HAVE YOU COUNTED THE COST OF FUNCTIONAL CREEP IN YOUR DATA CENTRE?

A FRAME WHITE PAPER BY GREG GOODE

There was once a definitive line between a data centre's supporting facility infrastructure and the data centre's IT systems. Today, that line has become blurred, and is expected to disappear, due to facility infrastructure and IT systems converging, physically and logically. This convergence is recognised as 'functional creep'.

Allow me to use an analogy here to illustrate the issue. The ubiquitous mobile phone was originally developed for wireless telephony communication. Who would have thought that a mobile phone would also incorporate PDA functionality, a camera, MP3 player and gaming, not to mention internet connectivity? This is functional creep: mobile phones are no longer simple telephones. As a result, IT departments have had to create support groups to manage the mobile phone, especially the BlackBerry and its equivalents as they bring desktop functionality to users and all of the issues that come with it.

If ever there was an issue challenging data centre support groups, it's functional creep: the functionality that facility infrastructure elements have added to the data centre equation. This added functionality presents itself in the form of network connectivity, appliances, applications and operating systems. The elements require integration and, if an organisation is to reap any benefit, on-going operations support; and that comes at a cost.

The facility infrastructure elements I am referring to are power, cooling, equipment cabinets, data cabling, the computer room environmental management system (CREMS) and fire suppression. These elements underpin a data centre's IT systems, namely the mainframes, blade servers, data switches, storage area networks (SANs), and so on.

To date, the IT requirements of facility infrastructure have been either under-budgeted or not budgeted for at all. So, in many instances, the functionality and its benefits are never realised. In most scenarios, the project that implemented the facility infrastructure never planned for its use as organisations invariably never have a strategy or tactical plan to integrate facility infrastructure with IT needs.

Keep in mind that current facility infrastructure systems are adaptations of earlier systems, which never had IT solutions as part of the product. The original elements were isolated with their own electrical and mechanical controls. They did not depend upon any information technology and were managed by 'others'. IT operations relied upon rudimentary feedback to know whether the facility infrastructure was supplying power and cooling, and that its operating state was within normal limits.

So, why is non-IT related equipment becoming an essential part of the IT domain?

Email info@framegroup.com.au

The convergence of IT systems with what were once separate infrastructure products is being driven by the environmental demands of the IT systems. While a greater concentration of energy is needed in equipment cabinets, the required reaction times to a failure are reducing. So, the systems need to be smarter and supply real-time data to IT operations staff so they can quickly make and execute informed decisions to minimise interruptions to customers. The consequences of not taking corrective action are growing exponentially as more IT power is plugged into an equipment rack.

Vendors are building totally engineered solutions which can deliver the correct environmental needs to equipment enclosures and at the same time provide feedback, very quickly, to those who need to know if there is an abnormal condition in, say, the supply of power or cooling. Note that while the taxonomy of the latest products can be quite varied and complex, their primary objective (cooling, power management, etc.) has remained the same.

This engineered complexity comes at a cost as it requires organisations to add a level of network infrastructure not previously catered for.

To explain the functional creep let's take a look at some examples of these new facility infrastructure solutions.

The simple cabinet power distribution units (CPDUs) were originally nothing more than a means of distributing power in the equipment cabinet. There was a single input power circuit and multiple outlets to attach servers and other appliances. Today, they not only distribute a single power circuit to multiple devices but also provide a network interface with an inbuilt web browser, measure input current and other electrical parameters, and switch outlets to allow remote management of the attached devices.

The computer room air-conditioner (CRAC) has the primary role of providing cool air, generally via an underfloor plenum. It, too, has been engineered to integrate with a server and manage the unit so that its temperatures and airflow can be adjusted by direct feedback from temperature probes in equipment cabinets. The result is yet another facility infrastructure element requiring network connectivity.

Even more complex cooling solutions are entering the data centre. These use a coolant which is circulated to equipment cabinets to provide high-efficiency cooling to servers that produce anywhere up to 40 kW of heat in an enclosure. These cooling systems have numerous metrics that need to be monitored on the input and output-side of the cooling loop: airflows and temperatures into and out of the cabinet along with total system status. The result is that network monitoring has been integrated into the solution.

So, the humble equipment cabinet now comes with managed power, cooling, data cabling management systems and network connectivity solutions; it can even have its own uninterruptible power supply (UPS) system. Just add a local web browser and the IT operations group can monitor and manage numerous metrics within an equipment cabinet and across the entire data centre—temperature, power parameters, alarms—as well as interrogate history logging.

So, how has functional creep become an issue for IT personnel?

This engineered complexity comes at a cost as it requires organisations to add a level of network infrastructure not previously catered for. This includes the added cost of involving network groups to cater for additional virtual LANs, adding network security measures, and considering Wintel or Unix support, additional application support and additional facility infrastructure design. Then there is the hand-off to operations and the on-going operation costs. These engineered facility infrastructure solutions are adding a complexity to the data centre that is not widely understood.

As new centres are built, and these solutions are provisioned, organisations need to consider how they integrate these solutions within their existing enterprise

network. In many instances the facility project management teams who are building the new data centre, or upgrading it, are unaware of the requirements and the issues that must be addressed. Vendors are not knowledgeable of their client's network, or the policies governing it, so they can't ensure that the facility infrastructure functionality is integrated. The risk is that it all becomes too hard and is left for another day. The basic facility infrastructure is implemented with basic controls, but the wider network and its management capabilities are orphaned.

A number of issues are leading to these disconnects. The initial project budget invariably has no provision for the cost to integrate such increased functionality. This is because the requirements are never understood or articulated very well when initial planning is undertaken by either consulting services engineers, vendors, or even an organisation's own IT staff. The costs could be additional switch ports, added security policies, a firewall appliance, added cabling costs, and the cost of the vendor to configure the functionality. Add to this the cost of operationally managing the facility infrastructure once it is commissioned—a cost that not only includes training but may include engaging additional staff.

Anecdotal evidence suggests that existing IT support groups, who deal with more traditional IT—servers, storage, network—are reluctant to identify with the facility infrastructure which has converged into their space. Implementing, supporting and managing power, cooling, environmental management systems and cabling systems has never been a consideration and, as noted, not strategically or tactically planned for.

The vendors engineering these solutions—oblivious to clients' IT strategies and support arrangements—assume that the value-added functionality, which is merging their product into the client's network, is a simple matter of configuring an IP address and making the relevant connections. Nothing could be further from the truth. If the engineered solution has a server it obviously has a network connection, a specific hardware platform, an operating system, an application and maybe a database. These must conform to the strategy of the client's enterprise IT environment and the tactical support model. To be told it's not an issue will ensure it's never connected.

Such network complexity raises many risks with intrusion security, application and operating system patching, bug fixes and application licensing, to mention a few. These are standard IT issues that need to be addressed in order to comply with any enterprise network.

There is a major paradigm shift occurring in facility infrastructure development.

There are a number of facility infrastructure elements which have, over the past years, gone from what we might call 'dumb' stand-alone elements to quite complex engineered solutions, converging smart systems into the IT network space. Whether CPDU, CRAC, equipment cabinet, UPS or totally integrated and fully-engineered infrastructure solution incorporating many elements, the trend is the same: these solutions are becoming more common in the current data centres being built. They will also evolve even further as IT systems place ever greater demand on facility infrastructure to deliver smart power, cooling and environmental monitoring solutions, to name a few. Consequently, their complexity will increase as will their level of convergence.

There is a major paradigm shift occurring in facility infrastructure development. Organisations need to fully appreciate the functionality of these solutions and evolve strategies and policies to adopt such infrastructure into their IT domain. And it is essential that vendors have a complete understanding of their client's enterprise IP environment if their solution is to provide full functionality.

The consequence of either party not addressing these fundamental issues is that the emerging, engineered facility infrastructure will never deliver its benefits to data centre operations staff. Moreover, organisations will have made a capital investment that is either under utilised, or worst still, never used.

HAVE YOU COUNTED THE COST OF FUNCTIONAL CREEP IN YOUR DATA CENTRE?

About Greg Goode

Greg is a senior Data Centre Practice Manager with Frame. He has extensive industry knowledge and expertise in a diverse range of ICT environments, gained over 35 years in the business. His career spans mainframe environments, enterprise communication networks, major tenancy technology fit-outs, and server room and data centre builds. With the convergence of what were once disparate infrastructures, Greg's knowledge and skills bridge the technologies in a section of the industry which requires its own specialist expertise, that is, the enterprise data centre.

FRAME®

Sydney (Head Office)
Level 11, 189 Kent Street
GPO Box 4647
Sydney NSW 2001

Tel +61 (0) 2 9323 2800
Fax +61 (0) 2 9323 2828

Canberra
Unit 9, 25 Buckland Street
PO Box 224
Mitchell ACT 2911

Tel +61 (0) 2 6122 6800
Fax +61 (0) 2 6122 6868

Melbourne
Level 7, 31 Queen Street
Melbourne VIC 3000

Tel +61 (0) 3 9927 3800
Fax +61 (0) 3 9927 3838

Brisbane
Level 1, 21 Mein Street
Spring Hill QLD 4000
GPO Box 2502
Brisbane QLD 4001

Tel +61 (0) 7 3009 7800
Fax +61 (0) 7 3009 7878