Data centre monitoring and management

e book

www.ECDsolutions.com.au

ECD SOLUTIONS
ELECTRICAL+COMMS+DATA
www.ECDsolutions.com.au

WESTWICK-FARROW MEDIA

Whether it's the server under the stairs or the world's largest - the 2,200,000 square foot SwitchNAP facility in the Nevada desert - the data centre is the hub of any business. In many cases, it is the business itself.

Increasingly, data centre security, power consumption and environmental monitoring are considerations on the radar for administrators. Data centres are susceptible to hits from all angles: viruses, spyware, network threats and cyberattack, heat, humidity, airflow and smoke. In fact, it's pretty frightening how quickly and easily a company's IT operations can be taken down, which makes it hard to understand why some companies do not implement a solid strategy for dealing with IT threats.

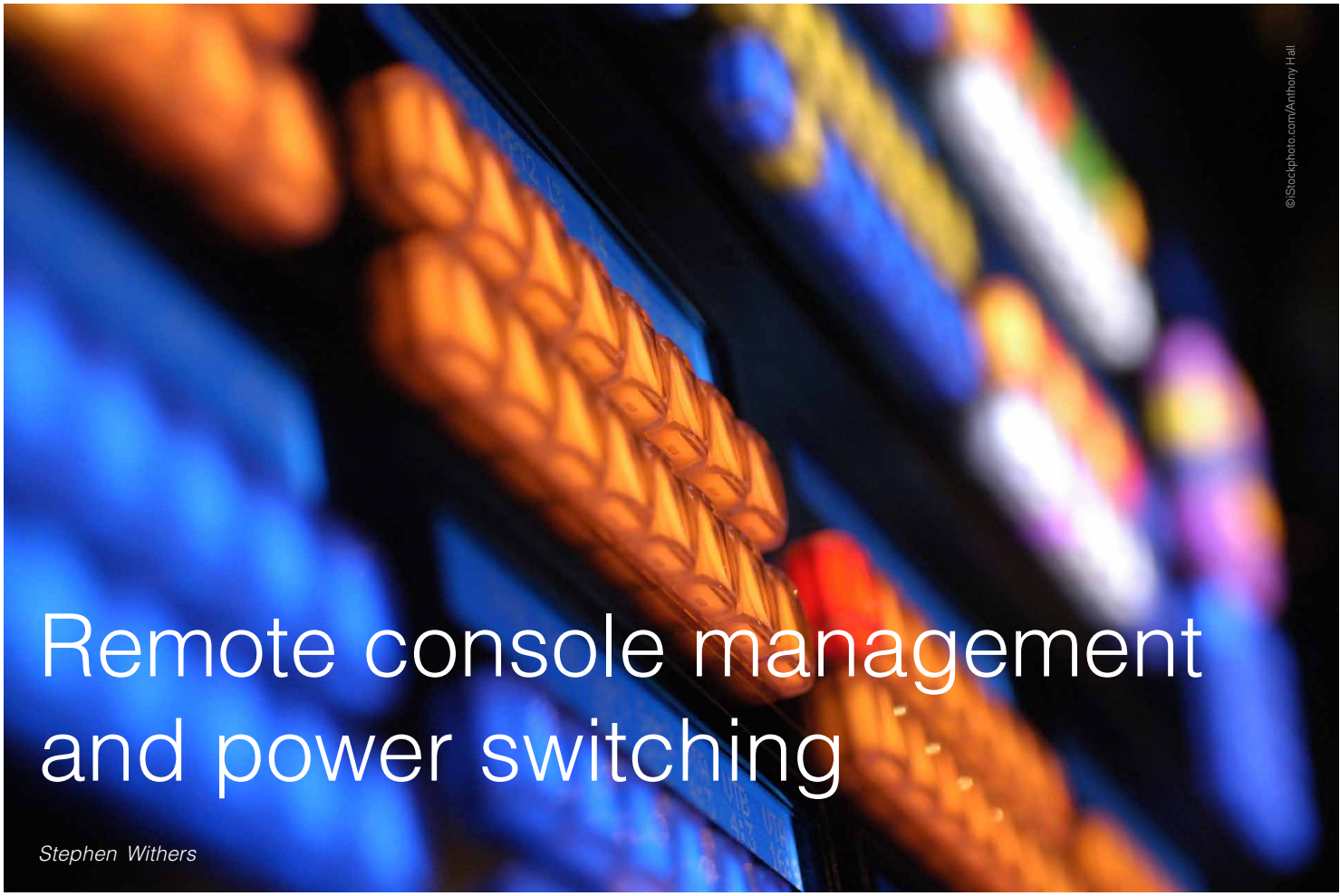
A combination of environmental and security monitoring, remote console management and remote power control gives administrators the power to control data centre environmental conditions and security, server and network equipment, and power distribution and usage. Automatic notification of environmental conditions or security breaches before the event disrupts network infrastructure can mean the difference between a minor inconvenience and a major crisis.

Couple rising power prices with the need to closely control the environment and data centres can easily be seen as the bad guy when it comes to the overall energy consumption of a business, but this needn't be the case. A bit of forethought in terms of design, a few behavioural changes and a system of monitoring and controlling power distribution can help keep energy use in check.

Today's data centre has an expected lifespan of just under 20 years, so making a few informed decisions and considered investment now can make all the difference a decade down the track.

Dannielle Furness
Editor – *ECD Solutions*

Contents



Remote console management and power switching

Stephen Withers

Once upon a time, almost all of an organisation's computing equipment would be in the same place as those responsible for keeping it running smoothly. Today's practices include locating significant pieces of equipment in branch offices where there may be no IT staff and taking space in third-party data centres (which makes physical access less convenient) instead of operating a private facility.

Fortunately, a number of technologies are available to overcome or at least minimise the negative effects of physical separation of systems administrators from the hardware they manage. Among them are remote console management and remote power switching.

Remote console management

A basic part of the picture is remote console management.

Many network or networked devices - servers, printers, routers, switches and others - include a web-based console allowing remote management and configuration. In addition, or alternatively, they may make provision for remote management via other network protocols such as SNMP, Telnet or SSH.

Apart from manual control using such protocols, there is a range of systems management tools from various vendors that allows device management from a centralised console, though not all such systems are able to manage all types of devices.

This approach is known as in-band management, because the management traffic flows across the same network as the rest of the data.

This is all very well as long as the network is running properly, but what happens when a device such as a switch or firewall is at least part of the problem and therefore network communications are interrupted? That's where out-of-band management comes into play.

Many devices are still fitted with a conventional serial port to allow the connection of a terminal (these days it's more likely to be a notebook running terminal emulation software rather than a dedicated terminal) for configuration or management. While it is possible to attach a modem to the serial port to allow remote management, that is rarely practical where multiple devices are concerned.

Enter the serial console server.

A serial console server connects to the serial ports of multiple devices and is in turn connected to a modem (for dial-in access) or via a completely separate IP network. This allows staff at other locations to 'dial in' (literally or metaphorically) to the console server and connect to the troublesome device. This means it is important that the console server has appropriate security features such as strong authentication (eg, via a RADIUS or Kerberos server) and logging - and, where dial-in modems are used, dial-back capability to ensure the call is coming from an authorised location.

If the console server is not accessible via the network (which is the main reason it would be accessed via the serial port), then the usual network security measures would not be available and so local authentication would be required. Other security measures include keystroke logging and automatic screen captures - such features do not reduce the risk of intrusion, but they do add to the audit trail.

Another issue is that the console server should be able to check that an attached modem is functioning correctly. If a simple re-initialisation fails to restore normal operation, rebooting via a remote power switch (see below) should do the trick. The server should also periodically check for a dial tone. Given that the modem is the alternative way into the console server in the event of a network failure, it is important to attend to any communications issues promptly and as far as possible automatically.

Console servers are not limited to out-of-band communications via serial interfaces. An alternative arrangement is to configure a completely separate IP network for communication between the console server and the central control point. Such a fallback network is much simpler than providing a secondary network path for every device, but if any components are shared with the main network it may not be possible to reach the console server in the event of an outage.

Remote reboot power switch

Sometimes a device is completely unresponsive, even on its serial port. In that situation all that is left is to cycle the power. How do you do that without gaining physical access to the device? Use a remote reboot power switch, also known as a network power switch. Such a device can be thought of as a remote-controlled power strip. Typically mounted in a rack along with the equipment it controls, the switch provides multiple independently controlled mains sockets that can be turned on or off via its network or serial interfaces. For maximum robustness, that serial interface can be connected to a serial console server along with the other devices.

Remote switches may provide additional functionality including automatic power-off if temperatures exceed a threshold or automatic power cycling if a network component becomes unresponsive (the latter being a particularly useful way of maintaining service levels, though the underlying cause of recurring failures should be investigated). These and other conditions such as power supply irregularities may also be reported via email or to a syslog or SNMP server.

More advanced models may include power metering at the aggregate or individual circuit level, as well as metering the actual input voltage.

Remote power switching can also be used to turn devices on or off when they are needed (possibly according to a schedule) to save power. In more complex environments they can also be used to balance power loads across the machine room.

Remote switching is not only for devices that run on mains power. Models are also available for remotely switching DC power, including 12, 24 and 48 V supplies. Such DC systems are said to reduce energy losses and therefore achieve greater efficiency, as well as being simpler and cheaper than AC power distribution systems.

Not all remote power switches are rack mounted: some models resemble an oversized power strip and are designed for vertical mounting within a cabinet and others are packaged in standalone cases to support a small number of devices that are not rack mounted (eg, a small branch office server or a kiosk in a shopping centre).

Both mains and DC remote switches may also provide automatic switching to a secondary power supply should the primary supply fail or become unstable. Combining automatic switching with remote switching in this way saves rack space.

Another way to save space - especially in smaller installations such as branch offices - is to select a device that combines the remote console server and remote power switching in one box.

As when choosing other pieces of network equipment, it is worth checking that a remote power switch supports IPv6 as well as IPv4, as the former is likely to come into common use within the lifespan of the device.

Conclusion

Remote console servers and remote power switches make it easier for IT operations staff to deliver improved service levels, especially where the equipment they manage is geographically dispersed or located at a third-party data centre with restricted access. Remote console servers make it easier to manage multiple devices with serial console interfaces and may provide a backup control path in the event of a network outage. Remote power switches allow power cycling without the need for physical access to the hardware.

These functions can be combined by connecting the remote power switches to a remote console server or by selecting a product that provides both capabilities from a single unit. ■

Energy use and data centres

Dannielle Furness, Editor, ECD Solutions

Just as the industrial revolution did before it, the information age has transformed our world and the way we operate within it. It's changed the way we access data and do business; the way we communicate, educate and consume information. It has given rise to entire industries and countless changes to employment and careers; jobs have been created and others rendered futile, often virtually overnight.

Communication methods and the equipment we relied on 20 years ago, such as faxes and dial-up modems, now seem as quaint as the quill and inkwell. The advent of mobile computing, the prevalence of smartphones and a move to cloud computing in more recent times have multiplied the effect and we now take for granted that digital files are permanent and can be retrieved at any time, from any location, in a matter of seconds.

For data centre owners and operators, the challenge is to cope with the constantly changing face of the industry. Not only must they factor in the impact of continual shifts in customer expectation and practices to adequately manage the mounting power consumption from this demand, but also 'crystal ball' into the future to ensure the projected life expectancy of the data centre (just under 20 years) is delivered and it meets commercial targets.

There are three principle considerations for the development and ongoing operations of a data centre, the nebulous nature of which make future-looking decisions all the more difficult.

Space

While the evolution of technology continues to shrink the physical size of hardware and we live in the era of virtual servers, there's no doubt the landscape has changed considerably since the 1980s, when a 1 GB hard drive was the size of a juke box. However, the sheer volume of data requiring storage ensures that space still dictates the direction for design and operations.

It's hard to imagine total global capacity, but in February 2011, the University of Southern California released research which calculated current worldwide data storage at 295 exabytes, or 295 billion gigabytes. And it keeps growing; in a study conducted by IT research company IDC in June of the same year, it was predicted that the world will generate 50 times current data production levels by 2020. It's all got to be stored somewhere. It's growing at such a rapid rate that in the not-too-distant future we'll hit a level that we haven't even derived a term for yet ... but that's another story.

Power consumption

There's no denying data centres are power-hungry beasts. Power to run the IT equipment itself, then power to run cooling and other environmental controls and ancillaries like lighting. Power consumption in a data centre is often measured using PUE, or power usage effectiveness. PUE is the ratio of total power for the facility, including cooling, lighting etc, divided by power utilised by the IT gear alone.

POWER USAGE EFFECTIVENESS = Overall facility power/IT equipment power.

Guidelines indicate an optimal PUE target of 1.0, meaning that almost all power usage is consumed by the IT hardware itself. Given the requirement for cooling and environmental controls to ensure that ambient conditions are the most favourable for the IT equipment, it's not uncommon to find a PUE closer to 2.0. Not uncommon, but not ideal either.

Cooling and environmental controls

Continual reliable operation is paramount in a data centre as any downtime can spell disaster. Hardware is susceptible to overheating if adequate cooling and ventilation aren't in place and even a few degrees can make the difference between business as usual and catastrophic failure. If the installation is fortunate enough to escape immediate failure, it can still suffer delayed malfunction as fragile electronic componentry can break down weeks after an overheating incident.

Factor in loss of business, hardware replacement and employee underutilisation during downtime and it's easy to see that the costs soon add up and why operators are so keen to avoid it.

How the big guys do it

Some of the world's bigger data centre operators including Google and Facebook, have been busy publishing information on their own centre energy-efficiency initiatives, temperature control and other cooling methods. Cynics might suggest that this transparency is a PR exercise, but if there's lessons to be learned, why not take heed?

Google suggests that most data centres are probably running cooler than they actually need to. They cite the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) and IT equipment manufacturers as expert opinion and suggest a slight temperature increase will not only have no detrimental effect on equipment, but will deliver an immediate measurable energy saving.

The company also implements a design ethos comprising thermal modelling and airflow controls. The modelling identifies potential data centre 'hotspots', so that equipment can be physically laid out in a fashion that delivers even temperatures across the installation. Methods of airflow control that require no energy, such as plastic curtains and blanking panels, are utilised to ensure adequate segregation between hot and cool areas. Where possible, Google uses water for cooling, rather than chillers.

The Open Compute Project, which has made public Facebook's so-called 'secret data centre recipes', is a bid to encourage data centre development that is more efficient from both a cost and power perspective. After 12 months redesigning their server specs, Facebook worked with manufacturers to achieve a 38% increase in efficiency and a product they maintain costs 24% less than the industry standard. They assert a PUE of 1.07 at the Prineville, Oregon data centre. Google claims between 1.06 and 1.12 across its centres, dependent on the interpretation of total facility power usage (it claims it uses a more stringent approach than others).

Design

So, while not every data centre is on a par with Google, Facebook or Amazon, lessons can be learned from the way the way the big guys address problems. The same basic design principles apply and the problems they are facing today are the problems of the future for smaller scale projects, particularly if you consider the projected lifespan of a data centre.

To assist with the design process, professional organisations such as ASHRAE make a wealth of information available to members including a comprehensive selection of publications specifically for the datacoms sector. These incorporate guides on best practice design for energy efficiency in data centres, power trends and cooling applications and real-time energy consumption measurements. See www.ashrae.org/bookstore for more.

Monitor, monitor, monitor

The importance of monitoring really can't be overemphasised and, as the size and scope of data centres increases, visibility from a remote location is imperative. With a simple monitoring system in place, changes to environmental conditions that pose a threat to system operation are identified before the crisis unfolds, via a web browser from any location.

Power usage monitoring is also useful and can provide valuable design input for data centre upgrade projects in particular. Many solutions offer everything from continual data logging and report generation, which give a snapshot of the situation as it stands, through to enabling corrective measures.

Systems incorporating redundant power switching provide a reliable method of automatically switching equipment to a backup power source, ensuring critical network devices are always up and running.

There was once a time where the power draw of a data centre would be the least of a contractor's concerns. As long as the install went according to plan, then job well done. These days, everyone on the project has an interest in keeping power costs down as the crossover between roles creates some blurring of lines of responsibility. At the very least, it makes sense to have an understanding of the factors that influence overall project power costs. ■

How to remotely reboot after a system lock-up

When a piece of LAN/WAN, telecom or other control equipment has 'locked up' and is no longer responding to normal methods of communication, it is often necessary to perform a cold boot. After the power has been cycled on and off, normal communications via the network can resume.

This can be difficult at unmanned sites or when the problem occurs outside business hours. Even if a reboot is needed while someone is around, you still have to hope that the employee is savvy enough to reboot the right device.

For systems administrators, the ability to perform a power cycle or remote reboot is also a means of avoiding communication disasters. One solution is a 'remote power reboot switch', which can be controlled by the systems administrator to ensure correct booting sequences in the event of system failures.

Such a remote reboot power switch is controlled via ASCII commands. This means you can reboot with a standard external async modem or over the TCP/IP network using a terminal server, comm. server or local server with terminal software.

ASCII commands sent to the reboot switch can either query the current status, turn on/off or cycle (reboot) the AC power of any AC equipment attached to the switch. Since the reboot switch is controlled using these commands and standard modems, only terminal emulation software is required to dial the site and switch the power. Also, real-time communication with the reboot switch provides a response after each command has been accomplished.

Applications for the remote reboot switch can range from common scenarios to more complex ones. Centrally controlled WAN environments have a range of equipment, such as server routers and dial-up equipment that frequently lock-up and require a reboot. More specialised scenarios involve satellite-controlled equipment at communication towers, cellular towers or radio equipment.

The units can switch any AC powered device. Heaters and air conditioners have been remotely turned on and off at unmanned sites to protect computer equipment.

Remote power reboot hardware is suitable for cluster management, where services are distributed across a number of computer systems.

For applications that require high amperage, heavy-duty/high-amperage reboot units have also been developed. The convenience of remote AC power control can be a welcome addition to your current network management strategy, and can also save time and expense of off-hours service calls. ■

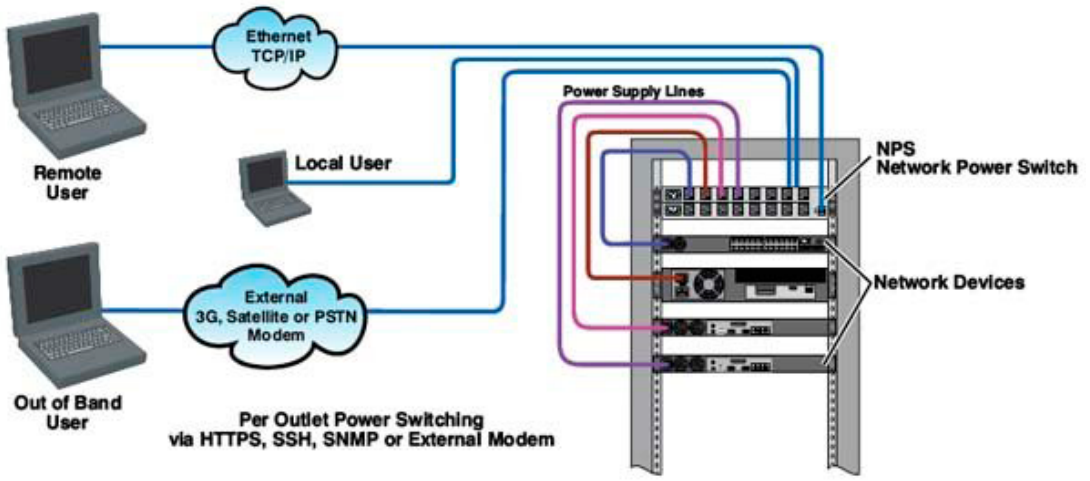


Image courtesy of Creative Commons

The data centre of the next decade

Anthony Caruana, Editor, Technology Decisions

We are in the middle of the third great revolution of technology delivery. The first was the mainframe era - where computing power was centralised and end-user devices were unintelligent terminals. Then came the PC era. Marked by massive increases in computing power, the pendulum swung completely with client computers having more power and servers being relegated in importance.

We are now in the third wave. Many services are centralised as data centres have increased in computing power and capacity while end users enjoy a massive variety in the types of equipment they can use and where they can use it. What does all this mean if we are planning a data centre strategy that will see us through the next decade?

The nature of business and what CIOs need to deliver to the business is changing at a pace that is impossible to react to. CIOs and decision makers are working at a time where business cycles are contracting and change is accelerating.

Robert Le Busque, Area VP Strategy and Development in Asia Pacific for Verizon explains: "When the curtain was falling on the Beijing Olympics the iPad didn't exist, the iPhone was only an infant and the digital universe was five times smaller than it is today."

The way businesses look at delivering applications and other services must adapt. During the mainframe and client-server eras, the IT department had control of the technology supply chain from infrastructure to applications. According to Trevor A Bunker, a Vice President with CA Technologies, CIOs will be designing and managing data centres that bear little resemblance to those of today.

"The data centre of the future, from the CIO's view, will not include the infrastructure. The infrastructure will be completely decoupled. I don't think that when CIOs think about the data centre that they'll even concern themselves with the infrastructure."

This begs the question - what is a data centre?

In our view, the data centre is where applications, business communications and business logic reside. Typically, the data centre has also included

physical assets like servers, storage and networking equipment but those have always been in place to serve the business.

Bunker believes that the physical infrastructure will be less important as time goes on. “Infrastructure provides limited competitive advantage. Infrastructure is ubiquitous. Everyone has pretty much equal access. The real competitive advantage is going to emerge from how we use the IT services running on the infrastructure regardless of where the infrastructure is.”

Still, what about the data centre of 2025? What will it look like? Will we still be constructing large rooms filled with hermetically sealed hallways and aisles of blinking lights? It’s hard to see a future where data centres aren’t part of the picture.

According to Gartner Research VP Phillip R Sargeant, data centres are becoming far denser with the amount of power that’s required in a smaller space, the amount of heat that is being generated and even the physical weight of equipment. All of this means that the choices CIOs need to make when building a data centre aren’t the same now as they were even just five years ago.

There is not a single piece of data that suggests energy prices are going to fall in the foreseeable future. Every year we see the cost of electricity rise. The federal government’s carbon tax hasn’t yet had a significant impact on prices but there’s little doubt that large users of power will continue to see the bottom line being impacted. Although there’s no universally agreed statement on what will happen to power prices over the next decade, you can expect your bills to increase by between 5% and 15% per year over the next decade.

Google’s answer to this is to build data centres where there’s access to cheap, reliable power. The locations Google chooses for new data centres show that access to cheap cooling, in order reduce power costs, is as significant a decision as proximity to communications.

Google’s data centre in Hamina, Finland, is able to take advantage of local seawater for its cooling system. Phillip Sargeant of Gartner says: “There are a lot of providers of data centres today building data centres in areas that they perhaps haven’t thought about before. They want to make use of the characteristics of the location. With cold locations they can use outside air for cooling for example.’

A critical measure of data centre power use is the power usage effectiveness index. PUE is a measure of how much power is used in a data centre for all the elements in the data centre. The aim to achieve a PUE of 1.0 - where all of the power being used by the data centre goes directly to computing. When the ratio rises above 1.0, the ‘excess’ power is being used for functions that support the computing operations.

Fujitsu recently upgraded a data centre in Noble Park, a suburb of Melbourne, with the aim of reducing the PUE to 1.7. The 6700 m^2 data centre was built in 1988. Built to Tier III standards, it incorporates four main data halls for cabinet and cage installations. The company reports all greenhouse gas emissions produced by Noble Park, as well as all others in its Australian data centre network, to the National Greenhouse and Energy Reporting System.

Location, location, location

It’s interesting that when looking back at past research what the issues were. In 2005, a Cisco’s advice focused on protection from hazards, easy accessibility and features that accommodate future growth and change. A significant part of a research paper described how to plan for natural disasters and even listed earthquake statistics.

Today, the location requirements are quite different. The accelerating density of computing power and rapidly increasing reliance on an ‘always on’ infrastructure means that our expectations of data centres have changed. While the considerations highlighted in Cisco’s report are still important, there are new things to consider for the data centre of the next decade and beyond.

In order to minimise the operational costs associated with running a data centre, businesses may need to reconsider locations. In the past, it made sense to put the business and data centre close together. However, given that connections across and between continents are getting faster and more reliable, it’s possible to choose locations with access to cheaper power and better cooling.

In the aftermath of the earthquakes that devastated Christchurch in early 2011, we toured the region and visited a new data centre operated by Computer Concepts limited. CCL's facility avoided being damaged - although the placard on the door telling us that the building had been checked was a poignant reminder of the damage not far away - but it also highlighted key considerations. CCL's facility was planning to secure its own water supply for cooling so that it wasn't solely dependent on power-hungry refrigeration.

Phillip Sargeant of Gartner highlighted to us that some data centre operators are now looking to go it alone when it comes to power as well. "There are two or three data centres using trigeneration where people have their own power plants to power data centres. Typically, some use natural gas to provide power into their own data centres," he said.

One of the challenges of any power generation technology is the inherent loss that occurs. For example, when electricity is produced at a gas-powered power station, significant amounts of energy are lost in the form of heat. Trigeneration seeks to avoid that by using natural gas to provide electricity, heating and cooling.

In addition, natural gas is a far more environmentally friendly, and therefore cheaper, fuel than coal or many other alternatives. As carbon emissions become a greater impost on the bottom line, being able to produce energy with lower carbon emissions can make a financial difference.

A recent trigeneration implementation by the National Australia Bank cost $6.5m but was expected to deliver $1m per annum in savings.

Power management is a key

Power management cannot be an afterthought in the next decade's data centre. It requires as much, if not more, planning and consideration than almost any other aspect of the data centre.

Power management is more than just worrying about the quality and reliability of supply and using low energy devices. In order to execute an effective power management strategy in the data centre, managers need ensure that the supply to every device is as reliable and cost effective as possible.

For example, automatic transfer switches can automatically switch a device from the primary to a backup power source without interrupting operations. This is done by constantly monitoring the power quality. Furthermore, the right power management equipment will also support remote management of devices by supporting remote power on, off and system restarts in the event of a system becoming unreliable.

Finally, smart power management strategies can make it easy to detect which devices are busy and adjust their power use depending on the workload. For example, research from Carnegie Mellon University suggests that some significant savings in power use can be achieved by powering off servers that are not in use and then bringing them back up to meet demand. This can't be done without effective monitoring and automated power management within the data centre.

What about the cloud?

There's no doubt that the decisions around what to do about your business's data centre needs will turn to the elephant in the room - the cloud. Past decisions were driven by different needs. As Trevor Bunker of CA Technologies puts it: "Whether it was the purely centralised model years ago, then client-server, each of the evolutions we've done for business applications has relied on one thing. That's LAN-speed network connections. That's how we built our enterprise apps. We assumed that they would run in the enterprise for the enterprise."

But those assumptions have been superseded. Bunker adds that "Anyone who's thinking about building a data centre - I would really have to ask them why. Why would you make that capital investment today? Is it really that strategic and that valuable to your business? Is it a competitive advantage for you? Many answer with frankly, it probably isn't. But it's how we've done things in the past."

Issues of data sovereignty, confidentiality, reliability, connectivity and commercial arrangements dominate any discussion of cloud services. It's interesting that service providers are starting to take a more active role in our region with Rackspace opening a new data centre in Australia and making specific mention of how it won't be subject to the Patriot Act although there's considerable debate about the veracity of that statement.

Both IDC and Gartner have recently published research suggesting that a hybrid approach will be a viable option. So, it's likely that your data centre in 2025 will have some local services and some either externally hosted or delivered as cloud applications. The physical footprint of your premises will no longer bound your data centre.

What will your data centre look like in the next decade and beyond?

It will be denser with more computing power per square metre than today. But it will also require more power and generate more heat. You'll be a lot smarter about where you build the data centre - if you build one at all - and you'll probably start by looking at the energy and carbon footprint as closely as the physical specifications of the equipment.

You'll consider making it either energy self-sufficient or less dependent on power from the grid.

Where there's no competitive advantage or a clear cost benefit, you'll probably use cloud services where providers can deliver on your operational needs and energy management goals.

What is clear is that the days of companies building large rooms with raised floors, expensive temperature management and large capital investments are fading because the criteria for making the investment decisions are changing. ■

Increasing uptime with improved environmental monitoring

Workers and customers, empowered by smartphones and widely available Wi-Fi services, want and are demanding 24x7 access to email, company network resources and websites. And thanks to today's global marketplace, even small companies must support round-the-clock activities.

Unfortunately, IT system downtime remains a problem for companies of all sizes. A 2010 ***eWEEK*** article reporting on an industry study noted that North American businesses suffer an average of 10 hours of IT downtime annually. The article went on to note that this downtime costs small companies about $55,000 in revenue each year, while large companies lose about $1 million per year.

To avoid the problems that can cause downtime, companies need to closely observe server room environmental conditions and be alerted when problems arise. This is an area where ITWatchDogs environmental monitoring solutions can help.

Examining the causes of downtime

Several data centre environmental factors can contribute to or increase downtime and service disruptions.

Heat can be a killer. Extreme heat build-up can fry a server, knocking it offline and perhaps damaging it permanently. Even moderate heat build-up can have an impact. Equipment failure rate doubles for every increase of 10°C, according to studies done by the high-performance computing researchers at Los Alamos National Laboratory. Increased failure rate due to prolonged heating has also been noted by the Uptime Institute and others.

When it comes to monitoring temperature, it is not good enough simply to nail a thermostat to the wall. Since the temperature can vary drastically around different pieces of equipment, you should consider placing separate temperature probes within individual racks or critical devices. That way,

problems with a broken fan or an air-conditioning failure will show up quickly. Similarly, you might be able to identify a server that is overheating due to it running an excessive workload.

To take nuances into account, ITWatchDogs environmental monitors are designed for today's crowded server rooms. They are small, ranging in size from only 10 cm long up to the largest models that are rack mountable at 48 cm/1U. The devices can run off of existing electrical power outlets and many support Power over Ethernet (PoE).

The monitors have built-in web servers and use standard networking protocols, including TCP/IP and HTTP. This allows server-room administrators and their technical staff to monitor temperatures over an ethernet network or remotely via the web from anywhere. The information is presented in a manner that allows quick inspection of current temperatures, as well as historical data to help spot heating pattern trends. Finally, all ITWatchDogs environmental monitors are capable of sending alerts via SNMP traps, email and SMS messages. Some devices can also trigger an external phone dialler to provide voice call alerts for up to nine phone numbers, when predefined thresholds are exceeded.

Other server-room environments can cause downtime problems and need comparable monitoring and alerting capabilities.

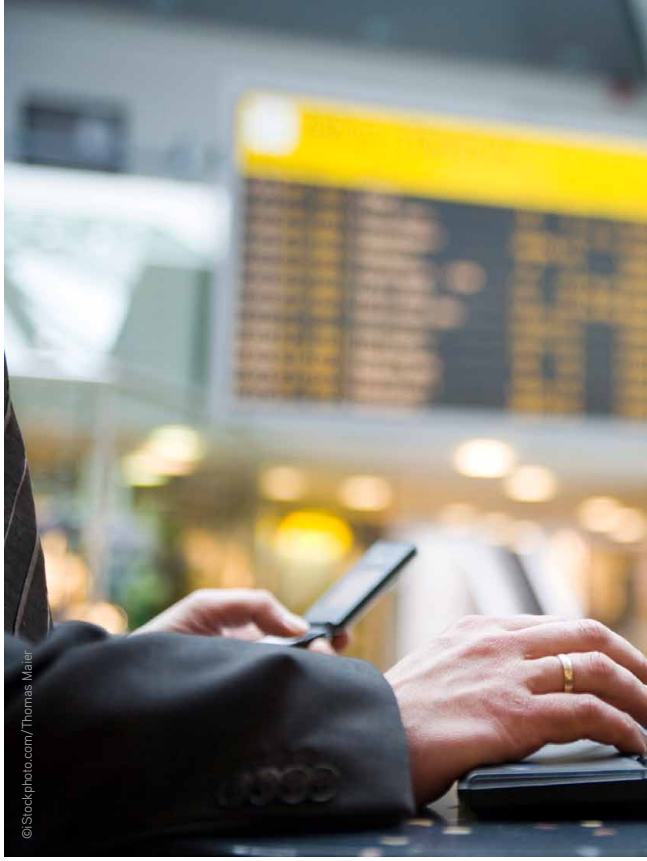
Humidity is another major threat. The reason: Humidity is the amount of water vapour in the air, and too much water vapour can form condensation on electronic components, leading to electrical shorts. If the humidity is too low, there is an increased chance of damage from electrostatic discharge. In either case, uncontrolled humidity can severely damage critical server components, causing the server to crash and shutting down access to applications and data.

Unfortunately, humidity is one of the trickiest environmental characteristics of a server room to measure and, as such, requires very close attention.

To measure humidity, most companies have focused on relative humidity. In fact, for years the guidelines followed were based on recommendations of the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). The group suggested that the relative humidity for computer rooms be within the 40 to 55% range. However, because relative humidity varies with temperature, ASHRAE now recommends that data centres measure absolute humidity, expressed as the dewpoint (it should fall within 5.5 to 15°C).

As was the case with temperature measurements, humidity can vary significantly within a data centre. So sensors must be placed throughout the room and server racks.

Water in a server room is never good news. Whether the source is a leaking or burst pipe, or a flood, water can easily shut down an entire organisation. Examples include:



- A water main break in Texas took down the computer systems in the Dallas County Records Building. According to ***The Dallas Morning News***, this "[crippled] operations for almost the entire county government".
- Rains flooded a T-Mobile data centre in the Pacific Northwest, taking down servers supporting the company's service activation portals and websites.

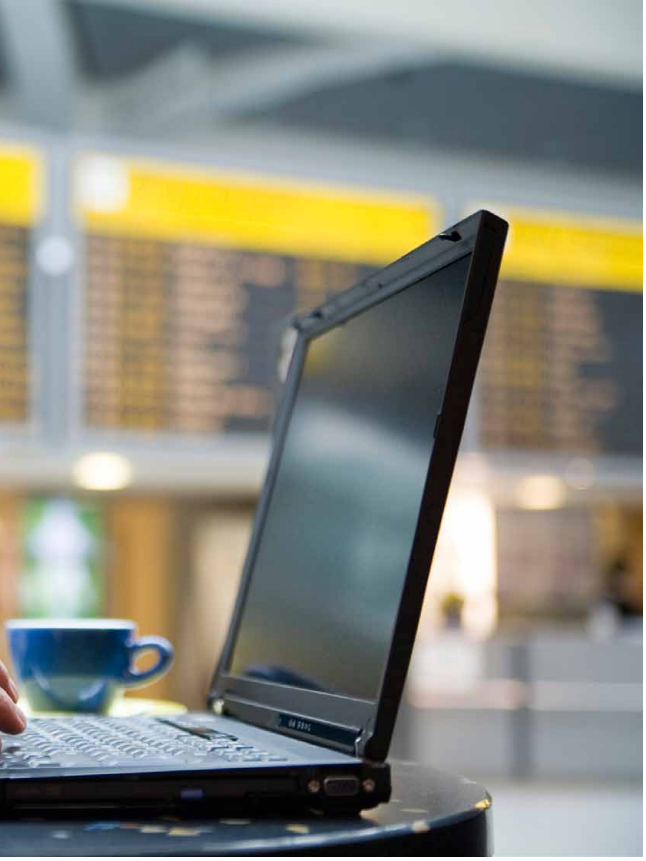
Water is usually measured using a cable that is run under an equipment room's raised floor. When water comes in contact with the cable, an alarm is triggered.

Proactive water monitoring should make use of sensors capable of detecting the presence of water over a large area so remedial action can be taken before it shorts out equipment.

A less frequent cause of downtime is fire and smoke. In 2008, a fire destroyed 75 servers, routers and switches in a Green Bay data centre, according to Data Center Knowledge. Smaller fires and smoke from equipment or frayed wires can trigger fire-suppression systems which, while much better today at safeguarding equipment, can still cause damage to IT equipment.

To detect fire and smoke requires more than traditional building smoke alarms. The problem is that when they sense smoke there may be no one around to hear it. What's needed is an alarm that connects to web-enabled environmental monitors. In this way, the smoke alarm works as it normally does, but its alert can now be sent via an SNMP trap, email, SMS and/or voice call to multiple IT staff members.

ITWatchDogs environmental monitors come equipped with various onboard sensors along with digital and analog inputs for external sensors, includ-



ing temperature, humidity, water, smoke and fire to name a few. The environmental monitors provide a way to remotely monitor server room conditions, view historical data to spot trends and receive alerts when conditions exceed predefined thresholds. The information provided by ITWatchDogs environmental monitors can help a server room staff:

- notice changing conditions and take pre-emptive action to prevent downtime;
- spot troublesome fluctuations and anomalies that might contribute to downtime;
- receive alerts when conditions warrant immediate attention.

Furthermore, ITWatchDogs climate monitors can be configured to display video feeds from up to four IP network cameras. The interface provides a quick view of remote conditions along with environmental measurements when logged in. For a manager working remotely or at home over the weekend, secure access to the interface is perfect to see who's in the server room and check what's going on from time to time. Upon alarm, a quick glance can also help determine if a trip to the facility is required or not.

And finally, when it comes to server room downtime, the elephant in the room is power outages. Power outages are the leading cause of downtime. Certainly, short outages can be covered with properly configured UPS systems. However, in some cases, a UPS might further contribute to equipment failure if it leaves servers running while the A/C remains off.

Naturally, if the power outage is longer-term - for instance, a severe winter storm tears down power lines - knowledge of the extent of the power failure is essential so that backup plans can be initiated.

For power monitoring, ITWatchDogs offers the Remote Power Manger X2 (RPM X2). This adds remote power monitoring and switching capabilities to any ITWatchDogs environment monitors supporting a digital sensor port. The add-on accessory presents real-time logging and graphing of voltage, amperage, real power, apparent power, power factor and kilowatt-hour to provide trend analysis and power metrics for future planning. The device enables users to set alarm thresholds for these measurements and it can remotely reboot locked systems or control system power via the secure user interface.

ITWatchDogs as your technology partner

To increase IT system availability, organisations need to take a proactive approach to monitoring the environmental conditions that contribute to downtime and disruptions.

Certainly, for years IT equipment such as servers, switches and storage devices have had temperature and fan sensors, as well as software to send alerts when temperatures rise or a fan fails. But in many cases, these systems only notify you once a problem is severe. Additionally, these monitors only give you information about an individual device.

Proactively monitoring conditions in the entire server room or data centre helps identify issues before they turn into a problem. This allows time to rectify matters before equipment deteriorates or fails.

ITWatchDogs offers a wide range of environmental monitors providing cost-effective ways for server-room managers and their staff to proactively monitor their IT infrastructure and maintain system uptime. The products provide a quick and easy way to keep an eye on remote conditions from a secure web interface and receive alert notifications when specified alarm thresholds are exceeded. The interface displays live video feeds and environmental measurements including temperature, humidity, airflow, light, sound, power and water detection. The measurements are logged and graphed for viewing trend patterns. External processes or applications can be automated on an alarm trigger or remotely through the web interface with units supporting output-relay control or with the Remote Power Manager X2.

ITWatchDogs' climate monitors use standard web server software to display their measurements and camera feeds. All management and monitoring tools are accessible securely via ethernet or the internet; no software installation is required. The monitors have SNMP agent software to integrate with popular networking management tools and they support SNMP v1, v2c, and v3.

Most importantly, the ITWatchDogs line of products provides the proactive monitoring needed to maintain high availability in today's data centres and equipment rooms.

For more information about ITWatchDogs, visit www.ITWatchDogs.com. ■

Interworld Electronics is the Australian distributor of ITWatchDogs

resources

from our sponsor

Interworld ELECTRONICS

Better systems. Better solutions

Founded in 1989, Interworld Electronics offers a full range of highly reliable industrial rack mount and embedded computer solutions, data acquisition and communications hardware, audio visual distribution systems, call centre recording, data centre power and environmental monitoring equipment. Our products and solutions can control manufacturing processes, collect data, control transportation systems, monitor power and increase data centre efficiencies.

Interworld Electronics is not simply a component re-seller; we focus on helping our customers meet their demands. We work together with you as our partner in developing and delivering a total solution for you or your clients. Our commitment to quality has attracted some of the best known public and private sector companies in industries as diverse as telecommunications, mining, petrochemicals, pharmaceuticals, defence, medical, transportation, call centres and data warehousing.

Interworld Electronics is an ISO 9001:2008 certified company.

Visit our website: http://www.ieci.com.au/

Physical Dangers Just as Important as Cyber-Threats
http://www.ieci.com.au/information/article.asp?Article_ID=863

Environmental Protection for Large Data Centres
http://www.ieci.com.au/information/article.asp?Article_ID=861

Power Management Products
http://www.ieci.com.au/products/class_index.asp?Class=9

Console Management Products
http://www.ieci.com.au/products/class_index.asp?Class=20

Environmental Monitoring Products
http://www.ieci.com.au/products/class_index.asp?Class=19