

Telephone reliability for alarm notification: Where have all the landlines gone?

A white paper from Sensaphone

SENSAPHONE[®]
REMOTE MONITORING SOLUTIONS

Technology advancements continue to open communication without tethering users to a desk – mobile phones, BlackBerry®, Bluetooth® technology, and wi-fi access, to name a few. Such tools overcome traditional communication barriers like location and accessibility. However, does fast and convenient new technology equal improved reliability?

We all know the frustration and inconvenience of dropped calls. In fact, one mobile telephone network's advertising campaign even touts its service as the one with "fewer dropped calls." Also, with today's saturation of e-mail, full inboxes and bounce-backs can compromise electronic message delivery. In the case of an emergency, interrupted communication is far worse than a hassle. Lost time from bad cell phone or e-mail connections can escalate a minor problem to a much larger issue.

In the scope of IT, some scenarios can't afford any lost time. In emergencies such as blackouts, floods, air conditioning failures, etc., backup computer room systems activate automatically to secure data and maintaining operations, even if just for a short time. If equipped with remote monitoring capability, those systems notify appropriate personnel about the problem and the attention required, giving IT personnel the opportunity to respond quickly.

But what happens when loss of power affects modes of communication – like Internet access or cell phone coverage? This paper discusses why timely and reliable alarm notification is part of a successful remote monitoring program and discusses the factors to consider when selecting a remote monitoring system.

Introduction

Remote monitoring of computer rooms is necessary in today's fast-paced, electronic-based business environment. Whether part of a larger network or a simple single-room configuration, the computer network is the lifeblood of an organization and must be protected.

With billions of dollars invested in a network and invaluable information contained in its computer systems, large corporations recognize the importance of protecting their infrastructure and intellectual property. Smaller businesses, with consequently tighter budgets, must justify the expense. Suddenly, return on investment becomes the priority over protecting their business from data loss and downtime.

Big organization or small, regardless of where or how a network is secured, problems are bound to arise. As discussed in an earlier paper (see "Monitoring the Computer Room's

Physical Environment," a white paper from Sensaphone), numerous environmental conditions threaten a network's functionality and can lead to expensive downtime and repairs. With a remote monitor and alarm notification system that uses multiple notification methods, emergencies can be dealt with quickly, and businesses will see the greatest ROI possible.

Notification Options

A remote monitoring system detects a problem: the temperature in the computer room reaches the unsafe threshold; water on the floor is detected; an intruder enters the facility; or any number of scenarios. The monitoring system kicks in, alerting appropriate personnel.

Receiving alarms via mobile phones, digital assistants and other devices frees IT managers to concentrate on other duties in the building or off-site. Smart managers will program their alarms to activate well before levels become critical.

“Whenever we’re called, it’s for a good reason,” said Mark Burnfield, records manager for Jefferson County, Washington, northwest of Seattle. Jefferson County’s government uses a remote monitoring system for its computer room. That room houses multiple servers and the support equipment that maintains the county’s entire computer network infrastructure. The computer room is located adjacent to the phone switch closet and even shares some of the same equipment, making protection even more important.

“Nothing is ever classified as a false alarm because (the remote monitor) is doing what it’s supposed to,” said Burnfield, the person responsible for protecting the county’s records. “In two instances when the microphone picked up excessive noise, it turned out to be a custodian vacuuming the room. But it could just as easily have been a hard drive about to crash, so it needed to be checked out. It comes down to being a public safety issue.”

The county is also monitoring vaccine storage conditions at the health department, located in a separate facility in Port Townsend. Their monitoring system pings the network router at the health department to ensure it is properly functioning. If the router does not respond, Burnfield said, “the assumption is that the power is out. We have tens of thousands of dollars in medical supplies stored there, and they need to be taken care of.”

Because of what is at stake, Burnfield’s team set up multiple contact options, including cell phone, landline and email notification. Some IT managers favor mobile telephone notification alone, overlooking the importance and security of using multiple communication modes.

During the largest blackout in North American history in August 2003, an estimated 50 million people were without power, affecting eight U.S. states and one entire Canadian province. The economic impact is estimated at \$6 billion. The disruption lasted several days in parts of the affected area, resulting in many expired power reserves. For example, cell phone service reliability dropped as cell towers used up their reserve of backup

power. Some people resorted to charging their phones with car chargers, only to find limited access to the cell phone networks.

So how were people to communicate with one another? Technically, the backbone of the Internet was still operating during the power failure, but most people could not access the Internet. That's because unlike analog phone service (landlines), the Internet relies on intermediate hubs, switches and routers. An Internet connection can have many communication links between the user and the Internet backbone. Such links may or may not have backup power, and it only takes one link without adequate backup to disable an Internet connection in a home or business.

Analog phone lines, on the other hand, have a continuous path to the phone company, which provides the backup power, making it extremely rare for an analog phone line to lose service, even during a power failure.

When IT managers limit notification to a single mode of communication, they put their computer rooms at risk. Forgoing the use of an analog phone line as a backup communication compromises the overall effectiveness of a remote monitoring solution.

(Ironically, one of the main causes of the 2003 blackout was the failure of the alarm system to alert managers to existing problems. This finding came from the U.S.-Canada Power System Outage Task Force, the body responsible for investigating the incident.)

Think Out-of-Band

Alarm notification plays an important role in the remote monitoring process. The best-case scenario is that your communication system is operating problem-free. However, if you are relying solely on your network to send out notifications, a router or firewall malfunction or some other disabling of the network pathway could delay alarm delivery. It sounds logical to have a system of checks and balances in place, but many companies fail to plan for such scenarios — leading to a huge risk when it comes to response time.

Many companies make the wrong assumption that the computer network does not go down, ever. They invest a lot of money and time installing the best equipment and backup systems and tend to focus on equipment performance, with little or no attention given to message delivery in the case of a network malfunction.

Including an “out-of-band” communication system is a must for IT managers. This is a communication path that occurs outside the existing method and adds another layer of backup by providing server access through an alternate connection, typically an analog phone line. For computer rooms and data centers, out-of-band means a path that does not rely on the computer network. This allows managers to access the server even when it is not operating properly.

Without an out-of-band communication system in place, a remote monitoring system’s effectiveness is compromised. SNMP traps and email notifications rely on the network. If the network is down, the alarms are not sent and the potential exists for wider system damage and extensive data loss.

It’s recommended to build an out-of-band communication outlet into the remote monitoring system, and an analog telephone line, with its reliability, is the ideal backup. Like the network, the analog phone line delivers voice messages, emails, text messaging and faxes, depending on the preferred delivery method. But the analog phone does not rely on the computer network to deliver those messages, meaning it will function properly if power fails.

Receiving Alarm Messages

When it comes to receiving notifications, message delivery preferences vary, and team members have multiple delivery options to choose from. That flexibility virtually assures that if an alarm is sent properly, someone will receive it. Additionally, remote monitoring systems are programmed to continue sending out notifications until a response is received.

There are four main methods of receiving alarms, each with advantages and disadvantages. It is important to keep in mind that these will only succeed if they have a functioning communication path out of the building.

Pagers

Before the cell phone explosion, pagers were the easiest way to stay connected. Remote monitoring manufacturers developed new products with the pager capability built in, freeing IT managers from their desks. The technology worked well, but had one significant drawback – it was a one-way communication. While two-way messaging eventually became available, it was too late, as cell phones and email surpassed it in popularity.

Cell Phones

Initially, cell phones acted much like pagers, receiving calls from the monitoring system when pre-programmed thresholds were met. As cell phone technology advanced, a mobile communication hub was created, with more and more people using the devices for email communications and Internet access. The technology clearly expanded the capabilities of remote monitoring systems, enabling IT managers and others to respond from remote locations. Beyond the basics, cell phones (and landlines) can check status, turn equipment on or off, and even follow alarm response time by other personnel. Cell phones are effective and convenient, but reliability issues make it necessary to consider having a second form of communication in place.

E-mail

With the development of e-mail capability on cell phones, e-mail notification grew in popularity. It's typically quick, with a single programmed message taking only seconds to deliver. However, there is one potential flaw often overlooked by remote monitoring manufacturers. If your email server goes down, the email is not sent. E-mail depends on many hubs, switches, and routers to be working, and message delivery requires e-mail servers be operational. It's common to monitor both local networks and servers, but if a

crucial network component fails, or worse, the e-mail server fails, IT managers can't rely on e-mail to properly notify personnel.

The most reliable method of alarm notification is outside your network. You need the out-of-band reliability of an analog phone line.

Telephone

Analog telephones remain the most reliable communication tool for remote monitoring systems. Traditional analog phone lines, also known as POTS (Plain Old Telephone Service) lines, connect directly to the phone company's central office. All central offices have significant battery backup with additional generator power that can run almost indefinitely, one of the reasons why, during a blackout, an analog phone will work.

Additionally, the federal government, through the Federal Communications Commission, requires all local exchange carriers to submit full reports detailing maintenance and reliability of the analog service. No similar regulation is required for Internet paths, including e-mail.

Computer rooms and networks need to be protected, and the best, most affordable way to accomplish that is to install a remote monitoring system that includes an out-of-band communication option. It makes sense to have reliable notification processes in place to make sure that the right people receive the information they need in the least amount of time.

What to look for in a remote monitoring system

If you are in the market for a remote monitoring system, aside from the functionality of the system itself, there are a few important factors to consider.

- 1) **Scalability.** Can the system grow or change with your needs? If pricing is a concern, planning becomes more important and adds value to the initial purchase.

- 2) **Installation.** How difficult is the system to install? Is a team of experts spending multiple days to get the system up and running? Or is a plug-and-play option more valuable?
- 3) **Peripherals.** Take a good long look at the peripherals offered by the system manufacturer. Are the components designed specifically for that system or are they universal components? Have those components been tested with the system? Is another vendor needed to complete the transaction?
- 4) **Notification.** What are the capabilities of the notification system? Are landline, cell phone, email and pager notification options available? Does the system automatically cycle through the contact list until someone responds?
- 5) **Return on investment.** How much does the system cost, fully installed, and how does that compare to the equipment it is monitoring? For some applications, it may cost several hundred thousand dollars to replace damaged equipment, information, etc., should a system fail. Is spending a few thousand to protect that investment worth it? Or can you risk not spending the money?

About the author: Bob Douglass is the vice president of sales and marketing for Sensaphone, manufacturer of the complete line of Sensaphone remote monitoring systems. For more information, visit www.Sensaphone.com or call 610-558-2700.