DMH Stallard

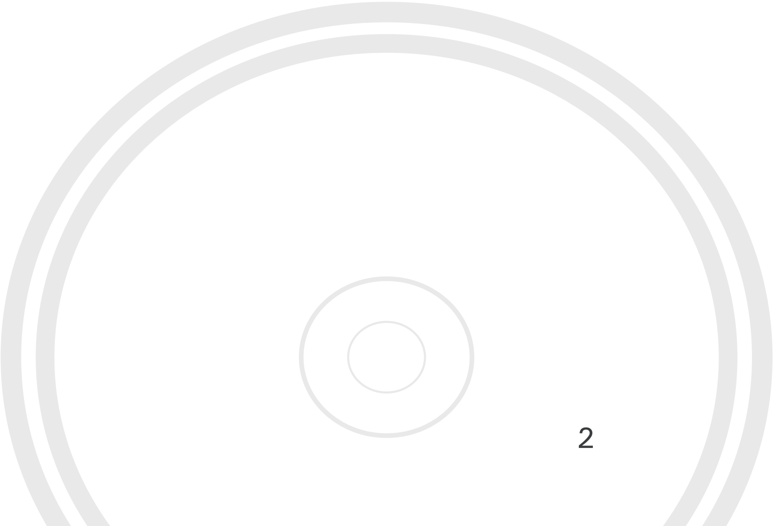
Secure Your Data – Protect Your Business

Practical solutions for the digital age of global communication and mass data exchange

A Report by DMH Stallard

June 2012

Contents



Introduction from Tim Aspinall
Managing Partner, DMH Stallard

At the start of 2011, DMH Stallard set out to deliver a series of detailed reports that would lead the debate across a number of critical business issues. With these reports our aim is to provide businesses with valuable insight into how they can protect their assets, reduce exposure to common risks and ultimately become more efficient and competitive.

Last year we published two reports, the first examined the value of intellectual property and the second tackled the topical issue of ensuring ethical practice and compliance. Both reports gained wide acclaim from the media and the wider business community.

I am delighted to introduce you to DMH Stallard's third report which explores how companies are coping in an increasingly data-driven digital age. As a successful and ambitious business ourselves we understand the ever increasing value of data. We wanted to know how other organisations are managing their data, how they store and transport it, and how they keep it secure.

As with our previous reports, we have undertaken several months of detailed research through face-to-face interviews with leading organisations. Our intention in this report is to provide answers to the questions that need to be asked of those providing IT strategy and operational support to their business. Most importantly, the answers have come from best practice employed by the real businesses that we interviewed. We examined the strategic direction businesses wanted to take and attempted to find ways of mitigating the risks of such alternative strategies.

I would like to take this opportunity to thank all the companies that we interviewed for their time and commitment to sharing their ideas and practices with us, with special thanks to Blackfoot for their close involvement with the project. They have all provided practical solutions for data security in the digital age of global communication that can add value to any business.

Tim Aspinall
Managing Partner, DMH Stallard

About Tim Aspinall
Tim is Managing Partner of DMH Stallard and is recognised as one of the country's leading lawyers. Tim works closely with many of the firm's larger clients and is responsible for developing long standing strategic relationships that help benefit both the client and DMH Stallard.

E. tim.aspinall@dmhstallard.com

Executive Summary

This report is not a technical guide for practitioners, rather it is a guide for CEOs and COOs who need to understand the important data security issues. It is to inform them of the risks that their organisation may be exposed to and what practical solutions they may employ to mitigate them. CIOs may also find this report useful as it is likely to endorse their approach to keeping data secure.

Data is of enormous value to a business and leakages can lead to a loss of reputation, fines by regulatory bodies and ultimately risk to the business as a whole if competitors can use the data to their advantage in the market.

There is no doubt that today's businesses are in the middle of a digital data explosion. This massive growth in data is coupled with changing expectations of how people can use this data to their advantage. This causes difficulties in keeping it secure, allowing the right people to access it and preventing the wrong people gaining access.

It is obvious from the interviews that some businesses are coping better than others. Also, it is clear that the old ways of managing and storing data are creating problems. In fact, many are counterproductive and increase business risk. There is also evidence of a clear cultural divide between those trying to use IT to improve the competitive advantage of the business and those trying to control how data and IT are delivered.

Interviewees also indicated to us how they are coping with the rapid rise in cloud computing, both as a medium for storing data and as a service to their business. All businesses are aware of the risks that the cloud can present in storing data securely.

This report guides Chief Officers in how to adopt best practice in data management and storage as we rush further and faster into a data rich, digital age. We also provide some background guidance on legal issues without making this a legal report and we conclude with our top data security tips.

The Data Explosion

Is this the next industrial revolution?

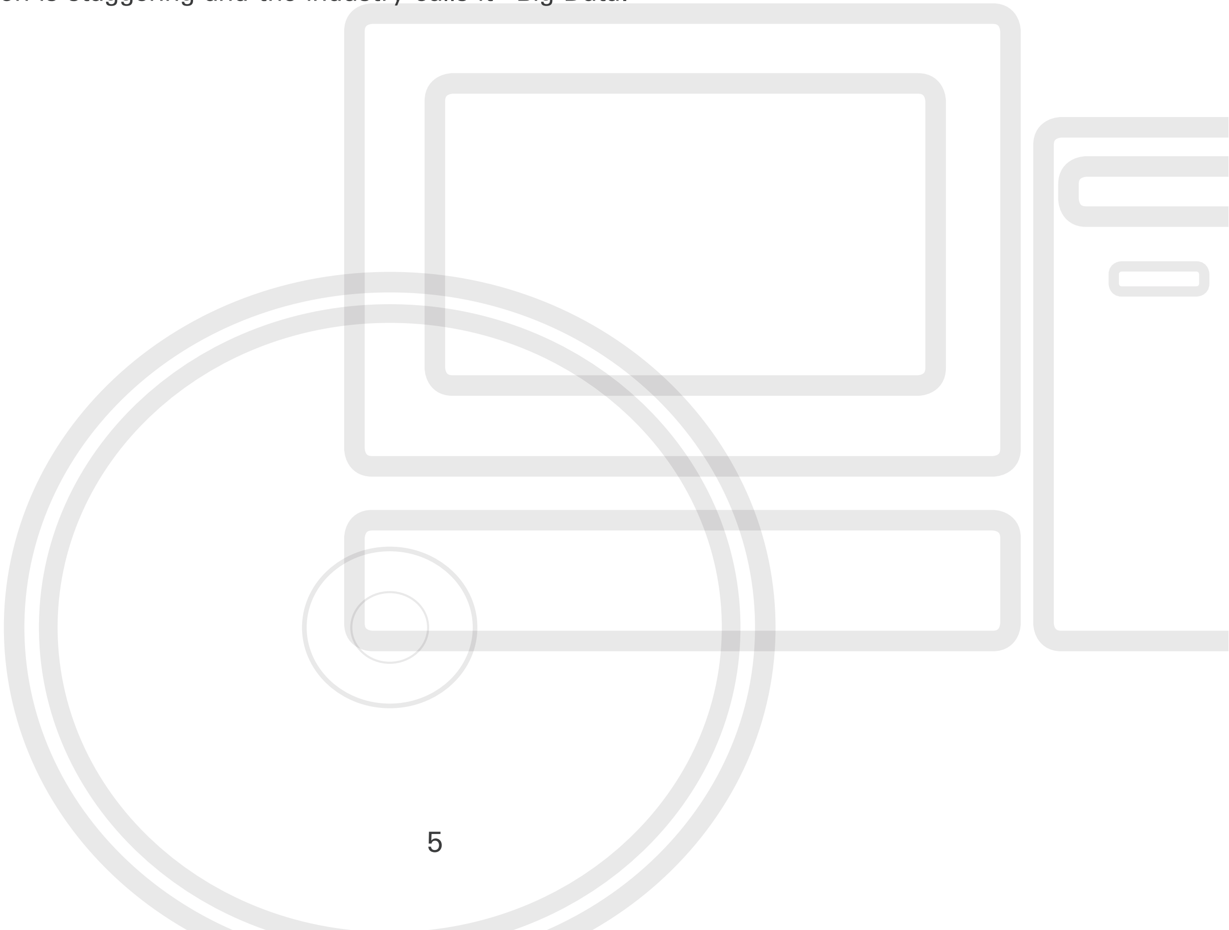
In the past five years more data has been produced than ever produced before. We are now moving to a paperless world where we communicate electronically using portable devices with increasing capability.

The world is producing data at a growing rate with some saying data volumes are doubling every two years.

> *"In 2011 the world is estimated to have produced 1.8 zettabytes of data. This is equal to 57.5bn 32GB Apple iPads which would allow us to build the 13,000 mile Great Wall of China twice as high."*

IBM says we are producing 2.5 quintillion bytes of data per day. "There are expected to be one trillion new devices connected to the internet in the near future, which will help drive 44 times digital data growth by the year 2020, 80% of which will be unstructured content and will require great effort to analyse."

This data explosion is staggering and the industry calls it "Big Data."



What does this mean for your business?

This data explosion has caused major problems to the IT systems that have been used in the past. The size of files has increased many fold and, with data being easier to access and move around, the risk of the data getting into the wrong hands is increasing at a dramatic pace.

Along with this, there is growing dissatisfaction from owners and employees that their businesses are not taking advantage of improvements in IT and that IT is not actually enabling the business; it is, in fact, holding it back.

In this report we discuss the issues of the data explosion, ensuring data protection and security and whether the cloud offers some solutions. We interviewed a series of businesses in the engineering and technology industries. We also interviewed technology enablers and cloud service providers.

We found some companies struggling to deal with the problems of today and some had concerns about whether or how “cloud” adoption could solve their problems with increasing data volumes.

> *“There is growing dissatisfaction from owners and employees that they are not taking advantage of improvements in IT and that IT is not actually enabling the business; it is in fact, holding it back.”*

Several interviewees said this digital data explosion coupled with cloud computing could be a new industrial revolution.

It was interesting to find that companies seemed to be more willing to talk about a sensitive subject such as “ethical business”, covered in a previous report, than they were to talk about how they kept theirs and others’ data secure and safe.

In this report we present both the good practices and the opportunities for improvement we found from the businesses we met.

What are the Risks?

The data explosion gives rise to many risks, but in this report we focus on the ones below.

Data overload

With so much data available, businesses can find that they are keeping data which is out of date or which is duplicated. In our interviews, we identified that businesses with fragmented or de-centralised data storage face data security issues and greater risks in determining what is the most recent copy of data and who has control over it. Other businesses have responded to this overload by centralising their data, configuring their systems to allow for proper version controls and providing sophisticated filter or search mechanisms for locating and accessing data. Keeping all data centrally can add to the risks of security and we examine this later.

Data leakage

Businesses face an ever-growing list of risks from data “leakage” or unauthorised access by third parties. This includes the scenario where the security around the data system is inadequate. For example, in 2011 Sony’s PlayStation Network, home to 70 million users, was hacked and user information (including credit card data) stolen. Most interviewees indicated that they believe their security is adequate. Some identified that they had spent a lot of time and effort in ensuring their systems are secure both on-premise and in the cloud. However, the average business is unlikely to be able to withstand a targeted attack by determined hackers. We examine cloud issues later.

Access by governments and competitors

Governments can get access to business data through legal action – see “External Influencers” later. Also, governments can get access through espionage. For example, significant data leakage occurred in 2009 concerning the F-35 Joint Strike Fighter programme with allegations that systems had been hacked by the Chinese authorities. It appears that the hack was aimed at another programme, not the F-35, but once intruders had breached security they “became invisible witnesses to online meetings and technical discussions.” Once the breach was discovered, the classified programme was halted while a new and costly security system was put in place.

Not every UK business is involved in projects with national security implications. However, all businesses should be wary of using smartphones or webmail in certain jurisdictions because part of the data traffic will be handled by the local telecoms operator, which may be susceptible to interception by foreign agencies. One interviewee said that, when they travel abroad they swap the SIM card from their smartphone to a more basic handset so there is no opportunity to accidentally send or receive data. Businesses should also be aware of commercial espionage by their competitors.

Careless use of social media

In a short space of time, the use of social media has become pervasive. Most interviewees have policies governing the use of social media by their employees. Some have embraced social media and use it as an official means of engaging with their customers.

It is crucial that businesses are aware of how their people use social media to reduce the risks of data security issues. At one end, people can leak sensitive data inadvertently by using the seemingly innocuous "Check In" facility to show where they are. If done at a customer's premises this could be a breach of confidentiality. At the other end, people can deliberately use social media to transfer information quickly and simply to a multitude of recipients, with the data then stored in an open cloud. We discuss the data security risks caused by people later.

Fines for data breaches

There is widespread awareness of the requirements under data protection legislation. Also, there is growing awareness of the possibility of a business being fined for data protection breaches. However, there appears to be the sense that the current level of fines is affordable to large businesses, with a current maximum fine of £500,000 although the actual fine is likely to be much lower than this.

> *"There appears to be the sense that the current level of fines is affordable to large businesses. But, if data breaches are affordable now, that will not be the case when the new law comes into force."*

Future developments in the UK

We anticipate that data security will become a much more pressing issue for all Chief Officers:

- Although businesses are rightly wary of moving their data off premise, cloud offers opportunities too good to ignore - we analyse this in more detail below.

- The Financial Services Authority is being replaced by two new bodies, the Prudential Regulation Authority and the Financial Conduct Authority. These new bodies will approach regulation with new vigour and will be looking to stamp their authority early by making an example of bad practice.

- The proposed new EU Data Protection Regulation, if passed in its current format, would see fines of up to 2% of turnover for the most flagrant breaches, although this might not be in force until 2016.

- The Information Commissioner has recently repeated his calls for the introduction of longer jail terms to act as a strong deterrent against data protection breaches.

Managing Access is Key

Restricted access and user rights

The key to managing data successfully is to ensure that the right people access the right data safely and securely. Employees only need to see the data that they “need to know”. This means segregating and controlling data and regularly reviewing the need and procedures to access that data.

There is considerable evidence that some companies ignore this and allow staff unrestricted access to vast amounts of data. This exposes businesses to disenchanted staff using data for malicious purposes. For example disgruntled US military personnel fed Wikileaks with highly confidential and potentially embarrassing information which affected national security.

Practical solutions

Employees do not need “blanket” access to data, rather they should be able to access data they need at an appropriate level. All data should be segregated according to importance.

Data can be categorised as:

- High risk, that is data having high financial or commercial impact or something affecting national security
- Medium risk
- General email and information of low risk

A forward-thinking company we interviewed segregated its data with different levels of security according to the consequences of the risk of losing the data.

Their “crown jewels” as they called it, including credit card, payment and customer data is kept in an ultra secure data centre in London. There is restricted access and security barriers to entry. Moreover, need for access is reviewed regularly and those either not needing access or who have not been using the privilege have their rights to access removed and must re-apply.

The company uses a “public cloud” for data of low value and utilises a SaaS (Software as a Service) in the cloud service for staff email.

Categorising and segmenting data enables employees to access discrete “packets” of data rather than complete databases. The important issue is that data is only accessed in minimal amounts to reduce risk and there is no need to store it on the hard drives of PCs. This is cheaper, more secure and easier to police than having data disaggregated amongst the workforce on laptops. Clearly, the ability to restrict access to data may be limited by the choice of software and a business should re-evaluate software functions at the same time as deciding on data access options.

Addressing issues

The straightforward view of one interviewee is that customers want to see their data storage like a piece of cheddar cheese, smooth, polished and impenetrable but what most actually have is Swiss cheese - full of holes.

The interviewee thought that companies try a never-ending sequence of iterations to plug the holes but should restart with a new approach, which is fundamental to developing a strategic approach to data security. It is advisable that businesses conduct regular reviews of how they manage data security and view the subject as a strategic task rather than an iterative tactical one.

What not to do

The method of security for many businesses is to have complex passwords sometimes up to sixteen digits long, often replaced monthly, to provide some sort of access security. We heard of one company where the IT department recommended all staff put a post-it note of their password on the PC monitor as an aide memoire.

Another company’s IT manager controlled users’ passwords in a non-encrypted Word file on his laptop. Another sub-contracted its IT support to a local IT firm but had no idea who in that firm was looking at their data and had not made sure that those involved had signed the appropriate non-disclosure agreements or had adequate security clearances.

This methodology is clearly ineffective. Another sometimes counter-productive view is that of treating data access as a physical security problem and not dealing with the cyber risk. We encountered IT security officers relying on barbed wire fences and restricted access, not realising that this would not deter data hacking.

This exemplified itself in one business we heard of which physically glued over 22,000 USB sockets to prevent them being used to move data. This is clearly ridiculous as the data could easily be moved using email or the internet.

Controlling Your Data

"The data kept at the centre is always up to date and everyone working from it is working in 'real time'."

One of the important issues that needs to be raised in dealing with data is controlling the size of data packages or files involved. This works alongside the data segregation mentioned earlier.

Keeping file size small helps improve transfer speeds and also reduces the amount of storage space required for back-up, therefore streamlining activities.

Some engineering businesses reduce the size of complex Computer Aided Design models - which are data heavy - to smaller "attribute" files which register the key design factors and geometry. In some respects this is similar to how an mp3 file takes the music data and compresses it.

Keep it central

The best practice is to encrypt and store data centrally where partners and contractors can access it quickly and securely.

Any investment in dedicated systems that can handle configuration control in the digital environment is usually cost effective as it can reduce the risk of concurrent working on the same product which produces confusion and wasted effort.

Collecting data

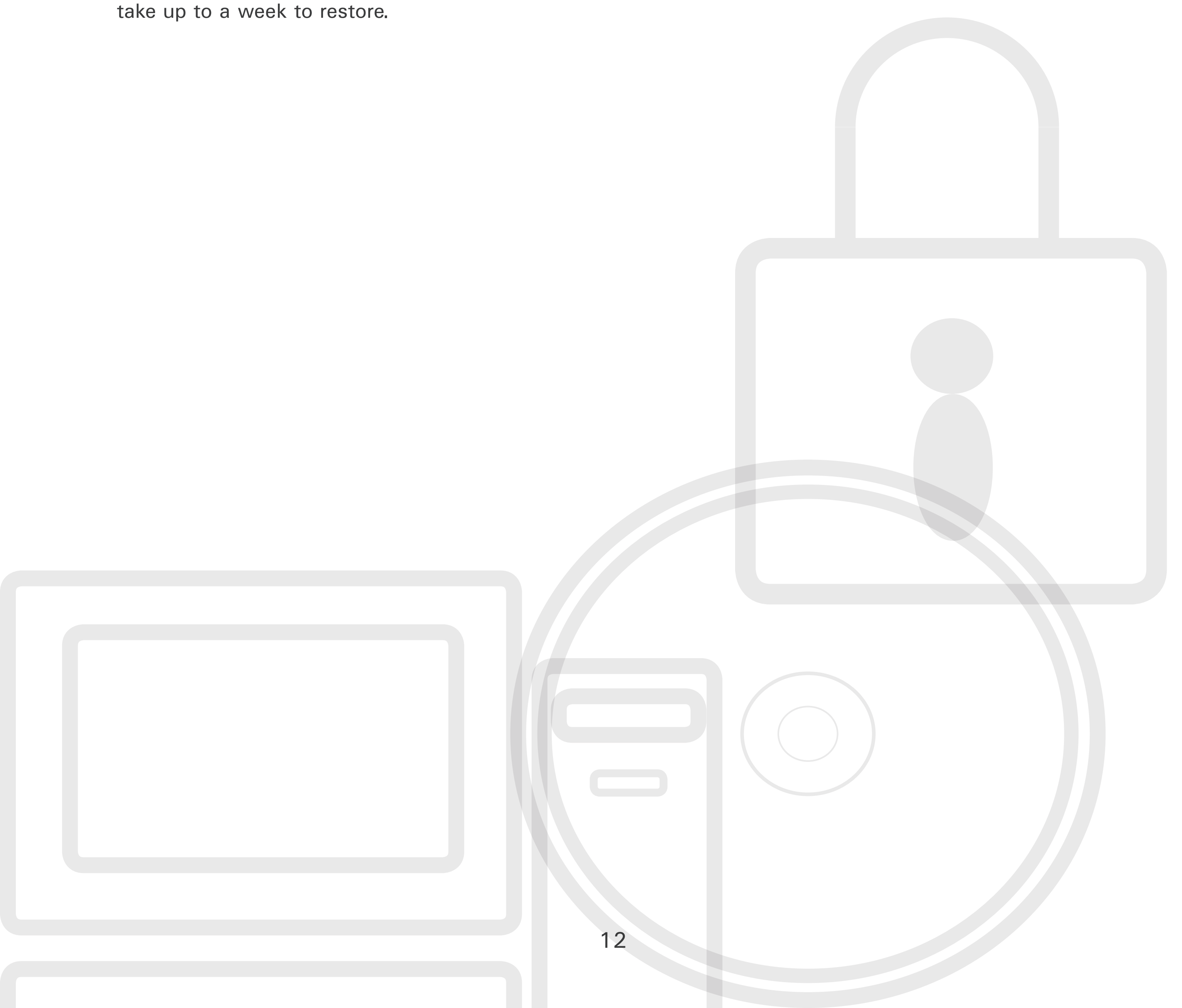
Many businesses collect data in a haphazard way, sometimes collecting data that they do not need or sometimes keeping it in case they may need it at sometime in the future. It is important to regularly audit and review what data is kept and remove data, particularly to protect the organisation from some of the regulatory pitfalls that can arise.

Storing data that is not required adds cost with the need for extra storage or servers. This takes up productive floor space that could otherwise be used by staff and adds to energy bills.

Keep back-ups

Backing up data is crucial for any business. In our discussions we found several instances of back-ups not being successfully undertaken, with businesses living under the false belief that they were. For example, a member of staff inadvertently caused a back-up tape to be corrupted while moving it offsite by placing it on the floor of a London Underground train thus exposing it to high magnetic fields from the live rail.

Backing up to the cloud can be an alternative, but is highly dependent on data volumes and connection speeds and may not be suitable for all businesses. Also, long term back-ups to a disk or cloud solution may work out more expensive than tape. One business had set its server to back-up remotely while it was idling only to find that, in fact, the server was starting to break down and was never idle. This meant that the back-up did not take place for a four month period when the server eventually crashed and the fault was discovered. Another business explained it had rejected cloud back-up as this would take up to a week to restore.



Bringing Your Own – is it cheaper?

In most organisations the traditional way of working is for the IT team to supply both PCs and smartphones, usually BlackBerrys, to employees to provide remote access to the company server for things such as email and data. This can tie up a lot of company cash in a rapidly depreciating asset.

We sensed within our discussions a growing recognition of "consumerisation" of IT - that employees wish to use their personal devices they are familiar with and enjoy using at work. Sometimes this is driven by the personal wishes of the CEO to use iPhones or iPads. This can lead to greater productivity and increased staff satisfaction.

Bring your own device

Some businesses encourage their staff by giving them a monthly allowance to facilitate their IT. It also frees up IT departments who are often busy fixing hardware that has not been looked after particularly well by their colleagues - our discussions indicated that employees were more likely to look after their own device with a higher degree of care than company equipment.

> *"Many companies are adopting BYOD policies or 'Bring your own device'. It can dramatically reduce the capital exposure and depreciation costs in the business. It also frees up IT departments who are often busy fixing hardware that has not been looked after particularly well by their colleagues."*

As personal devices often have small data storage capabilities the company is then moving toward the more central storage of data advocated above. This obviates the need and capability for vast amounts of data to be stored on the device's internal memory and thus reduces the risk of losing that data if the device is lost. Effectively the employee is working from data in a virtual environment.

A solution that enables BYOD to work securely is by using software that creates a "partition" in the device thus separating work from personal data. No information can pass across the partition and if the individual leaves, the organisation can remove or disable the software preventing access to company data and with the device reverting to normal.

Another similar way businesses are embracing BYOD is to provide employees with encrypted USB sticks with a remote access program pre-stored in them. This allows them to use any device to connect to the company network while effectively partitioning the device and creating a secure area for the employee to work from. When the stick is removed the device becomes as it was before. No data, viruses or malware can move from the secure area of the device into the other or vice versa. This is a cheap and effective way of enabling remote working.

However, some argue that although a business can save money up-front as the user will buy their own device, the hardware costs represent a small proportion of the overall cost, which is mostly comprised of support costs. Until recently, many businesses had a “Microsoft-only” policy - many still do - and they might not have the expertise in-house to support Apple or Android products. The business needs to identify to what extent it will support a personal device, particularly if each person has a different choice of device. It could ask the user to support their own device via warranty claims, but this may result in a dissatisfied user and could give a third party access to the business’ data.

There is a clear sense that BYOD is the future but businesses need to assess it fully first. Businesses must ensure that the savings they make on hardware costs are greater than any costs to their IT departments in supporting a plethora of devices. Also, they must ensure they have properly addressed access to data.

Marrying People and IT

We found during our discussions that data security was mostly compromised by the behaviour of people.

This was sometimes due to deliberate behaviours that were designed to harm the company, but in the majority of cases it was employees deploying "work around" solutions in an attempt to do their day-to-day work. This was usually exacerbated by the fact that the IT departments had clamped down so severely on the ways data could be accessed and transferred. By using the mandated channels and procedures it was nearly impossible to work effectively.

Examples included a business which followed a highly risk averse strategy, their server was based off premises and could only be accessed through a dedicated landline with bespoke encryption. There was no internet connection to the server. Not surprisingly staff simply copied data onto USB sticks and emailed data to personal email accounts to enable them to work remotely.

> *"The key to success is to create an enabling culture in the business that constantly checks and reviews how IT is utilised, brings issues out into the open, respects and manages risk appropriately and doesn't stop people doing what they need to do."*

Successful counselling

Obviously, the more sensible approach is not to ignore what is going on in the company but to deal with it.

Perhaps the approach to follow is that of one business that used a "survey of truth" to find out what staff were doing to move data around. This uncovered some of the approaches listed above. More importantly it determined what the needs of the business were to improve productivity.

The solution decided upon was to set up a dedicated process for moving data around or outside of the business. When staff want to use the service they have a series of questions to answer including "warning statements" before the data can be transferred. By doing this the employee is aware of the commercial consequences of moving the data and additionally they take personal responsibility for the data transfer. For security purposes, the process was set up so that permission expired after seven days and the data stored in the transfer area was deleted.

By doing this there is no need to develop work arounds and the employee takes personal responsibility for the fact that they are moving the data and that they are aware of the risks that they may be taking.

Another seemingly obvious but often forgotton step is to regularly review and revoke permissions for employees to access databases, websites or software packages. In addition, one should close down these access rights if a member of staff leaves and remember to refresh the password so that they can no longer obtain access.

Divided tensions

Many problems are often driven by strategic tensions in the business. In many organisations there is a conflict between, on the one hand providing security thereby protecting the business, and on the other hand improving productivity and exploiting technology.

Several interviewees were of the opinion that the role of the traditional IT Director or Chief Information Officer should be replaced by a Chief "Innovation" Officer. CEOs should be tasking the CIO with investigating and implementing solutions that ignore the barriers that are put in the way by conventional thinking.

We also were told of instances where, under independent audit, some IT staff had been discovered abusing IT systems in a way unbeknown to the management. One employee had been discovered using the server to run a dating site whilst another was using the server to store his movie library.

Businesses with an "enabling culture" must nevertheless remember to protect valuable data, in particular from exiting employees who may seek to take advantage of a careless approach in this area. Creating a culture of respect for confidential information, and having a reputation internally for the protection of data and enforcement of IT policies, will go a long way towards deterring staff from inappropriate behaviour.

Cloud – Is this the future?

Cloud computing means different things to different people. The Cloud Industry Forum has published some useful whitepapers which clarify the cloud. Many businesses are wary of the cloud and some have not addressed it. Others, including large companies, are already adopting cloud solutions.

What are the benefits?

- Reduced capital expenditure
- Regular, predictable operating expenditure
- Freeing up of precious physical space and reduction in power usage
- Flexible, scalable data storage and processing
- Central storage so all data is available from a single source
- Accessible anytime, anywhere
- Software applications can be kept updated simply and centrally

What should you be asking?

- How secure is the service?
- Do you still own the data?
- Where in the world is the data being stored and by whom? Does that jurisdiction comply with your regulatory or contractual requirements? For example, must you store data within the EU?
- Is your data portable and how can you move the data around if you need to switch providers?
- How do you access your data?
- Does the provider respect the privacy of your data and prevent it being shared?

Security

With the correct security procedures in place, security can be built into cloud solutions. In fact, security at a data centre is usually considerably greater than data "on premise" and thus the cloud can be safer and more practical, provided that connectivity is sufficient. "Security through obscurity" is not a valid justification for keeping data on your own servers. Data centres are designed to hold off cyber attacks and can be more secure than in-house servers.

"It is worth remembering security is at the core of data centres."

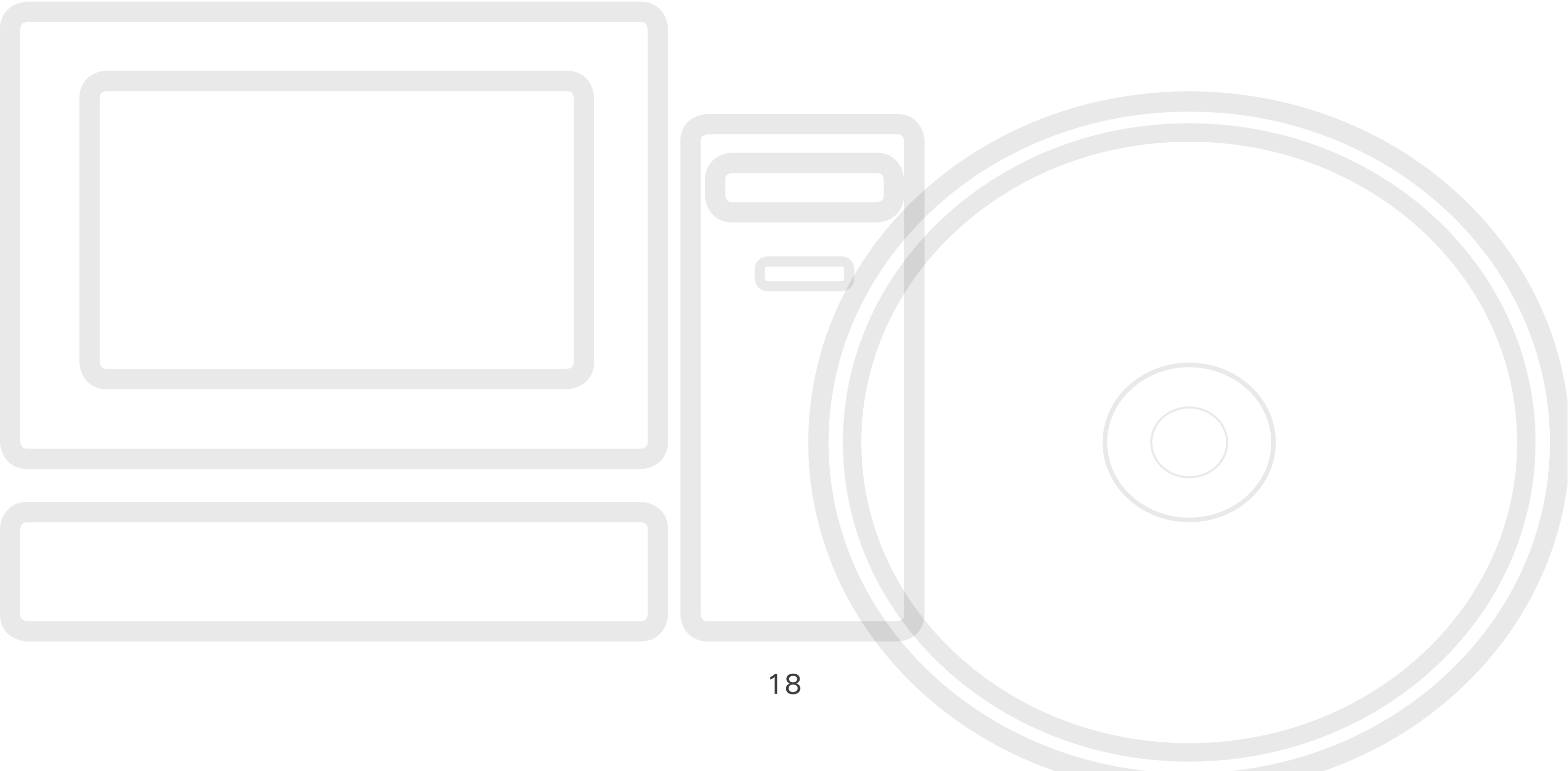
Many of us already trust valuable personal data to the cloud. Email accounts such as Yahoo! mail and Gmail contain a lot of our personal information. Many of us upload photos to Flickr and Facebook or use Dropbox, Google Docs or Evernote to store our documents. All of these are cloud applications and most of us have no idea where the data is stored, who is looking at it and what happens to it when we try to erase it. As consumers we readily accept the risks that come with these free services, but these risks are often unacceptable from a business perspective. It is worth researching if your employees are using these services to store business information.

Implementation

It is clear that cloud implementation needs a systematic approach. Some businesses are using public cloud for the less important data they hold but prefer to use a private or hybrid cloud for their most crucial data. This can mean the crucial data is stored on the business' own premises with the rest being stored externally.

If you are thinking of cloud, think of this:

- Cloud can be more secure than traditional IT, but you must factor in data security from the start
- Research the market and perform due diligence on your cloud service provider. Has your cloud service provider got any recognised accreditations?
- Assess whether to hold data on-premise or in the cloud. If in the cloud consider whether to encrypt or "tokenise" data
- Do not abandon key IT disciplines and do engage with your provider on security issues. Can they address your concerns? If not, walk away



Top Ten Tips

1. Strategy

Create and then regularly review IT and data strategies for your business. Ensure that they act as enablers for your business and help improve productivity.

Listen to your staff and survey their opinions. Try to understand how they use IT to perform their work. Aspire to use the most up-to-date and enabling software and hardware you can afford.

Help your people "do what they need to do."

2. IT leadership and team

Your IT team should be in the vanguard of making your business work effectively. If they are not, challenge them. Do not allow them to be the "anchor" dragging you back.

Seek second opinions and strategic advice regularly. Explore "Bring Your Own Device" to reduce capital expenditure, improve productivity and improve staff morale.

3. Data management and segregation

Ensure your data is easy to access for the right people. Use compressed or attribute files to keep the volume of data movement low. Keep data up-to-date and do not hoard data that you do not need.

Make sure that access to data is controlled rigorously on a need-to-know basis. Prevent staff storing data on hard drives and USB sticks or sending it to webmail accounts and home PCs.

4. Security

Do not be obsessed with physical security. Remember, data security is not the same as conventional security and that a different way of thinking is required.

- Understand what data you have
- What is its value?
- What do the bad guys want?
- What is the risk to the business if you lose it?

Think of security as a Formula 1 style braking system for your business. If the brakes work really well and are used effectively, you can go faster.

5. Back-up

Make sure data back-up is part of your disaster recovery plans. Regularly back-up your data using various means, tape, disk, cloud etc. Make sure the back-up has actually taken place and attempt restoration from that back-up regularly.

6. Audit

Regularly audit your IT system, including data security processes, to keep up-to-date with security measures. Perform "bottom up reviews" and resist piecemeal improvements.

Audit your team and your IT sub-contractors and identify who needs access to secure data and how often they use that access. Remove access rights from those who are not using the privilege.

7. Cloud storage

Remember, cloud is another resource available to businesses. Unless your IT team regularly implements data security updates, cloud might be more secure than your existing on-premise solution. But, before moving to cloud, evaluate what level of security your chosen cloud provider offers. Make sure that your connections to the cloud can cope if you intend to move large amounts of data back and forth.

8. Transferring data to the cloud

Do not forget, many cloud providers are based outside the UK/EU. Are you comfortable that the US government might access your data held by the cloud provider under the Patriot Act or that you could be contravening the International Traffic in Arms Regulations (ITAR) by moving data to an unsuitable location?

Ensure that you have the rights to remove the data and that it will be erased completely if you require it.

9. Avoid data protection fines

The new EU data protection regulation could mean fines of up to 2% of turnover for data security breaches. Evaluate your data security processes now and take action to ensure you are prepared.

10. External help

Do not be afraid of asking for external help. You may have capable people but an external review is always worthwhile. It may actually agree with your own team's recommendations which they have been making for some time.

A Word on External Influencers

Data protection laws

The Data Protection Act places obligations on business in relation to personal data. In particular, there are safeguards over the use of data, whether and when to obtain consent from individuals before processing their information, and restrictions on transferring data outside the EU. In our interviews we found that there is generally a clear understanding of the need to keep data secure although, from a business perspective, this is not confined to personal data but all important information held by the business.

The Information Commissioner's Office, the body responsible for overseeing data protection in the UK, has the ability to impose fines of up to £500,000 for data protection breaches. In June 2012, the ICO issued its largest fine, £325,000 against a public sector body, Brighton and Sussex University Hospitals NHS Trust, for failing to wipe personal data from computer hard drives. Recently, the ICO revealed that although the private sector accounted for more than a third of all data security breaches reported, they were fined less than 1% of the overall total. This suggests that either data breaches by the public sector are more severe, or the ICO has yet to catch up with big business since winning these powers in April 2010. Also, even though the Financial Services Authority has the power to issue greater fines - and has done so recently as evidenced by its £3m fine against HSBC in 2009 for data security failings - it has been criticised for its lack of regulatory oversight, particularly in the banking sector.

On top of this, the EU's attempt to harmonise data security via the 1995 Data Protection Directive has not been as successful as hoped, with different implementations of the same law across the different EU member states. The proposed new Data Protection Regulation will finally see the same (personal) data security law apply across all EU member states and will include measures to streamline red tape and cut costs but also, as we saw earlier, increase fines.

International Traffic in Arms Regulations (ITAR)

Data security is also affected by ITAR, which is the means by which the US government restricts the export of technical data in relation to defence articles and services. UK businesses working with US partners on military projects can get access to US data under an appropriate agreement and under a licence granted by the US government. This licence will generally contain restrictions on the further flow of that data. This is likely to mean that a UK business will need to implement measures to segregate data to prevent certain employees, consultants and business partners from accessing that data.

The USA Patriot Act

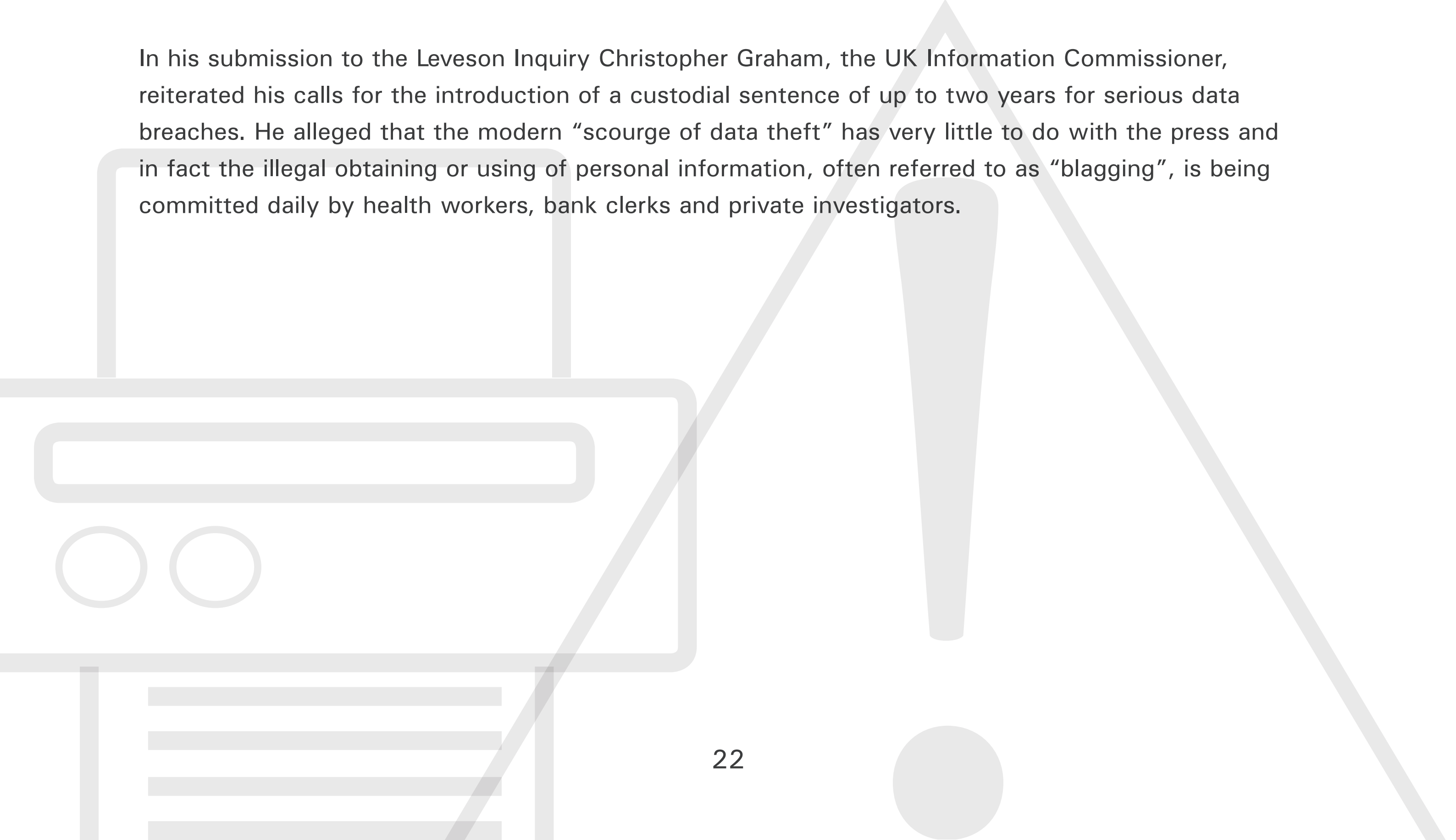
It is widely known that this Act is the means by which the FBI can get access to confidential data. In June 2011, Microsoft's UK MD confirmed that it would comply with the Patriot Act as its headquarters are based in the US. This means that if you do business with a UK subsidiary of a US-based cloud operator and you specify that English law applies and you choose a UK-based data centre operating under EU data protection laws, the FBI can still get access to your data.

The UK has its Anti-Terrorism, Crime and Security Act and the Regulation of Investigatory Powers Act. These give the UK government broad powers to intercept communications and gain access to data, including where it is protected by encryption or passwords and the government is likely to increase not decrease these powers. Also, the US and other governments can get access to UK-based data via treaties which the UK has signed up to. Ultimately, the best way to keep data completely secure may be to keep it in a bespoke on-premise solution. Having said that, not every business is likely to be investigated by the US or UK government for criminal or terrorist activities, so Patriot Act fears are probably a little exaggerated. However, there is a firm view that "nothing can prevent government espionage."

The Leveson Inquiry

Finally, garnering huge press coverage and public interest, due in part to the involvement of celebrities and politicians, the judge-led Leveson Inquiry was launched in 2011 in the wake of the News of the World's alleged "hacking" of the telephone of murdered schoolgirl Milly Dowler. Lord Justice Leveson is examining the practices and ethics of the British press and intends to publish his report later in 2012.

In his submission to the Leveson Inquiry Christopher Graham, the UK Information Commissioner, reiterated his calls for the introduction of a custodial sentence of up to two years for serious data breaches. He alleged that the modern "scourge of data theft" has very little to do with the press and in fact the illegal obtaining or using of personal information, often referred to as "blagging", is being committed daily by health workers, bank clerks and private investigators.



Acknowledgements

Our thanks go to those senior executives who gave their time so generously to contribute to this study, either through interviews or telephone conversations.

Blackfoot

www.blackfootuk.com

DMH Stallard would like to extend special thanks to Blackfoot for their close involvement with the project.

Blackfoot UK are security specialists dedicated to protecting their clients' reputations and profits through the provision of strategic and pragmatic information security and compliance advice. Blackfoot are committed to enhancing the customer's experience, whilst future-proofing businesses against the ever changing and dynamic data security landscape.

Asos plc

www.asosplc.com

ASOS is a global online fashion and beauty retailer and offers over 50,000 branded and own label product lines.

Closertag

www.closertag.com

Closertag's mission is to create clear, fluid and useful cross-channel experiences for mobile native apps, mobile web sites, mobile web apps, interactive TV and beyond.

Creation UK

www.creationteam.co.uk

Creation is one of the UK's leading independent vehicle design, development, engineering services and programme management specialists.

Mott MacDonald

www.mottmac.com

The Mott MacDonald Group is a diverse management, engineering and development consultancy delivering solutions for public and private clients world-wide.

Ospero

www.ospero.com

Ospero is a global infrastructure as a service company (IaaS) based in London with regional offices in North America and Asia Pacific, operating one of the largest single vendor data centre grids in the world.

Ramsac

www.ramsac.com

Ramsac makes IT simple through the provision of strategically led, professional, proactive, outsourced IT services. With an menu of options ranging from technical support to an outsourced IT director, ramsac deliver people focussed, business class solutions.

Voith Engineering Services

www.voithindustrialservices.de

Voith specialise in flight physics, system and structural engineering, life cycle management, cabin and cargo layout as well as maintenance, repair and overhaul.

About the Authors

David Seall C.Eng FRAeS MiMMM
DMH Stallard, Strategic Adviser, Manufacturing

David Seall is a leading authority on the UK manufacturing sector and is DMH Stallard's Strategic Advisor, Manufacturing. He was previously Chief Executive of the Engineering Employers Federation for London and the South East (EEF South) for over 10 years, working with hundreds of companies. Prior to this he enjoyed a successful career in the aerospace and defence industry.

David is an expert in strategic management and business planning and is an exponent of Lean Manufacturing and Lean Enterprise. He is an adviser to national, regional and local government on manufacturing, business support, skills development, science and technology and innovation. He is a Chartered Engineer and Fellow of the Royal Aeronautical Society.

E. david@davidseall.co.uk

Frank Jennings
DMH Stallard, Partner and Head of Commercial

Frank Jennings is a lawyer specialising in cloud & technology, data security, intellectual property and commercial contracts. His clients come to him not just for his specialist legal advice but also rely upon him for his "can-do" mentality and his pragmatic approach to solving problems and managing risk.

Frank chairs the Cloud Industry Forum's code governance board, blogs at TomiLaw.com and regularly presents on cloud and data security issues. Independent legal directory Legal 500 says he is "commercially minded" and a "clear thinker" and rates him #1 for Technology & IP.

E. frank.jennings@dmhstallard.com

DMH Stallard

About Our Reports

At DMH Stallard, we take pride in our commitment to our clients and building long term relationships with them. That is why we commissioned our Strategic Advisor for Manufacturing, David Seall, formerly CEO of Engineering Employers Federation South, to work with us on a series of reports aimed at helping those in the manufacturing and technology sectors.

Our first report, “Plan, Protect and Prosper, How Manufacturers Leverage IP to Create Value and Safeguard their Futures”, was published in May 2011. The report was based on interviews with directors of major UK manufacturing businesses operating globally – and examines how best to protect high value design and process innovations and how to overcome potential pitfalls.

The report has become an essential touch-point for all manufacturing businesses, particularly in light of the Hargeaves Report’s recommendations.

We published “Ethics and Compliance, How Manufacturers are Embracing the Challenge and Reducing their Risk”, in November 2011 and provided an insight into the critical issues businesses are facing in this area.

For copies of either report, please email scott.garner@dmhstallard.com

If you would like further information or would like to share your views on any of the issues raised in our reports, please email david@davidseall.co.uk

About DMH Stallard

We are proud to work with some of the most innovative and successful organisations in the country, including major financial institutions, FTSE listed companies, private equity backed businesses and high profile public sector bodies. We are also delighted that the firm continues to be recognised with industry awards and in 2012 was awarded the Corporate Law Firm of the Year at the prestigious Insider Dealmakers Awards.

We are dedicated to making our clients the centre of our business. We want to develop long-term relationships with our clients and invest considerable time and resource to support this. The feedback to this approach is always extremely positive and new clients have commented that our commitment to building the relationship and making it successful is refreshing.

We provide integrated teams from our offices in London and Gatwick, that are capable of working on large complex projects which require expertise from multiple disciplines. This approach ensures our clients have access to technically excellent advice across the board that is efficient, economical and aligned to their needs.

We continue to recruit some of the best talent in the City, and our approach continues to attract clients looking for a genuine alternative to traditional City law firms.

www.dmhstallard.com

Our Offices

London
6 New Street Square
New Fetter Lane
London
EC4A 3BF
Tel: 020 7822 1500

Gatwick
Gainsborough House
Pegler Way
Crawley
West Sussex RH11 7FZ
Tel: 01293 605000

DMH Stallard LLP is a limited liability partnership registered in England (registered number OC338287). Its registered office is Gainsborough House, Pegler Way, Crawley RH11 7FZ and it is authorised and regulated by the Solicitors Regulation Authority. The term partner is used to refer to a member of DMH Stallard LLP. A list of members may be inspected at the registered office. The firm is represented around the world through its international network. The materials appearing in this publication do not constitute legal advice and are provided for general information purposes only. No warranty, whether express or implied is given in relation to such materials.