VoIP and business continuity
This issue of the journal contains various articles exploring this important issue:

VoIP - most businesses plan to implement but business continuity risks not clear
The results of Continuity Central's survey into Voice over Internet Protocol.

Continuity planning for VoIP
Lawrence Imeish provides advice on how to harden and protect VoIP and IP telephony networks.

VoIP - vulnerability over Internet Protocol?
Consultant Wil Allsopp highlights some of the risks inherent in Voice over Internet Protocol.

VoIP – is it really suitable for mission critical telecoms?
Iain Franklin, European VP of Entercept, gives his opinion.
VOIP - MOST BUSINESSES PLAN TO IMPLEMENT BUT BUSINESS CONTINUITY RISKS NOT CLEAR

The results of Continuity Central’s survey into Voice over Internet Protocol.

VoIP is assumed by many market analysts to be the technology of the future, but have the business continuity risks really been considered? Continuity Central recently conducted a short survey to throw some light on this area.

The survey, conducted throughout February, found that 80 percent of respondents either already have or plan to install VoIP solutions. 14 percent have fully implemented VoIP systems; 37 percent have partially implemented VoIP; 15 percent have not implemented it but expect to in the short term, while 14 percent expect to implement in the longer term (24 months+).

There appears to be little consensus on the potential impacts of VoIP on business continuity. 30 percent of respondents thought that VoIP would reduce risks overall, with 23 percent thinking the opposite. 12 percent believe that VoIP will greatly reduce risks; 18 percent that it will slightly reduce risks. 14 percent see a slight increase in risks and 9 percent feel that risks will greatly increase once VoIP solutions are in place. 22 percent of respondents thought that risks would not change and 25 percent didn't know what impact VoIP implementation would have on their business.

Continuity Central asked respondents to add some comments to explain their view on the risks of VoIP. A selection of responses are listed below:

* This is an answer from one of my senior network analysts regarding this issue. There is no single thing that is going to provide business continuity and disaster recovery. Redundancy must be built into the production network so it can withstand multiple outage types. The strengths that convergence and VoIP bring are the agility and ability to recover quickly by bringing up sites fast and cheaply. It also allows you to layer in redundancy in the production LAN much easier and most cost effectively.

* My own experience shows me that VOIP is prone to:
  a) Interception and redirection to SPAM voice mailboxes & sales
  b) The quality of audio is inconsistent during a call, and is sub-acceptable for business and personal conversations
  c) The VoIP calls are subject to intermittent delays and voice artefacts, disrupting the train of thought and conveyance of information.

* VoIP will only be implemented as Voice-over-VPN for persons who will be required to work from home during an emergency or quarantine situation. This technology will permit the PC microphone and speakers to be used for voice communication at the same time that the PC is being used for business applications, and only one communications link is required.

* As a consultant that installs VoIP and IP telephony systems, I find the biggest risk in their implementation usually comes from the customer not wanting to spend the extra money on the backup and redundancy systems. These systems are not just for the VoIP Network (i.e call manager clustering or remote site survivability with call manager express) but for the entire network, such as UPS for all routers and switches, and a proper stable routing protocol running. A VoIP or IP Telephony rollout is only as good as the network it overlays, and most of the time the existing network is vulnerable to outages. A properly designed and deployed VoIP system will give the same if not less risk due to the IP ability to find multiple paths to a given destination. In the TDM world, if a voice T1 goes down between two offices, that would usually be the end of
calls, even if other types of WAN connections exist between the two points. In an IP world if part of a WAN network fails, so long as a back route is found the calls will go through (with a possible short delay for network change over), usually with no configuration to the VoIP or IP telephony system. The important message is that a properly designed and deployed VoIP can actually be more stable than a traditional PBX while still offering expanded functionality and cost savings.

* Power requirements have become more important for VoIP continuity. The network now must support the entire company operations, an outage will affect more systems than prior to VoIP. A properly designed VoIP network will not create the much more risk.

* I believe VoIP is the future. In the near future we should start seeing wireless technology integrating with VoIP. This is when I believe VoIP will hit the market hard worldwide.

* VoIP is a backup to our present voice installation. Two call centres back each other up. If one centre goes down the other receives calls on the VoIP phones alerting team of problems at the other facility.

* Currently our entire campus depends on a single PBX located in the data centre. If we lose that building or the data centre we lose all voice on the campus. Our new Cisco VoIP system is located in another building and can operate independently from the PBX and data centre.

* With some companies, voice communication may be impacted in event of IT hardware outages, thus making emergency voice communications more difficult. However, if availability and recovery have been factored in at the design stage (very rare, I know) then use of alternative hard or mobile systems should mitigate.

* We use VoIP as a backup to the switched PSTN. During the New York power failure, we were able to coordinate recovery with the folks in New York even though we couldn’t get any calls through via cellular or the PSTN. I would never recommend using VOIP exclusively however. It’s just one more layer of redundancy that has become available at a very competitive cost, although not as cheap as some would suggest.

* VoIP solutions are often based on the Microsoft operating systems, and while virus writers continue to target Microsoft, there will always be a risk. For example both Code Red and the blaster viruses also attacked Cisco networking equipment, and Blaster in particular Cisco VOIP solutions - see [http://www.theregister.co.uk/content/archive/32340.html](http://www.theregister.co.uk/content/archive/32340.html)

* My company is a lending organisation that is divided into wholesale and retail operations. The company maintains several hundred retail operations nationwide all supported from a single headquarters location. A fear of losing voice communications has made VoIP a dirty word. And that is before the concept of recovery is considered.

* Our SP can re-route inbound calls from DDI to associated mobiles or PSTN lines. I argue that this is reduces risks.

* Risks may not increase or decrease but they will certainly differ compared to today’s situation.

* There is some question as to whether VoIP will perform in high volume environments.

* We have had VoIP for some two years now with Cisco IP Phone 7960. There is no integration with the desktop as yet. When true convergence of voice, data and video occurs then the risks will become significant because of the reliance that people will place on the technologies. Without the convergence it is just a smart phone.
* VoIP technology, although saving considerable sums of money, has huge implications, as far a business continuity goes. The very fact that IP addressed voice routing is systems and networks based, means that it has an inherent single point of failure - overload, damage, or take out part of a network, and you’ve taken the communications system. Which is why the bank I work for restricts communications to hard wired solutions which (hopefully) have greater operational resilience.

* Instead of having only data over the network we would rely on the network for voice also. If a fully meshed multi-vendors network were not established we could face once again a single point of failure.

* More eggs into one basket. When voice was separate it was a separate recovery and separate resources. Now it is dependent on IP being available. Perhaps I am staid in my opinions, and once it settles down and beds in - I will feel better.

* VoIP is great in a production mode. The recovery of the Call Manager has yet to be determined by Cisco. When brought up at our company they acted like it was the first time they thought about recovery. Frustrating very ‘bleeding edge’ from a recovery standpoint. Remember, VoIP requires special handsets that have approx. costs of $350 each. To leverage VoIP in recovery mode means you need to have duplicate phones in storage.

* With redundancy is the right places, there will only be a short term risk increase as there is with all new systems. It is being done as a business operations improvement rather than just a BCP action and it is felt that it will increase reliability.

* We used VOIP as a backup when cell phones and circuit switched services were unavailable during the NYC power outage. We continue to implement it for low priority and backup services.

* We will have trouble communicating during power outages, impacting our continuity and emergency response capabilities

* With VOIP, if you lose the data link you lose it all. With separate systems, you can still maintain communications.

* Use of VoIP reduces our risks as it allows for simpler switching of telephone lines in the event of disruption at one of our sites.

* The technology is so new that risks have not been identified. Once risks are identified, then plans can be formulated.
CONTINUITY PLANNING FOR VOIP

Lawrence Imeish provides advice on how to harden and protect VoIP and IP telephony networks.

As more organisations look to IP telephony and VoIP to boost productivity and reduce overheads, business continuity managers should re-evaluate their existing data networks to assess the new challenges faced. Adding VoIP or IP telephony can be a relatively simple, or very difficult process. Any VoIP integration specialist will tell you that spending time planning the service, will produce a stable and readily accepted system. Adding voice to a data network magnifies the importance and risks of the network. The integrated network becomes an extremely critical piece of the business and should be well protected. Imagine the loss in productivity and revenue when a network outage affects not only the users’ ability to access network applications, but their ability to make and receive calls.

Business continuity planning for IP telephony involves examining every layer of the network and all its dependant components. The most important part of any IP voice system is of course the IP. When adding critical services such as voice to an IP network, be sure to understand the service is only as good as the network that carries it. Many times VoIP and IP telephony services fail due to lack of attention to basic IP connectivity and IP QoS.

IP network link redundancy becomes vital when supporting an IP telephony system. Most IP voice systems require centralised call processing; this is where the call routing decisions are made based on dialled digits, time of day, and network utilisation, etc. Loss of connection to the call routing service or application failure would lead to all IP phones no longer able to make or receive any calls. For this reason, all WAN links that carry voice or voice signalling should be made redundant with shadowed circuits or at the very least ISDN backups. All backup links should be tested on a regular basis during maintenance windows to confirm they automatically cut over when the primary link fails. The IP routing protocols (OSPF, EIGRP) should also be optimised for fastest possible convergence upon a network change and should recognise VoIP as ‘interesting traffic’ capable of initiating the backup link. It’s beneficial to test the failover configuration and measure the time it takes for calls to pass after a WAN Link failure.

In terms of IP and Ethernet redundancy, it’s best that each edge switch have at least two links to the core switches. This will create redundancy in the LAN even if one of the core switches fails. It is difficult and expensive to cluster the edge switches, a secondary solution is to have a cold unconfigured standby switch ready to deploy in the event the edge switch fails.

ADVERT:
Within IBM we have over thirty years experience of business recovery planning. Our experience can complement yours to create, test and maintain your own effective business recovery plan. The business recovery plan that you create must reflect the needs and views of your organisation. Working together, we will define a recovery strategy that suits you.  
http://www-5.ibm.com/services/uk/portfolios/bcrs.html
VoIP and IP telephony systems can terminate calls in one of two places; to another IP telephony device/endpoint or a VoIP gateway that interfaces to the local PSTN. Call routing redundancy is often overlooked when deploying or managing IP voice systems. If the enterprise has multiple offices or multiple gateways, backup call routing schemes should be devised so that outbound calls will make it to the PSTN even if the preferred local gateway or PSTN service is down. For example if there are two offices, one in New York and one in Washington, and the local Washington gateway fails, all the users outbound calls from Washington could be sent to the NY via a WAN connection (leased line or internet VPN) and dialled back to Washington using the NY gateway. This could be an expensive solution because during the local outage, all outbound Washington calls would incur long distance charges and the backup gateway would need to be designed to handle the extra call capacity. Another backup option is to send the organisation’s calls to an Internet telephony service provider for termination; usually $0.02 - $0.05/min for North American calls. This creates new security concerns but is a viable option for companies that do not want to invest in the additional hardware costs. A correctly designed and managed redundant IP Voice system will take advantage of IP’s inherent survivability/rerouting capabilities. This, plus VoIP’s ability to make call routing decisions contingent on the IP network’s status, makes for a robust and survivable voice communications system.

Each vendor has their solution for a high availability call routing service, usually a central cluster or two, or nodes with decentralised limited call routing services as backups (i.e. Cisco Call Manager and Call Manager Express). When deploying voice services, take advantage of the vendors’ clustering and redundancy solutions and integrate them in the IP voice network, it will pay off exponentially in the event of a hardware or application failure or outage.

An important IP voice design and management detail is the need to ensure that every network element that carries IP voice has adequate UPS and backup power. This extends to more than just the routers, switches and gateways, to include any DSX panels, call managers, CSU/DSUs, Wireless bridges, and even locally powered IP telephones. An effective design for LAN IP phone redundancy is to use edge switch to power the IP phones, this saves the need for a separate UPS for every phone set. If the switch and phone support 802.3af (Power over Ethernet) it would be wise to make use of it. It is helpful to create a flowchart that traces a typical IP call and note each powered device at every ISO Layer that the RTP Stream (the call) or call signalling traverse during the course of a call, end point to end point and confirm they all have proper backup power. If the power goes out to the office during an emergency the IP phone may be the only means of calling for help, therefore it is crucial that the phone and the whole IP voice system always function.

Finally security in an IP voice environment is also magnified; a hacker in the network will not only steal or damage files, but could possibly access the VoIP/PSTN gateways and prevent legitimate users from making or receiving calls or even make thousands of dollars in unauthorised calls. IP voice security is an extension of basic IP security; it is assumed the network already has existing firewalls and other security architecture. If it does not, then IP voice should not be deployed until the IP security is hardened. IP voice has special requirements for firewalls and user authentication. Depending on the protocol the system uses - H.323, SIP, Skinny - the firewall may need to be configured to allow incoming RTP traffic over a range of UDP ports, this can create a security risk. The best solution is to use VPNs between sites connected through the Internet and to ensure that those VPN devices have the processor power required to pass the voice packets with minimal delay. Another solution is the newer VoIP specific firewalls that actually work with your call routing systems to dynamically open and close ports on a per call basis. Needless to say any calls (or data) crossing the public internet should be encrypted. IP voice also allows for real time call accounting and active toll fraud detection, these features should be activated if they came with the billing software.

Although it may appear that VoIP creates a more complicated and vulnerable network than traditional TDM based telephony, it is important to point out its benefits. The strongest factor in
deploying IP telephony is the direct monthly cost savings reaped from a substantially reduced telecoms bill. Enterprises have seen their phone bills slashed by as much as 60 percent when deploying IP voice. There are other factors such as improved worker productivity, faster customer response times, and reduced cost of any moves, additions, or changes due to web based user provisioning. The deployment of IP voice services also provides an opportunity to unify your network and combine what were once two separate systems into one manageable, integrated, redundant unit. Finally IP telephony sets the stage for new applications and services. Imagine having the power to access vital company data and applications directly from an IP phone or a Wi-Fi IP phone handset while making/receiving calls, or receiving your voicemail via e-mail and on a web page. These new applications and services will make it very difficult for anyone who has experienced IP voice to go back to legacy PSTN. In fact, a properly planned and managed IP telephony or VoIP network will give the enterprise as much if not more survivability and availability as a comparable legacy system and still provide new features and applications which the legacy system simply cannot.

Lawrence Imeish is a consultant specialising in IP telephony and VoIP deployment. He holds a CCIE, and has over 10 years planning, deploying and managing enterprise networks. He can be reached at Lawrencelme@hotmail.com

GemaTech’s mission statement is to develop and market leading edge, innovative solutions for the Virtual Call Centre, Remote Worker, Help desk, Customer Relationship Management, Business Continuity and Least Cost Routing markets.

Our current product range covers:

Call Centre Solutions: with the world’s first truly integrated Virtual Call Centre system. The Remote Service Manager;

Disaster Recovery for Telephone Systems: the revolutionary Business Continuity Manager.

Digital Least Cost Routing: with GemaTech’s LCR, the worlds most advanced ISDN-30 routing system.

http://www.gematech.com

WANT TO MARKET YOUR PRODUCTS AND SERVICES TO THE BUSINESS CONTINUITY MARKET PLACE? Visit http://www.continuitycentral.com/advertise.htm to find out how Continuity Central can help.
VOIP - VULNERABILITY OVER INTERNET PROTOCOL?

Consultant Wil Allsopp highlights some of the risks inherent in Voice over Internet Protocol.

During the past few years the two most significant focuses for remaining IT budget have been security and cost saving systems capable of demonstrating rapid ROI. But in almost all areas of business there is a trade off between risk and cost. As companies have double-locked the doors by spending on security for the data network, they may have left the windows open by pursuing saving in areas such as VoIP (Voice over Internet Protocol).

The VoIP ‘revolution’ has been talked of since the 1990’s as the ‘next big thing’ in the enterprise telecoms sector; saving companies vast amounts of money on both call charges and internal network infrastructure and support costs. But just as the VoIP market is finally taking a cautious step towards delivering some of its long-overdue promise, the increasing priority of IT security may force it two steps back.

Recent research, by Secure Test, on the Cisco 7900 series VoIP phones have revealed serious security concerns (Note: Secure Test have independently tested the Cisco 7900 as this is the most widely used enterprise VoIP solution. Similar problems may well exist in other vendors products). With susceptibility to both DoS (denial of service) attacks and interception issues, it is clear that transferring phone systems to an IP network opens them up to many of the same security concerns as Ethernet data networks. More worryingly, phone systems may be harder or even impossible to patch.

Like many IP devices Cisco’s VoIP phones are vulnerable to ARP (Address Resolution Protocol) spoofing, allowing ‘man-in-the-middle’ attacks and including data interception and packet injection. This means that any VoIP phone can be tapped by anyone else with a phone on the same network, any individual VoIP phone can be crashed easily and any VoIP network infrastructure is heavily vulnerable to DoS attacks.

Looking first at the vulnerabilities of VoIP phones to DoS attacks, Secure Test’s initial research has shown that Cisco 7900 series phones, specifically where running the default Skinny (SCCP) protocol for messaging, can be crashed relatively easily using one of several methods. By attaching a PC to the VoIP network it is possible to send malformed messages to a target phone or to cause a buffer overflow on one of several fields resulting in a crash. By performing any of these attacks on the switchboard phone, research demonstrated that it would be relatively trivial for an attacker to disable an entire phone system in minutes.

Further research then went on to show that using a similar DoS attack, a Cisco 1760 VoIP enabled router was also vulnerable. Sending a message of 50,000 characters plus to port 2000 (the TCP port used by the router to communicate with the phones) causes every VoIP phone on the network to reboot or crash, completely disrupting communications.

Given the number of Cisco VoIP implementations in companies where the telephone constitutes a business critical system this vulnerability quite rightly send chills down the spine of many a communications manager, especially as avoiding the problem is difficult. Ideally, Cisco would release a patch to better handle malformed or malicious traffic and recover from network errors. However, whilst Secure Test responsibly informed the vendor of the problems several months ago, as yet, there have been no visible signs of progress. Understandably there may be greater problems in patching ‘dumber’ devices such as telephone hardware, relative to providing security updates for PC’s and servers. But, if the window of exposure cannot be effectively shortened by a company with the development capacity of Cisco, this could be seen as a good argument not to run phones on open IP networks until these problems have been overcome.
Having discovered the vulnerabilities with regard to DoS attacks, tests then moved on to see whether the ARP spoofing attacks, specifically data interception, were possible. Any fan of spy films will know that telephone tapping is perfectly possible on traditional PSTN based phones. Since this usually requires a hardwire tap to be set into the PBX, however, this becomes a question of the physical security of the core infrastructure. Initial tests on VoIP phones, however, have shown that where data is not encrypted, it is relatively easy to intercept, listen-in on or record conversations on any phone, from any other phone point on the network. Worryingly, most of the commonly used VoIP phones do not encrypt traffic by default and currently, many do not even support the necessary protocols to make this possible.

Initial tests on the Cisco 7900 have proved that it is possible to carry out an ARP attack on a target phone which draws the data stream through the attacker’s computer. As any conversation is transmitted in the clear using standard RTP (Real time Transfer Protocol), this can easily be decoded, listened in-on and recombined in real time, leaving the victim(s) none the wiser.

As researchers found it relatively simple to develop a tool to automate this process, it can safely be assumed that such tools are freely available on the Internet. This means that where VoIP handsets do not support the secure RTP protocol necessary to protect traffic (as with all current Cisco phones) it should be assumed that all communications could be intercepted.

All of the attacks outlined above are difficult to guard against as they work using the very essence of convergence; that you do not physically segregate the data network and the phone system. Even where separate IP networks are used, you can simply plug a PC in to the telephone network via the phone port. As one of the major advantages of VoIP is computer telephony integration (ie. screen pop-up with call information and multi-channel CRM systems) most hardware phones contain a built in switch to allow a PC and a phone to occupy the same port.

Looking beyond this, the increased sophistication of an IP based telephone network even makes it easier to create Trojans to carry out these and other attacks remotely. Secure Test most recent studies suggest that once a network has been infected, this makes is perfectly feasible to tap VoIP calls and carry out DoS attacks remotely from outside the company network.

**Wil Allsopp is a consultant with Secure Test.** Secure Test will be demonstrating VoIP vulnerabilities over Internet Protocols on their stand at Infosecurity Europe 2004, Europe’s number one IT Security Exhibition. Now in its 9th year, the show features Europe’s most comprehensive FREE education programme, and over 300 exhibitors at the Grand Hall at Olympia from 27th to the 29th April 2004.

http://www.infosec.co.uk
VOIP – IS IT REALLY SUITABLE FOR MISSION CRITICAL TELECOMS?

Iain Franklin, European VP of Entercept, gives his opinion.

Voice over Internet Protocol (VoIP) and converged networks are fast becoming an attractive alternative to traditional office networks, in terms of cost, return on investment and ability to integrate with other enterprise applications, such as customer relationship management systems. Vendors are telling customers that the quality of service (QoS) of a traditional telephony system can be achieved over IP using intelligent routing and packet optimisation, but one area many vendors are a little grey on, is how security fits into the QoS equation...

Matthew Kover, a Yankee Group analyst recently said of VoIP: ‘voice is just a different application that's running over the same IP infrastructure, so all the vulnerabilities that exist in your other IP applications, also exist in this application.'

On this basis, is it really safe to talk?

VoIP is now a practical reality for any organisation reviewing its communications infrastructure: issues surrounding bandwidth, standards and QoS have all been addressed and deployment is becoming easier all the time. There is still however, one core obstacle that could blight the success of any implementation and indeed industry-wide confidence in the technology: many VoIP gateways and applications are based on traditional operating systems and IP technology, leaving them victim to all the same vulnerabilities and hacking problems of any IT infrastructure.

A traditional phone system is isolated from its organisation's IT infrastructure and is largely hard-wired, key factors in its availability and stability.

ADVERT:

Synstar International is a leading provider of Business Continuity Services in the UK, Ireland and the rest of Europe. Synstar has provided these services for over 19 years, (previously as Computer Disaster Recovery and Granada Business Continuity) covering over 500 incidents with a 100% success rate in helping customers get back to business-as-normal.

Experienced staff in Synstar's Business Continuity Centre of Excellence works with existing customers and new prospects, building solutions that support them in achieving the highest levels of availability for their businesses given any form of interruption. This means we must be ready and able to consider business continuity approaches to people and workspace; to business interfaces and systems; and to the technology infrastructure.  http://www.synstar.com/services.html
Conversely, VoIP runs as standard network traffic on the LAN infrastructure, and in many cases the hardware supporting VoIP runs on platforms that utilise standard operating systems. Suddenly a corporate telephone system is exposed to all the vulnerabilities, viruses and risks of the LAN. It is difficult to see how IT managers and employees will cope without IT and telephony systems in the event of unplanned downtime. VoIP technology may be reliable in the lab, but in the wild it is only as safe as the weakest security link. As we all know it is not uncommon to have an e-mail 'outage' for a few minutes or sometimes longer due to unforeseen network problems. This is normally tolerated in a typical office environment, however this kind of failure would be totally unacceptable with the phone system.

"In the past, when IT systems have failed, employees could turn to the phones to remain productive, but where can they turn if the entire communications infrastructure is offline? More importantly, what will customers think when they cannot get through? Typically in our time critical world probably not much - they will just phone the competition. It will be a lot harder to hide downtime from the outside world. The paradox is simply that a technology designed to save money could end up costing more than you imagined in lost business opportunities.

The security risks associated with VoIP cannot be totally eliminated, but can be reduced. Best-of-breed security products exist to protect all areas of the network from the gateway, to the server, to the desktop, but these must be pro-active tools. Technologies like firewall, IDS and anti-virus software can only protect an organisation from what is already out there, so are always one step behind the hackers. Any hack targeted at the VoIP server will have to be proactively and transparently dealt with if major downtime is not to be inflicted on a critical piece of your business infrastructure - the phone system.

The success of VoIP within organisations will not be decided by the quality of the technology, but by the security implementations in those companies. So, is it safe to talk? Ask your IT manager....

www.entercept.com

ADVERT:

Leading companies in every industry rely on LDRPS (Living Disaster Recovery Planning System) to build cutting-edge continuity plans.

LDRPS 9.1, our latest release, takes business continuity planning to a whole new level with unprecedented power and flexibility. What's more, LDRPS 9.1 comes with new functionality that makes LDRPS easier than ever before! And that's true no matter which LDRPS version you use. From a single-user system to an enterprise wide web-based initiative, LDRPS looks and functions the same. What's more, as your company and planning needs grow, your data moves with you from one version to the next effortlessly.

With incredible new functionality and packed with unique features, LDRPS 9.1 is designed to meet all your planning needs. MORE INFO - http://www.strohlsystems.com/Software/LDRPS/default.asp