COMPARE BUSINESS PRODUCTS

The Hidden Costs of VoIP

Is It Worth the Investment?

Contents

The Hidden Costs of VoIP

A Computerworld article on VoIP asks readers to imagine that they have a device that is 100% available (well nearly), quite secure, costs of use dropping all the time and absolutely no dearth of spares or even vendors, an application that needs zero user training and has extremely high user acceptance.

> VoIP has hidden costs and it is important that they are discovered and factored in before the project commences rather than after…

This, the article says, describes the POTS (plain old telephone system) quite accurately. Why on earth would someone want to switch over to VoIP with its quirks and dependence on the Internet or other networks and a need for the user to supply infrastructure – as against POTS where the company is mandated to even provide standby battery power for 48 hours?

The answer is equally plain and has been covered in detail in many different publications and papers. VoIP offers so many benefits over POTS that users find the offering extremely attractive and ever increasing numbers of companies are making the switch from POTS to VoIP. This resembles a herd movement.

The problem with a herd is that the dust it generates hides the potholes in the road. The movement to VoIP is no different. When vendors or CIOs do the calculations, the savings and return on investment (ROI) appear very lucrative. However, any experienced player will be able to confirm that there are many hidden costs that most users may not come to know till late in the rollout.

Users often learn of these costs the hard way, hence this paper on the hidden costs of VoIP.

Revamping Internal IT infrastructure

The first hidden cost of VoIP comes in improvements to the IT infrastructure that businesses need to make while setting up VoIP in their premises. As long as the network supported email, html and databases, it could get by without needing very high quality

networks internally. However, bring in real time applications such as VoIP and video conferencing and the entire scenario changes.

Network

VoIP quality is very dependent on the latency of the network. By latency, a network engineer understands the time taken for a data packet to reach its destination. Typically in an Internet Protocol environment, data packets can arrive with a delay or get lost in transit, but since the receiving station sends out an acknowledgement of packets it has received, the sender simply repeats the missing packets.

> VoIP requires improvements to your internal IT infrastructure.
>
> This improvement also helps the company IT Systems perform better.

This approach cannot work in a real time application. If a voice packet does not reach its destination, repeating it would only increase confusion at the other end. About 250 milliseconds is the maximum that can be tolerated for a decent conversation. Professionals in the VoIP field say it should be lesser than 150 milliseconds.

As a result, companies planning to switchover to VoIP need to ensure that their networking equipment has the lowest latency possible. This may mean replacing your LAN cabling with gigabit Ethernet or a fiber backbone, upgrading switches and routers, and so on. These costs themselves may be high and will in general not be part of the estimate that the VoIP vendor may have given.

Power Supply

Besides networking components, it is well understood that companies switching over to VoIP need to improve their power supply as well. The reason is simple. With the public switched telecommunication network, the service provider was mandated by law to provide for adequate battery banks to keep the system powered up for as much as 48 hours in the event of a power failure. These companies had battery banks and adequate generators to handle major power failures. However, with VoIP, once the data packet enters the company premises, the responsibility to handle it becomes that of the user.

Besides the networking issues discussed earlier, power supply becomes another weak link.

If one looks at a large office complex, the local area network would use a number of switches and other devices before finally terminating in an IP phone on someone's desk. Every networking device that comes in the route needs to have reliable, uninterruptible power supply. Simple desk UPS's will not suffice unless the entire building has full back up generators. In some cases, companies may install separate power cabling for their networking components alone and make do with a smaller emergency generator coupled with a battery bank.

Technically, both power supply improvements and improvements in the company's network do not form part of VoIP installation. Phone calls will go through even if they are not improved. Yet, they are critical components and to get business-class VoIP - as opposed to a simpler set-up for a home phone - user companies have no option but to make these improvements. This is the first hidden cost of the VoIP phone system.

Hidden Benefit

However, there is an associated benefit. In every case, improving the IT infrastructure pays rich dividends. Users find that their applications work better, web pages do not hang and database responses improve. Users also move rapidly from simple voice to video and use richer web applications.

The solution, perhaps, is to understand that this improvement is essential and therefore companies must treat this as inevitable and conduct a survey and improvement of their systems before commencing the VoIP switch. This will separate the costs of the two and will ensure that return on investment calculations for VoIP are not forced to take account of general IT infrastructure improvement.

Vulnerability & Security

VoIP introduces a number of vulnerabilities into a company's phone system. Small businesses need to be particularly careful because they may not have the trained and qualified manpower that larger companies can afford.

Besides not having the right manpower, small businesses are also likely to be lesser resilient to business disruptions. Therefore small businesses need to take greater care of their VoIP installations.

> Ariz. based research firm InStat surveyed 220 IT professionals from companies of all sizes.
>
> More than 75% of respondents at companies that have implemented VoIP plan to replace their security appliances within the next year.

The primary VoIP threat categories are listed below:

Threat	Explanation
Confidentiality threat	Calls could be eves dropped on, recorded and the voicemail could be tampered with. This could result in loss of sensitive information and corporate secrets and to identity theft.
Availability of service	Denial of service attacks and attacks similar to those on computer networks can all potentially impact VoIP availability. Viruses and worms are an issue as well.
Authenticity of User	VoIP is vulnerable to registration hijack and caller ID spoofing. This could disrupt work and lead to identity theft.
Larceny / Stealing	VoIP Toll fraud, theft of data etc.
Voice Spamming	Unsolicited calls and stuffing of voicemail boxes.

Two of these vulnerabilities are discussed in greater detail below.

- **Denial of Service (DOS):** The motive of a DOS attacker is to overwhelm the service and force it to shut down and either cause large harm or demand ransom to stop the attack. Those of us who follow such news may be aware that during the 2012 London Olympics, the servers for the Olympic press agencies were subjected to a denial of service attack that flooded them with 300,000 packets per second. The servers had to be shut down and backups had to be activated. Coming to VoIP, TelePacific experienced a denial of service attack in 2011 when its normal levels of 34 million call initiation requests suddenly shot up to 69 million. Naturally all systems were overwhelmed and it became impossible to make even a single call. Mitigation of these threats requires advanced firewall handling skills and skillful analysis of network traffic. Many small businesses may not be able to afford these skills and could be very vulnerable to a denial of service attack. This is a major hidden cost as is the possibility of disruption of business.

In the traditional (POTS) phone system, there is a separate channel carrying administrative data about prioritizing calls and related information. Even if the calling lines are overwhelmed, administrative corrections can be undertaken.

In the VoIP scenario, network data is transmitted on the same infrastructure as the VoIP traffic and therefore network messages are also susceptible to be blocked in a denial of service attack.

- **Identity Spoofing:** While it is possible to spoof one's identity on a PSTN connection, it is far easier to do this on a VoIP system. This means that an attacker could be able to pass himself off as someone else and obtain information that he was not authorized to receive. The issue becomes more critical because a VoIP system is often connected to the company's internal information systems to provide an automated way of handling calls or providing information (e.g. billing or order processing details). If the sole authentication of the caller is via a caller ID, then the company could easily give data to the wrong person. The solution here is to decide which data is critical to protect and ensure that a secondary identification is looked for before releasing any information.

Cascading effect: Any impact on the telephone systems of an organization has a cascading effect on the overall system. It is one system that links all systems. Therefore companies would have to assess the impact of an underperforming phone system on their manufacturing, sales, marketing and accounts, and so on.

Implementing Basic Security

The fundamental step in setting up a VoIP system is to ensure that the network is divided clearly between voice and data. While the physical infrastructure will continue to be common, the network addressing scheme will differ for the two. It then becomes easier to control security threats (although technical management becomes slightly more complex).

> Many users do not reset default user names and passwords. Yet, they protest when their systems are broken into.

All VoIP equipment comes with login information already preset. All default user names and passwords can be found by a simple Internet search. In many cases, default user names and passwords continue to be used. VoIP equipment may also be left in an 'un-hardened' state by not shutting down services and ports that are not required. Researchers have been able to log in to company VoIP servers from the Internet with ease. Obviously hackers would be doing this as well. Phone vendors build the capability for a remote log in in so that they can log in remotely to solve any problems but there is no reason why this capability should be left open. Unfortunately, many times this is left unguarded with only the default passwords protecting the system. Once again it comes down to the knowledge of the company's IT staff.

Fax over IP

Using a Fax machine over the VoIP connection can be tricky and frustrating. Fax machines are designed to work over the typical PSTN lines and involve a system of communicating with each other to ensure what is sent is received at the other end. There are error correction mechanisms built in and these ensure that the fax systems work globally.

With VoIP, there can be gaps in transmission caused due to latency and jitter. This is particularly likely once the VoIP packets use the Internet to reach their destination. Fax machines connected to VoIP lines interpret gaps as end of message signals and terminate a connection. Building fax machines specifically for VoIP transmission is not a good solution because the machine at the other end could be an analog machine and this could cause further difficulties in communication.

While an individual using a home VoIP connection may not be much affected, businesses need rock solid fax and can be badly impacted if this cannot be achieved. The fax standard for using PSTN lines was evolved in 1980 and did not anticipate the Internet. In recent years, the T.38 subsystem has been evolved to handle this issue and it takes the standard fax signal and alters it appropriately (and adds redundancies) to ensure that it can travel over the IP network. At the receiving end, the process is reversed. Businesses looking to use fax over IP will need to ensure that their service provider offers T.38 and request their VoIP service provider specifically for fax over IP. Needless to say, there could be an additional cost that is not listed in the original VoIP proposal.

Limitations of VoIP Services

The limitations of VoIP are fairly clear, but sometimes things could be hidden in plain sight. Here are some limitations:

- **Internet Connectivity**: We may take it for granted, but the fact remains that connectivity to the Internet could fail, or be brought down by a virus or a power outage and suddenly the user could be left with a sleek phone that does not do much.

- **Sound / Video quality can sometimes be poor**: Much depends on the state of the infrastructure and the bandwidth you have hired. If the traffic is high and many users are using voice or video, then something has to give. Usually it is quality. While acquiring more bandwidth may solve the problem temporarily, the use of video may need to be permitted to only selected users.

- **Calling Emergency**: While a 911 call from a PSTN extension automatically informs the operator of your location, this is not so for a VoIP call. More often than not, the call could land on a supervisor line which may not even be manned all the time. This is

now being corrected with the Enhanced 911 service that attempts to put this right, but the work is still in progress. In the meantime, users cannot take 911 services for granted if they are using VoIP.

- **IT related ills**: Most bad things that can happen to IT networks and affect your computers will probably affect VoIP as well. This is why VoIP cannot simply be left to fend for itself once installed. It has to be managed and monitored.

Impact on Legacy Systems

Many legacy systems absolutely need an analog line to work.

There could be a number of machines tools in use in a company that use analog lines in their control channels. You will need to make sure that they can work using the new VoIP line. If the equipment is new it probably can, but if it is legacy, it is better to be sure.

In many cases alarm systems may not be able to work over VoIP and the alarm company you use may insist that you get an analog line to connect the alarm system to their office. There could be problems with point of sale devices and credit card readers as well.

This is one hidden cost that simply cannot stay hidden and if a company is forced to discover it later, it can certainly be career threatening. This issue must be resolved before the project for VoIP conversion even starts.

Does VoIP make Sense for Your Business?

The discussion so far could have turned off many readers. Why go in for VoIP if the hidden costs can be so high? There are several reasons why you will need to seriously consider VoIP in spite of all the hidden costs.

- The benefits are simply too large to ignore. VoIP leads very naturally to Computer Telephony Integration. In simpler terms, this means that your phone system and data networks can talk and accomplish work together. The simplest possible example is if a client wants to check her order status. Using an interactive voice response system,

she can check her ongoing work and make changes, alterations and special requests. The phone system works with the back-end database to make this happen 24x7 without any kind of operator assistance.

- Because VoIP is, after all, a data stream like any other computer communication, it can be manipulated by clever software programming, and great features that would have cost the earth in a PSTN environment become possible at very little cost. A user can move to any desk and log on to the phone system: calls to his number will find him there. Telecommuting suddenly becomes very easy and practical to achieve.

- Different extensions can be specified for day and night calls on the same number. Your voice response system can let callers select the language they prefer to use and connect them to appropriate people. All of this costs very little to implement.

- In any case, PSTN is on its way out. Another few years and businesses would be forced to switch because their legacy phone systems will no longer be supported. In France, for example, 95% of the calls are VoIP. Sooner or later other countries will achieve similar use rates – especially among the developed countries.

For these and other reasons on the same lines, it does make sense to plan a switch over to VoIP. Small businesses will find it makes good business sense to use a hosted VoIP solution rather than trying to manage one themselves. In this system, the VoIP server runs on a cloud platform and you simply hire a number of extensions. The user just needs to connect his phones to the Internet and ensure that he has sufficient bandwidth to support the service. All issues of server management, security, viruses etc. are handled by the service provider who could be handling millions of lines and therefore would be in a position to get highly qualified manpower to manage them.

Yet another advantage of a hosted VoIP system is the support it gives to business continuity. There have been cases where a natural or a manmade disaster has made premises unavailable or so badly damaged that working from there is impractical or unsafe. Businesses cannot afford to be cut off from clients, suppliers and retailers. You can move to any location – a motel for instance or another office – and log in using an Internet connection. Clients may not even come to know that you have had a business disruption.

Summary

There are a number of hidden costs to VoIP connectivity and use. While the basics are fairly straightforward, business-class connectivity requires more than a simple Ethernet jack to plug into a phone. You need to create an environment for the phone system so that it can give you robust services. This brings in hidden costs.

Being aware of the hidden costs and factoring them in before you go in for your VoIP solution is the only way to minimize their impact. This means a careful study of your requirements and using appropriately qualified staff to understand what the business really needs.

The writing is on the wall for copper lines. It is only a matter of time. Knowing VoIP and its costs – both hidden and visible – will help you make a controlled transition.

References

Computerworld article on differences between POTS and VoIP
http://www.computerworld.com/action/article.do?command=viewArticleTOC&specialReportId=741&articleId=98945

Hidden Costs and Savings of VoIP
http://www.computerworld.com/s/article/98933/The_Hidden_Costs_and_Savings_of_VoIP
http://www.economist.com/node/14214847

VoIP Security Vulnerabilities
http://www.sans.org/reading-room/whitepapers/voip/voip-security-vulnerabilities-2036

Frye, Emily, Staiti, Gregory (2005), "Hold the (Internet) Phone! The Implications of Voice-over-Internet Protocol (VoIP) Telephony for National Security & Critical Infrastructure Protection", I/S: A JOURNAL OF LAW AND POLICY, Vol. 1:2-3
http://broabandtrafficmanagement.blogspot.in/2011/10/telepacific-shares-details-of-ddos.html