

Data architectures and security issues

By Clive Longbottom, Service Director, Quocirca Ltd

The last article covered how organisations are faced with a complex, intertwined and often changing set of laws, rules and regulations that often pull against each other. The biggest problem for many organisations is in layering the needs of one set of regulations against the needs of another - without breaking the previous one. At a legal level, it is hard enough, yet solving the legal issues may have massive benefits to the organisation when it comes to the facilitation of business processes, as well as securing intellectual property assets across and beyond the organisation.

However, existing standard approaches to information security tend to mitigate against a real solution to ensuring that the intellectual property of the organisation is fully secured - and this can have far reaching implications.

For example, many applications depend on application-level security. The problem here is that once someone is in the application, they have full access to the overall application and its data itself - there are no more checks on what is happening from there onwards. Other applications may have a level of granularity within the application, using roles and responsibilities, while others may go as far as database level information security.

However, each one of these is essentially a walled garden approach - once a person has entered within the wall, they can roam freely. Indeed, outside of the more formal applications, the security of more ad-hoc information is often overlooked. For example, how secure are any documents being held on a user's C: drive - or even on a shared drive? How about when such information is on the move, whether via email or via portable storage? How about when secure data is aggregated in a formal and agreed manner through a business intelligence tool and turned into a report - is that report then stored and moved in the clear?

We also have to look at how the wall to this garden is crumbling around us. Software as a

service (SaaS), cloud computing and composite applications are increasingly creeping in to the architectural mix, and this has led to breaches in the wall with data moving backwards and forwards in manners where traditional information security approaches struggle to be workable.

Even for organisations that see themselves as still removed from the emerging architectures of SaaS, Cloud and so on, the use of mobile devices such as laptops, mobile phones and other access points means that the overall security of data has to be considered - both from a legal and an internal governance point of view.

It is clear that ensuring that information is always within compliance is not just a matter of simple application level security, nor of just layering on encryption for data at rest or even on the move. Something has to be done that goes back to the very basics of what is truly needed, and that creates an environment where information is inherently secure, where changes to the various forms of governance, risk management and compliance (GRC) load does not mean having to start all over again.

This means that we have to look at divorcing ourselves from the basic proposition of computing that has supported the business over the past 50 years or so - the application. As we move to a more open world, particularly as we share information up and down the organisational value chains and also use external functionality to bolster what is available within the data centre, the focus has got to become the underlying data itself.

Each item of data will have a nominal value to the organisation - from essentially nothing (e.g. an email asking someone if they are going out for a drink later), through important (e.g. details of a customer, including house details) to critical (e.g. the latest documentation and discussions around that patent that is in the process of being filed). This is made more complex in that it may be aggregation of different informational assets

that create that value - for instance, the figure 76.52 may have little meaning on its own, but when combined with "Brent Crude" and "November futures" suddenly takes on a lot more meaning if you happen to be a futures trader.

The data will probably be held in silos at the moment, it may well be a mix of formal data and ad-hoc information held across multiple data bases and storage units. Work will have to be done to sort out the existing environment- but it really should pay for itself, not only at a GRC level, but also in bolstering the efficiencies and effectiveness of the business itself.

But, if we can no longer use an application model as the centre of our GRC universe, where do we go? Again, we need to go back to the very roots of technology, and what it is meant to be there for - to facilitate the business. Business run by processes and tasks - not on applications. Processes change on a regular basis, and applications struggle to reflect this. Processes are dependent on information being moved between entities - whether this entity is a person or an up- or downstream automated part of the process.

The application becomes essentially immaterial - the business process becomes king. The organisation has to sit down and codify its processes as clearly as it possibly can. The touch points between the process and data become important - if a touch point is not secured correctly, then an entity has the opportunity to access data or information that it is not meant to - and the risk is run of opening the organisation up to legal and other GRC issues.

Therefore, the key need for an organisation before implementing a compliance oriented architecture (COA) is to sit down and identify its processes. In itself, this can be an illuminating exercise. Many processes are in place because "it is the way we have always done it". Uncovering the real needs can lead to far more efficient and effective processes, which on its own may well provide the organisation with a competitive edge. The path towards a COA should not be seen as a cost, which is where existing security solutions have historically sat. A COA is a business investment, it opens up new opportunities and provides far greater overall capabilities.

The next article in this mini-series will look at how the various aspects of a COA come together, how an organisation can start to move towards implementing one, and will cover the architectural aspects that will create an environment where information is under far greater control - so making it easier to demonstrate compliance, being able to open up the organisation for greater collaboration along value chains, and in gaining the most out of the data and information assets within the organisation.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at
<http://www.quocirca.com>