it contains is a critical business asset. As the FS industry continues to evolve and their data landscape continues to change, data will still need to be stored, protected, secured, analysed, shared, aligned and managed in numbers and ways that were inconceivable less than a decade ago.

Governments and regulatory bodies have realised that as the volume of data grows and is used within an ever wider commercial context the risk of misuse and criminal activity also increases. Therefore, new legislation has been introduced to protect the interests not only of the FS organisations involved but also the rights of the individual.

Increased competition as well as new technologies and advancements both innovative and disruptive are continually emerging to challenge the market presence that has long been seen as the entitlement of the established FS organisations. These changes bring with them further data challenges, and in order to meet those challenges, retain (and grow) their customer base and successfully deliver against their business strategy FS organisations are having to change the way they view and manage their data.

Trying to implement both operational and technological change within FS organisations places significant strain on the business, the IT infrastructure and the employees. So, FS organisations need to understand how they are going to react and adapt to these changes to ensure that their short, medium and long-term business objectives are met. Technology was once seen as the answer to all business problems, however, FS organisations are now beginning to realise that technology on its own is not a panacea to solve their increasing business issues. The key to implementing the correct business changes as well as deploying the most appropriate technology solution lies with understanding their data and how it is viewed, aligned and managed within their organisation.

FS organisations now understand that in order to address the business challenges they face they not only need the correct operational and technological solutions in place they also need to have the correct people in place as well. Not having the required level of data expertise in the organisation constitutes a significant business risk.

This White Paper has shown that the rapid increase of data volumes, the strain on existing infrastructures, the increased need for security and privacy, new and emerging technologies, increased competition, increased digital channels into existing and new markets, evolving customer requirements, increased legislation and the need for employees with the correct data skills continues to generate significant business issues for FS organisations.

But, before any action can be undertaken or business issues and requirements addressed, the data first has to be fully understood within the context of the business, correctly aligned to business strategy and managed in the most appropriate way. It is this understanding, alignment and management of the data that is the key for FS organisations when it comes to meeting their business objectives.

Because, data that is not fully understood or correctly aligned not only delivers no business value, it cannot be said to be compliant, this lack of understanding constitutes a significant business risk, be it reputational, financial, operational or legal. It is these areas that Fujitsu and its strategic partners can work with FS organisations to enable them to understand, align and achieve compliance around their data.

How Fujitsu and Veritas can help FS Organisations address their data requirements

Working together, Fujitsu and our strategic partner Veritas deliver the capabilities that FS organisations require in order to meet the significant data challenges that they now face. By taking advantage not only of our combined and extensive data knowledge and experience within the financial sector but also our complementary technologies and services FS organisations can be assured that they will be dealing with a partnership that not only fully understands their business objectives, but also has the combined expertise and integrated product portfolio necessary to meet their data requirements.

We fully acknowledge that technology will always play a fundamental role when it comes to the management of FS data. However, we also recognise that any technology that is deployed, in order to maximise investment and deliver the anticipated business benefits must first be correctly aligned to the immediate business requirements and long-term business strategy.

That is why we take a business centric approach to looking at data, from how the data is created and ingested into an organisation, to how it flows and is accessed throughout its lifecycle, down to its business criticality and how it is stored, protected, secured, analysed, shared and maintains compliance. This enables us to build up a detailed data picture which allows for greater data understanding in terms of both business and compliance objectives as well as correct data alignment to business requirements and strategy.

Working in close collaboration Fujitsu and Veritas can help address some of the most pressing data issues faced by FS organisations:

Data Management

To combat the data deluge that FS organisations are currently experiencing and in order to reduce risk by meeting their business and compliance obligations there is a strong requirement to be pre-emptive in data management. Our purpose-built retention management platform allows FS organisations to execute diverse strategies in order to meet business and regulatory information retention requirements.

- Centralise retention management across email, files, social media, and more.
- Capture all records electronically including voice, SMS and MMS.
- Provide granular retention periods and WORM storage.
- Scale easily from managing 100s of users to 100s of thousands.
- Deploy on-premises, hybrid configurations, or in the Cloud.
- Archive to help improve backup and recovery performance.

Predictive Analysis

The increased volume and complexity of data coupled with the need for greater understanding and compliance means that FS organisations cannot afford to address issues after they have occurred. Our predictive analysis solution gives FS organisations the capability to analyse, track and report on their data, allowing them to deliver organisational accountability for file use as well as security. It can scale to petabytes of data and billions of files giving FS organisations the ability to comprehensively manage their file requirements, while also integrating with archiving and security solutions to prevent data loss and ensure policy-based data retention.

- Automate governance through workflows and customisation.
- Drive efficiencies and cost savings in unstructured data environments.
- Maintain regulatory compliance for information access, use, and retention.
- Protect confidential information from unauthorised use and exposure.

Risk Reduction

Today's FS environments are fast-growing, often fragmented, and overwhelmingly complex. FS organisations face daily questions about whether their data is protected appropriately, whether it can (or should) be deleted, and whether they are exploiting the most cost-effective storage opportunities. Our data visualisation solution helps FS organisations address these challenges by providing an immersive visual experience that offers a complete picture of data across both on-premise legacy environments as well as Cloud infrastructures.

- Aggregate a comprehensive view of the global information environment.
- Identify areas of value, areas of risk, and areas of waste.
- Reduce the unnecessary cost of useless data storage.
- Prioritise targets for regulatory compliance and security investigations.

Increase Resolution Times

The legal and compliance regulations faced by FS organisations require immediate responses to any official requests, this time constraint can place significant pressure on both the business and IT. Our eDiscovery solution has a simple, intuitive interface which allows FS organisations to respond to requests in a timely and detailed manner.

- Deploy a single solution across the entire eDiscovery lifecycle, from legal hold and collections through analysis, review and production.
- Easily map the entire data landscape to locate relevant documents and communications.
- Trigger advanced analytics and machine learning to uncover critical evidence.
- Reduce manual effort and mitigate human error with workflow automation.
- Achieve quick deployment through a purpose-built appliance, software, or hosted as a service.

Improved Data Understanding & Business Alignment

The key for FS organisations in achieving a data management capability that can assist them in successfully delivering against their business objectives is a greater understanding of their data and improved data alignment. Our data consultants and architects understand the financial sector and the data issues that FS organisations are facing. We have the knowledge and experience to bring together both the business and technology to build up a detailed picture of the data landscape giving FS organisations not only a better understanding of their data but also ensuring that their data is correctly aligned to their business requirements and strategy.

- Produce a fully validated up-to-date picture of the current data environment, mapped to both the business and the technology.
- Identify areas where “quick wins” can be easily achieved in order to reduce cost, mitigate risk and improve service levels.
- Produce a strategic roadmap for the data environment based on business objectives.
- Create a set of Guiding Principles that will ensure that future requirements and changes to the data environment will be in-line with corporate strategy.
- Identify areas identified where any capital outlay will have maximum effect as well as the ability to effectively structure the data budget over a period of time.
- Identify areas of wastage within the data environment that is costing money but delivering no discernible business benefit.

Because we understand the size of the data issues currently faced by FS organisations and the pressures that they bring to bear we have made our engagement process simple and flexible to ensure that any FS organisation we deal with gains the maximum business benefit from engaging with us, one example of a data engagement is outlined below:

1. Co-creation Workshop:

- Understand key data areas and remedial actions.
- Recommend initial steps towards solution.

2. Information Governance & Data Management Assessment:

- Identify readiness and maturity with regard to your data management.
- Understand the data and ensure correct alignment to your business and your requirements.
- Evaluate risk against unstructured and personal data.
- Provide business case inputs and remediation action plan.

3. Deploy the right solutions to meet your business objectives:

- Establish a technology solution to solve key data challenges.
- Give you greater control over your data by allowing you to Locate, Search, Minimise, Protect, Monitor and Move your data as your business requirement evolve.
- Provide you with a solid data platform allowing you to meet your data requirements and strategy.

Why FUJITSU and Veritas?

- Fujitsu has been a trusted provider to financial services firms for more than 40 years
- Fujitsu consultants and architects are specialists in their field, they understand your business and can talk your language when it comes to your data
- From compliance to open banking to quantum-inspired computing, Fujitsu brings expertise into key areas
- Fujitsu can provide an end-to-end solution from a trusted provider
- Fujitsu have been supporters of UK Finance and the Centre for the Study of Financial Innovation
- Veritas Technologies empowers businesses of all sizes to discover the truth about their data
- Veritas can help in accelerating digital transformation and solve pressing data and business challenges
- 86% of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage.

Contact:

For more information, please contact:

Mark McAlpine
Business Development Director –
Financial Services
mark.mcalpine@uk.fujitsu.com
+44 (0) 7867 837 759

Gordon Nother
Data Protection Specialist
gordon.nother@uk.fujitsu.com
+44 (0) 7867 832 170

Steve Smith
Principal Architect
steve.2.smith@uk.fujitsu.com
+44 (0)7867 821 624

© FUJITSU 2018. All rights reserved. FUJITSU and FUJITSU logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use. Fujitsu endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same. No part of this document may be reproduced, stored or transmitted in any form without prior written permission of Fujitsu Services Ltd. ID-4901/05.2018