The role of IT facilities IN BUSINESS CONTINUITY

The term ‘fire safety’ takes on a whole new meaning when you consider how easily your operations would grind to a halt if your data or systems were destroyed, writes DEAN WILSON, managing director of Emerging IT.

These days just about all functions of business including procurement, remittance, payroll, communication, sales management, marketing and accounting, plus many more, are reliant on technology in some form or manner. Facility managers will also have a full understanding of how important information and communications technology (ICT) has become to the way they plan, execute and govern their roles and responsibilities.

Data collected over time and tracked in relation to clients or customers, suppliers, trends in sales, and product development is the market intelligence that will make or break the sustainability of your enterprise. Therefore, it has become a critical risk management issue to ensure the facilities that house your IT infrastructure are as safe as possible from the myriad disasters that have the potential to bring it all to a grinding halt.

Put simply, when you have an efficient technology backbone with systems, applications, data and services that are critical components of your business, it is important to remember that you also have a significant risk to your business.

Just think what your organisation would do if it tried to go about its operations tomorrow without its ICT even for just one day. It would dramatically affect the ability to do business. So imagine the potential impact on operations if all your technology infrastructure and/or data was destroyed, or even just not available for any extended period of time.

Risk mitigation

ICT is at the core of business continuity. Therefore, most organisations that deliver ICT services to the business will have a service management framework that will include a facilities management process that manages the risks around the physical environments that house ICT infrastructure, and which is aligned to business objectives.

For this reason, it is a facility manager’s responsibility to ensure that the physical environment where the IT infrastructure is located is managed with a priority that is in accordance with the value of ICT to the organisation.

www.fmmagazine.com.au AUGUST | SEPTEMBER 2014 FM

IT facilities management includes all aspects of managing the physical environment; for example, power and cooling, building access management and environmental monitoring.

In 99 percent of cases, loss of ICT function would be a total disaster so, for that reason, facilities managers need to be involved in the management of this risk and have a comprehensive disaster recovery plan to ensure there is no FM impediment to business continuity. Effectively, your business continuity plan is an insurance policy for your technology infrastructure and data, which in many cases represents the core of your organisation's business.

Hoping that it won't happen to you is not a strategy for disaster recovery and business continuity. You have to have a plan with the ITC operations team that is ready to be activated in the event of unforeseen circumstances. If you are not sure how your IT infrastructure would survive a flooded data centre, a fire or malicious damage, or the many other risks to your data and infrastructure, then you don't have an effective disaster recovery and business continuity plan.

You need to replace the hope that nothing bad will happen with certainty that, if it does, it will not have any negative impacts on the business. As a facilities manager, you need to make the safeguarding of IT infrastructure one of the highest priorities in your portfolio of responsibility.

Recovering from disaster

Consider the example of one of our customers late last year. It illustrates some of the key components of a good disaster recovery plan that ensured the organisation sustained business continuity.

QEP is a Melbourne-based national business that undertakes wholesale and retail trading in flooring supplies and tools. At around 6pm on Thursday 19 September 2013, a massive fire broke out and quickly engulfed its entire factory and administrative offices, as well as threatening neighbouring businesses.

After more than 100 fire-fighters and over 30 vehicles spent 90 minutes bringing the blaze under control, QEP's entire office area and the equipment within – including all the network and server infrastructure and desktop PCs – had been destroyed.

Fortunately, QEP had an enterprise-wide back-up solution in place that saw its critical data safely secured at two separate locations, as well as having a fully redundant replica of its core applications and configurations ready to receive the data at a moment's notice.

When disaster struck, QEP was able to restore the data to a mirrored environment on a server at a pre-designated data centre, so the organisation could continue critical customer interaction by the next morning.

QEP's facility manager had worked collaboratively with ICT to mitigate the risks of extreme incidents such as this devastating fire to ensure that business continuity would not be interrupted. Together they had devised a disaster recovery plan that allowed for off-site systems to be switched on and uploaded with all of the critical data that was needed to recommence the core business without interruption.

Managing ICT facilities for continuity

So just what are the key elements of your ICT facility management and business continuity plan?

QEP endured potential disaster at the hands of fire, but there are many other things that can take out your data without warning and these are risks that you need to plan for. Flood or water damage is the other obvious one, but many businesses forget to cater for events such as malicious or accidental damage, vandalism or sabotage by staff members, viruses that corrupt data and even loss of power... just to name a few.

Meanwhile, as the QEP case study also demonstrates, the threat may not only affect your business. Had the attending fire services personnel been unable to contain the enormous blaze, many of the neighbouring businesses would also have been gutted by fire.

ICT physical environments need to be built and maintained for the specific needs of the equipment they house. A reliable source of electricity is a key consideration, so they need to incorporate some form of uninterruptible power supply solution that includes automatic switch-over to an independent generator if the main grid or connection to it fails.

The micro-processors that run computer systems generate a lot of heat and will fail if they get too hot, so cooling is also something that needs to be managed to avoid the risk of failure in the main system. Often server rooms will need to have an independent air-conditioning system with a unique thermostat, so that the environment can be regulated at the optimum temperature.

As with any other business plan, there needs to be a valid business case to have a sustainable IT continuity plan and to get the required commitment from management.

Today, most organisations have developed business continuity planning and set their IT infrastructure, processes and business model to reduce the impact of natural disasters and outages they may face. Many, however, do not undertake testing of their plan to set benchmarks, complete a gap analysis, identify areas where improvement is required and develop a roadmap to include all missing elements.

There are many service providers that will be able to support your business continuity and disaster recovery plans in relation to ICT. Or you can choose to manage it all internally. The important thing is to make sure that you do have a plan and that it covers all of the bases, so that almost any imaginable scenario will not affect your business continuity.

Know your business

As discussed, your ICT continuity plan is an increasingly important component of the overall business continuity plan and therefore it needs to be aligned with defined business strategies and objectives. Wrong or incomplete solutions will

not achieve what they are meant to do and will lead to the wasting of time and money.

Facility managers are right there in the thick of developing an ICT business continuity plan and, in fact, are probably the best people to be driving it, as they have the skills to assess the risk variables.

A regular company-wide risk assessment exercise needs to be undertaken in relation to ICT systems, applications and security to ensure all potential risks to the physical environment are covered. Then the recovery plan needs to be set accordingly. Additional flexibility can be achieved by outsourcing some ICT functions – such as the help desk – which makes the company less reliant on internal people in the case of having to enact your recovery plan.

Of course, people are a key element in ICT continuity plan, so creating a plan that depends on a small number of personnel represents a threat to the overall effectiveness of the plan. What if one of those people is unavailable for some reason?

You need to identify a pool of employees who are capable of responding in an emergency. You then need to initiate a set of best practices, such as job rotation, staff mobility in the job contract, a succession plan and training to ensure that people are ready to run the plan regardless of their positions or experience in the organisation.

Your ICT continuity plan should not be an afterthought when preparing the budget. It has to be included in the company business continuity plan, so that you are seen to be having a proactive approach to ensuring that ICT is always available – even in the event of disaster – and that funds are available to activate it if required.

Constantly evolving options

There are many new trends in technology such as virtualisation, mobile devices, cloud computing and social media, which all need to be assessed and utilised in the event of needing to activate a disaster recovery plan.

Some of these new technologies introduce complexity, so maintaining the IT environment may require associated new skills and resources, whether they are trained up internally or contracted. There are obvious benefits in reducing the complexity of your disaster recovery plan and keeping it simple for operational staff to run while also eliminating potential sources of human errors.

One of the best ways to reduce the costs of having to buy, rent and maintain alternative facilities, such as a disaster recovery site, as part of your ICT continuity plan, is to look for mutual agreements with other organisations or third-party services providers to share IT infrastructure and office space in contingency situations.

In the event of a total destruction such as experienced by QEP in the above example, replacing the hardware could be affected by the availability of stock. Therefore, a high level recovery plan would also give consideration to leasing or procuring new IT infrastructure (including data communications) and arranging with suppliers to have them carry a contingency stock of IT equipment and software etc, to be available at short notice.

Meanwhile, password protection is also a key consideration to maintain data security. Authentication IDs and passwords need to be stored in two geographically separate and secure locations with more than one IT staff person having access to all passwords and codes.

Once you have established your ICT continuity plan, every major application enhancement, technology infrastructure change or new service offering should have its own BIA (Business Impact Analysis) and risk management reviewed for applicability. In addition, changes need to be assessed via an RTO (Recovery Time Objective) and RPO (Recovery Point Objective) to ensure that change

In 99 percent of cases, loss of ICT function would be a total disaster so, for that reason, facilities managers need to be involved in the management of this risk and have a comprehensive disaster recovery plan to ensure there is no FM impediment to business continuity.

management is embedded as part of the business continuity plan life cycle.

It is important to remember that your overall business continuity plan and its subsidiary ICT disaster recovery plan is an ongoing process, which will not stop after testing. It has to be tested, maintained and updated on a regular basis as required.

These processes will familiarise staff and IT teams with the continuity and recovery process should it ever have to be enacted. They will verify the effectiveness of the selected strategies and the readiness of the recovery site, and will identify improvements required to the process and infrastructure.

The recovery tests should be conducted at a business or ICT service level, and should avoid focusing on components such as hardware, systems and applications. A particular service may require different servers, data on several local drives or user network connectivity.

Roles and responsibilities

Organisations are urged to assign individuals and teams to lead, drive and run the ICT continuity plan. Authority should be given to a crisis management team to make the process effective and sustainable. Auditing plans and procedures will enable an impartial third-party review of regulatory requirements, laws, standards and best practice frameworks to provide recommendations.

Finally, the business's perception of risk must be changed. It should come as no surprise that risk management and continuity planning often end up siloed into separate functional areas. Changing the perception and culture has to begin at the top level with a top-down approach to the following tasks:

- putting the organisation in place
- instituting reporting at the top level to avoid any conflict of interest
- including continuity management on the board meeting agenda
- ensuring that a continuity section is included in every corporate document
- initiating policies and procedures to promote and develop internal control and compliance functions
- conducting regular risk assessment to determine changes in the organisation's risk profile and assess performance, and
- proceeding with regular audits.

In all circumstances when it comes to ICT continuity and disaster recovery planning, you should avoid at all costs a philosophy that decrees that 'the boss knows best'. Senior management must listen to and accept the thoughts and ideas of others, in particular the experience and specialist skills of ICT and facility management personnel. ●

To further discuss managed services, disaster recovery and business continuity, Dean Wilson can be contacted via: deanw@emergingit.com.au Or visit www.emergingit.com.au.