

The actuality of a compliance oriented architecture

By Clive Longbottom, Service Director, Quocirca Ltd

In earlier articles, we have looked at how the data is the most important part of any environment, and how a compliance oriented architecture (COA) can help in maintaining information security, as well as how it can enable true audit and governance compliance.

This final article will look at how the various parts of a COA come together, and the sort of tools that an organisation will need to have in place to ensure that a COA works for its needs. Initially, a means of adequate identification of the user is needed. "Challenge and response" systems, based on username and password, are not sufficient these days, and some form of two-factor authentication is recommended. Whether this is in the form of a one-time token, such as provided by the likes of RSA with SecurID or CRYPTOCARD's offerings, or a biometric device such as Authentec's fingerprint readers, LG's iris recognition technology or VSS's Voice Protect voice recognition system, you need to have a means of creating a trusted link between the system and a validated individual.

The next area is understanding the context of where the individual is. Here, understanding whether a person is sitting at a desk within an organisation or is sat in a public café begins to dictate the sort of information that the person should have access to at that point. Further, knowledge of the kind of device they are using will also dictate the kind of information that they will be capable of fully accessing on a sensible level. Increasingly, systems management software from the likes of IBM, CA, BMC and Symantec is capable of picking up this information, and making it available to other systems.

Such contextual knowledge needs to be pulled together in one place, and this will generally be a directory service, such as Microsoft's ActiveDirectory or IBM's Tivoli Directory Server. The use of a configuration management database (CMDB), which is provided with the majority of systems management tools, will enable information from multiple sources to be

pulled together and validated rapidly, also allowing for pattern recognition engines, such as Cisco's and SOURCEfire's intrusion prevention systems (IPS) to rapidly identify patterns of traffic and end user behaviour that are not normal and could therefore be a threat. It is important that information is, in itself, secure. Wherever possible, all data should be centrally stored, with a minimum amount being allowed to be stored locally. It should be the case that all information at rest is encrypted, using technology such as WinMagic's SecureDoc or TrueCrypt, which provide full-disk encryption.

Information on the move should also be encrypted, using technology such as provided by AEP Networks or PGP. The key, though, is to keep it as simple for the user as possible - no screens giving options of "what form of encryption do you want - AES, 3DES, Blowfish or Other?" Data being transferred between one storage medium and another, for example for snapshots, backup/restore or mirroring needs, must also be encrypted, and tape-based systems should use encryption such as seen with LTO-4 tape systems.

Next, we need to look at ensuring that the user is enabled as much as possible to carry out their work, and this means that we have to secure against accidental information leakage. Here, data leak prevention (DLP) systems from the likes of Clearswift, Code Green networks and TrendMicro can ensure that certain types of document can have constraints on usage (such as emailing, forwarding, printing) applied on them, and some of these solutions use advanced content inspection technology to ensure that the content of specific documents does not compromise an organisation's defined security.

Again, this tends to be predicated on the main data being stored centrally, such that access and usage keys can all be stored and managed centrally.

Users increasingly need to have access to centralised systems when they are on the road,

and here, the use of centralised systems must be considered. If it is possible to ensure that a user can only access data centrally, and doesn't carry it around with them, the chances of data being lost or misused are minimised. Virtualised desktops and thin client computing from the likes of Citrix, Microsoft and VMware are prime contenders here. However, many workers will need access to information while on the road, and may not have an "always on" connection capability. For these people, along with information encryption, there will also be a need for the use of digital rights management around the documents or data being stored. Here, vendors such as Adobe with its LiveCycle ES or ArtistScope offer means of ensuring that documents can only be read only by those who have the correct rights in place, but can also apply time limits on how long a document can be stored before the user has to touch the corporate network again, so ensuring that ex-employees and thieves have only a short period of time to try and break through all the security features before the information is destroyed.

Alongside this, standard security approaches such as the use of anti-virus, anti-spam and virtual private networks (VPNs) need to be applied as well.

Taken together, all of the above provide an overall security platform where a focus can now be applied on how the governance, compliance and audit (GCA) solution can be layered over the top, which will cover more than many of the governance, risk and compliance (GRC) "solutions" that are pushed in the market. Such security should ensure a greater level of knowledge of where information is and what events are occurring around it. A large portion of this will be based on the use of business reporting and business intelligence tools against the different storage systems in use. This will also require the capability to aggregate different data sets, often held in dispersed storage systems, and provide technical and management reports on the environment. Here, the likes of IBM with Cognos, Oracle with Hyperion and SAP with Business Objects all have technology that can be applied to meet the basic needs. However, when looking at legal compliance, it is necessary to ensure that only the information that a legal body has the right to look at is

supplied to them. Even at an internal level, it is important to ensure that if a top-level executive delegates some form of reporting to a junior person, that junior person cannot access certain data such as employee salaries, executive home details or whatever. Therefore, the reporting has to fit in with the security platform like a hand in a glove.

When running a report to show compliance with, for example, the German version of data protection compliance, it will be different to that for compliance to the UK-based DPA. Therefore, the overall solution must use the contextuality of the person accessing the system, the sort of data that is covered by the audit or compliance request, and the events that have been carried out on the data in question.

Storage is a core need across all of the above – even when we are looking at the security requirements. Storage virtualisation and storage management capabilities, from vendors such as EMC, Symantec, CA and IBM provide the necessary means to securely and effectively manage all the storage assets so as to provide a unified platform for the data residing on it.

The above may seem very complicated, but many of the solutions mentioned will have a degree of overlap with others. The main effort in putting together a COA is around the forethought - ensuring that the basic policies and procedures are in place before any technology is thrown at the problem. Only then can a Venn diagram be drawn up with the various vendor names in place along with what their technologies promise to deliver. By investigating the overlaps, many niche vendors can be removed from the equation, simplifying the overall mix of vendors in the final COA solution.

As deperimeterisation continues and the need to deal with external partners grows, the need for a COA also grows. The information contained in this mini-series of articles should enable an organisation to approach the issue with a greater deal of knowledge and understanding, and create an effective, efficient and flexible system that enables, rather than constrains, 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>