An explanation of the process and Customer requirements

Overview

This document outlines the requirements that should be met prior to providing out of hours service for a customer. These requirements will ensure that the customer site is in a secure and supportable state in order to increase uptime and litigate against business interruption through service failure and rogue software such as spyware, viruses and malware.

These requirements also ensure that NCI's support technicians are able to access the equipment under support by the most efficient method. The customer's requirement for out of hours support indicates that their systems are key to the running of their business and as such provisions must be put in place to maximize availability.

All of these requirements can be implemented and supported by NCI, following a discussion with the customer to ascertain exact details of the systems and services to be covered NCI will provide a quote detailing all costs involved.

It is common that some of the systems will be in place already as they follow NCI's standard business practice.

Process

An NCI representative will meet with the customer to ascertain their requirements. Following this meeting NCI will draw up a schedule of products and services to be supported. The schedule will also detail the supports hours and a full list of requirements that must be met prior to starting the out of hour's contract. This list will detail all costs involved with implementing the requirements. After successful implementation these requirements a start date will be agreed and the customer will received letter confirm the start date and call logging process.

Standard Requirements (all customers)

Network Security:

Operating systems:

Customer must have an operating system covered by Microsoft main stream support, as time of writing this is Windows Vista or above for desktops and Windows Server 2008 or above for Servers.

Anti-virus and Spyware

All PC's and Servers on the network to be supported must be covered by a managed anti-virus and spyware solution. A managed anti-virus solution is one that is monitored to ensure each device has up-to-date virus definitions, and one that will alert NCI in the event that any device fails to receive or deploy up-to-date definitions.

REQUIREMENT: NCI's Gold, Platinum or Pro Support Contract or managed anti-virus solution.

Email protection

All inbound and outbound email should be protected by a hosted anti-virus and spam filtering solution, the solution should filter 100% of all known viruses and 90%+ of unsolicited email. The server and/or firewall should be restricted to only accept inbound email from the hosted filtering provider:

REQUIREMENT: Microsoft EOP, Messaglabs or GFI.

Security updates

All PC's and Servers on the network to be supported must be covered by a monitored security patch deployment system. A monitored security patch system will deploy Microsoft security patches to all PC's and Servers on the network and alert either NCI or an onsite administrator or any failures which can then be mitigated immediately.

REQUIREMENT: NCI's Gold or Platinum Contracts or WSUS and onsite IT Administrator.

Gateway Filtering of viruses, spyware, malware and intrusion prevention.

The customer's network must be protected at the internet gateway by a device capable of intercepting rogue software such as viruses, malware and spyware. This device should also be able to spot and block intrusion attempts from hackers, bots or internet devices.

REQUIRMENT: Sonicwall and either a Comprehensive Security Suite subscription or anti-virus, spyware and intrusion protection subscription.

Additional requirements for specific services and hardware

Each major service has been handled separately, if you require out of hours support for any of these services or hardware the recommendations must be met. In certain cases the implementation of these conditions may mean that out of hours services may no longer be required, in particular if the solution provides full redundancy during a service outage such as through the use of Hyper-v replication or server mirroring.

Internet Connection

Standard broadband connections (ADSL/Fibre etc..) do not have a Service Level Agreement or time to fix guarantee. In particular if there is a problem at the local exchange BT are under no obligation to fix the issue in a set time. For this reason alone NCI cannot guarantee a fix for internet connectivity when the cause is related to an issue outside the customers network. To litigate this problem a backup or failover circuit wireless circuit is required.

REQUIREMENT:

Backup Internet Circuit – 3G/4GBackup with Fixed IP Address (The Sonciwall range of firewall from 200 upwards all support this configuration)
A site survey may be required to ascertain coverage; an external directional antenna can be installed to boost the signal if necessary.

In addition, the internet router must be from an NCI supported manufacturer and NCI must have all login credentials and ISP credentials including any relevant phone numbers and security phrase.

REQUIREMENT: Router types: Zyxel, Draytek, And Cisco

Email (Exchange Server)

Exchange email is generally dependent on local server availability, however NCI are able to provide a Business Continuity solution to get around the problem of a failed local exchange server. The business continuity system allows user to logon to a web portal during an outage and access a 1 month rolling archive of their mailbox, they are also able to send and receive email from the portal.

REQUIREMENT: Email Business Continuity Solution such as Microsoft EOP or GFI.

SERVER

A local file server is often a single point of failure for one or more services and line of business applications. It is vital to ensure that all data and configuration is backed regularly and that there is a disaster recovery solution in place. Tape backup is not the ideal solution for this as it is a selective backup and may not be backing up everything on the server. There is no way for NCI to monitor if backup job are modified and removing items from the job may mean that you cannot recover the server at all. For this reason an all-encompassing and monitored backup is essential, with synchronization to removable media that must be taken offsite or stored in a fire proof safe. The backup system must immediately alert us in the event of a failure.

REQUIRMENT: NCI's Backup and Disaster Recovery Appliance (BDR) and at least 3 removable drives to store an offsite copy.
A single BDR can backup multiple servers, act as a standby server and enable restore to dissimilar hardware.

In addition NCI's technicians also need to be able to access the server remotely, even if the operating system is not loaded in order to remediate any boot problems that may arise efficiently without attending site.

REQUIREMENT: IP KVM connected to the server or HP Lights Out (HP Servers) or Dell iDrac Enterprise (Dell Servers)

Training, Testing & Information Sharing

The customer should nominate one or more key staff to interface with NCI during an out of hours support call. These staff should be aware of all items covered on the schedule and the hours of operation. They should be trained on how to access or implement any backup or continuity systems during an outage. Training will be provided by NCI. Cribb sheets for access to these systems should be made available to all staff and stored in a central location.

The customer must schedule with NCI a test of each of the backup, continuity or disaster recovery systems. This testing must be performed at least once per year.