

# Communicating in a Crisis

## What Really Works

A white paper by  
Harvey Fawcett,  
Siemens Insight Consulting



### Introduction

Crisis Management and Business Continuity professionals understand that effective communication before, during and after an incident can drastically alter the outcome of that incident.

When an organisation has determined the most effective mix of communications media, i.e. the means to communicate, it should apply sufficient attention to deciding what to say and when to say it, then design and implement a sufficiently robust testing and continual improvement process.

The communications industry has created an extremely wide variety of means to communicate, but each one has a number of characteristics that should be taken into consideration when planning to communicate in a crisis. In a crisis, the normal selection criteria may not be applicable or those criteria may take different priorities. Simplicity, ease of use, reliability under heavy use and basic effectiveness take on added importance.

This paper explains what commercially available communication systems really work in a crisis, drawing on real world examples of communication in both

large and small scale incidents. Specific information on how systems coped during the New York 9/11 attacks and recent London bombings is also included.

### Landline Telephone Threats and Issues

Traditional landlines still form the overall bulk of business and domestic communications capability. The Public Switched Telephone Network (PSTN), whether analogue or digital, is inherently resilient beyond local exchange level.

Widespread events such as flooding, chemical release or denial of access from disease control measures may result in essential maintenance not being carried out on these exchanges. This lack of maintenance may lead to a gradual deterioration in capacity and reliability.

The main threats to the PSTN capability from an organisation's perspective are power failure, equipment failure and damage to cables. Only the most serious events will create an overload condition but it can and does happen.

In a wide scale incident the PSTN can come under enormous stress, but all telecommunications providers have

comprehensive call management systems to ensure availability; the most generally used method is call gapping.

Call gapping prevents calls going into the network and is carried out at a local exchange level; the caller will hear a pre-recorded announcement and be urged to try again later. It is a valuable technique used to allow the network to function and can be visualised as a turnstile, allowing calls to enter the network at a controlled rate: so many calls per time period, with the rest being denied access, i.e. a busy signal.

Essential users such as the emergency services, government departments, hospitals for example, have traditionally had access to the Government Telephone Preference Scheme (GTPS).

The scheme is operated by BT and other carriers and categorises telephone lines into three levels; the top level being vital to protect the country's interests in the event of an attack and the bottom level being normal commercial or domestic.

The system works by giving priority to those at a higher level. Enhanced GTPS is being discussed and will enable organisations not traditionally eligible for the scheme to be included.

Although the actual communications infrastructure may cope, the ability to make and receive calls in a typical office may be impacted by issues such as power availability, hardware faults or simply the ability to cope with demand. For example, in a wide scale incident, calls to and from a typical office will peak dramatically as calls to and from relatives are frantically placed.

### **Recent Experience**

Recent experience in London in the aftermath of the Tube and bus bombings shows that most fixed line carriers experienced a doubling of traffic over the normal average for similar days. It is interesting to note that the providers plan for 4 times

normal traffic over New Year but, of course, there is a difference between a planned event and the events of the 7<sup>th</sup> of July 2005.

The overall telecommunications network is comprised of many organisations that cooperate closely through a number of forums to protect its overall integrity. This happened on July 7<sup>th</sup>.

It was agreed to introduce call gapping for those numbers beginning with 07, i.e. mobile numbers, to prevent too much traffic entering the mobile networks *from* the fixed networks.

The New York experience was slightly different because significant infrastructure was damaged (at 140 West Street, a major telecommunications hub) and this, coupled with the significant increase in traffic, resulted in widespread unavailability of the fixed network.

Faced with a significant increase in demand fixed telephone networks generally cope. Where massively increased demand, is combined with widespread infrastructure damage, as in New York, they are less likely to and it is impossible to guarantee.

### **Recommendations**

Organisations should consider power protection, maintenance contracts and other protective measures to ensure the availability of telephone equipment.

Those wishing to protect their landline communication capability from local infrastructure damage, for example damage to underground cables or building entrance facilities and exchange failure, can deploy independent routing of telecommunication circuits. This can be very expensive, but is often worth the investment for critical circuits.

Having diverse suppliers of telecommunications capacity can also enhance resilience, but they should be carefully deployed as many of these will use some, or all, of the incumbent carrier's infrastructure, sometimes even the same cable and therefore actually deliver very little resilience.

Large multi tenant buildings may also have separate cable risers and these should be used, where applicable, to provide cable resilience. Diverting mobile calls to a central office can dramatically increase traffic and this should be discouraged during an incident.

Organisations with multiple sites have traditionally looked at fixed links between sites to carry both voice and data traffic. These fixed links, whilst as susceptible to damage as normal telephone lines, are not affected by external traffic fluctuations and provide an excellent means of communicating between sites.

More dynamic voice networking systems may be prone to traffic fluctuation issues and organisations should closely investigate service levels and contract terms

Having a number of people able to quickly assume the role of telephone receptionists and technical procedures to enable this is good practice in order to increase an organisation's call handling capacity, as is providing standard 'what to say and what not to say' action cards.

Recorded message lines also form a valuable means of providing information to large numbers but check with the service provider about contention and maximum call connections to ensure that any system is appropriately sized.

### **IP Telephony Threats and Issues**

Resilience and recovery of IP telephone systems is different in the details but, not fundamentally different to other IP network systems. Given the appropriate contractual and technical arrangements these should perform as normal fixed landline systems.

Traditional digital or analogue telephone systems supply power to individual desktop telephone devices. IP telephones are no different; they still need power. This is delivered either locally through a power adapter or

over the network using Power over Ethernet technology.

In power fail conditions locally powered IP handsets will be inoperable unless local power protection is provided. Those using Power over Ethernet will remain operable only if the devices injecting power are also suitably protected.

Power over Ethernet devices draw considerable power; heat loads within communications cabinets and equipment rooms can be increased dramatically when deploying this technology. Overheating and loss of power are major threats to IP telephone systems

### **Recent Experience**

There is little practical evidence available to draw any distinction between the performance of traditional and IP telephone systems in a large scale event.

### **Recommendations**

Resilience and recovery of these systems is different in the details, but not fundamentally different to other IP systems. Given the appropriate contractual and technical arrangements, these should perform as normal fixed landline systems.

Traffic across IP networks will increase dramatically in a crisis as people turn to external web sites, make and receive calls over an IP telephone system and generate increasing quantities of email traffic. Bandwidth and capacity planning processes should ensure that critical services such as voice are not degraded during high traffic conditions.

Organisations should pay close attention to environmental and power protection systems, especially if they have been deployed into equipment rooms specified for traditional systems heat and power loads

Internet access also gives individuals access to public and private IP voice systems that use the Internet, for example Skype or Vonage.

Most of these types of service also allow the caller to break out into the public network. Providing key individuals, for

example crisis managers, with access to these services provides them with another means of communication.

## **Mobile Telephones Threats and Issues**

No one can dispute the usefulness of mobile telephones, as demonstrated by their widespread adoption. In a crisis they can be invaluable tools, but like any form of communication, there are issues that should be understood. There is also a great deal of misunderstanding about government imposed preference schemes restricting access.

Although using radio links instead of copper or fibre wires, mobile networks operate in a similar manner to fixed networks when under crisis conditions.

Any public network will be able to manage fluctuating demand and it is in the operator's interest to operate robust and reliable networks, but there are limits to the amount of traffic that can be carried.

There is a great deal of confusion about the ability of the emergency services to switch off mobile networks to reserve capacity for emergency service personnel. The technical ability to do this is written into the specification for GSM (Global System for Mobile Communication) networks. All GSM networks can apply access control. There are 15 levels of access with 10-15 reserved for essential users such as the emergency services.

In the UK, Access Overload Control (ACCOLC) is a control programme which the cellular radio network providers have agreed to implement at the request of the police or Cabinet Office to ensure that, in an emergency, the public safety services and other relevant authorities will have priority access to cellular radio systems which might otherwise become congested by non-essential users.

The police are normally the only authority permitted to invoke ACCOLC, which is designed only to support critical users at the scene of a major

incident. The key factor that people often misunderstand is that ACCOLC is only implemented at a local level, usually in a relatively small area.

It is also likely that in a crisis many of an organisation's staff will not be in the immediate area of an incident that requires ACCOLC because of exclusion zones and cordons.

When ACCOLC is invoked, only handsets with a SIM that has the appropriate access level can be used; all other SIM's will simply be blocked, except for 999 and 112 calls. Commercial organisations, generally, do not have access to these SIM's, although certain key individuals in critical commercial organisations may be granted access to these.

Threats can be categorised as those of availability due to network damage, overloading or deliberate restriction and those of miscommunication due to human factors. These human factors, such as misunderstanding or misinterpretation, are common with other forms of verbal communication, but can be exacerbated by overload measures taken by networks.

Mobile network providers are beginning to deploy 'push to talk' systems that allow mobile telephones to be used like walkie-talkies with very rapid call setup and group calling. This capability may be useful in certain circumstances, but there are a number of different methods that networks are using to implement this type of service; interoperability and billing issues are still yet to be fully resolved across all networks. There are also cultural issues around the intrusive nature of 'push to talk' calls.

Corporate mobile networks using call groups and short dialling codes will be equally affected by network loss.

## **Recent Experience**

As with fixed networks, mobile networks in New York on 9/11 were subject to both massive increase in demand and significant infrastructure damage. Again, in London the issue was traffic increase but not infrastructure, so the effects

were not as severe and were certainly shorter in duration.

In London on the morning of the Tube and bus bombings, the mobile networks were subject to unprecedented traffic volumes, for example Vodafone experienced a 250% increase in call volumes.

Call gapping and half rate encoding were implemented by some networks to alleviate congestion problems; a half rate encoding sacrifices call quality for call capacity but is only used at a local level. Call gapping, in a manner similar to landline networks, controls inbound traffic onto the network.

3G networks experienced less of an increase but that is due to lower adoption of 3G networks and handsets.

In the various papers and enquiries after both events it was made clear that commercial mobile telephone networks, whilst being very resilient and flexible, are not there for public safety but for personal and business communications. Organisations and individuals should bear in mind that massive increases in demand and/or infrastructure damage simply cannot be accommodated; there are commercial limitations to capacity and resilience and that user's should be realistic. Unfortunately, some emergency services found themselves reliant on mobile telephone for some communication; this caused problems as mobile network congestion increased.

In an analysis of the cold facts, the mobile networks in both incidents coped very well and traffic returned to normal levels by the evening or the next day. It cannot be ignored, however, that there were definitely issues with network availability and congestion.

In the aftermath of the London bombings, a decision was taken by the Gold Co-ordinating Group (the overall strategic command function), at 10.30am, not to invoke ACCOLC because it might have hampered the

rescue effort and it was thought that the value of allowing people to use their mobile telephones, thereby reducing panic, far outweighed any potential communication problems for the first responders.

There was also a concern that the relevant staff that might benefit from ACCOLC may not have had the relevant ACCOLC enabled handsets. The emergency services have their own radio systems and one (British Transport Police) had Airwave, a TETRA based trunked private radio system solely for the emergency services and selected commercial organisations.

O2 were requested by the City of London Police to invoke ACCOLC in an area 1km around Aldgate East, which they did from midday. There is still some controversy surrounding this; why the City of London Police invoked ACCOLC despite the Gold Coordinating Group deciding it was not required and only O2 were requested to invoke ACCOLC. It was removed later that afternoon at 4.45pm. O2 estimated that in excess of 1 million calls were blocked by this decision.

The network operators only authenticate the requesting force, not Gold Control; this may change in the future in light of this issue

It should also be noted that having an ACCOLC registered SIM does not do anything unless ACCOLC is actually invoked. If your organisation does have ACCOLC registered SIM's, the decision not to invoke may have an adverse impact on your communications plans, if those plans assume the invocation of ACCOLC.

ACCOLC was ,and is under review. The capability remains, but the likelihood of its use is becoming less and less. The increasing deployment of Airwave into the police and fire service, ambulance trusts, the MOD and other responders, is decreasing these critical organisations' reliance on public networks.

## Recommendations

The vast majority of incidents experienced by an organisation will not result in any issues with mobile communications whatsoever, therefore they remain a valid choice for communicating in a crisis.

However, organisations wishing to maintain communications during large scale incidents should be aware that mobile network capacity is finite.

The effects of mobile network congestion can be mitigated to some extent by spreading the networks in use, using different providers and 3G networks, especially for members of the crisis management team.

Encourage staff to keep mobile calls short, and where possible, use other means. Also clarify procedures for leaving messages and, if possible, call mobiles from a landline rather than another mobile.

## SMS Threats and Issues

Text messaging or SMS (Short Message Service) allow mobiles and computer devices to send and, retrieve simple textual messages up to 160 characters in length. Longer messages can be joined together or concatenation but this is not normally recommended in crisis situations, where brevity and clarity are important.

SMS messages are less resource intensive than mobile voice calls, so networks can better cope with increased demand. As they do not need both ends of the 'conversation' to be switched on or have adequate signal, the message has a better chance of getting through in very high demand environments.

Message delivery times may increase, but there is a very good chance of the message eventually getting through. Whilst generally reliable, there are very few providers able to provide absolute delivery time guarantees.

SMS providers can report on message delivery status although evidence of delivery does not confirm that the

message has been read, or perhaps more importantly, understood. SMS providers may use low quality, high latency routes in order to deliver low cost bulk marketing messages, but delivery is not guaranteed.

Text messages are persistent; they can stay in the network for many days until the subscriber's handset logs onto a cell. Whilst useful, this can also cause obvious problems. The message may be sent on Wednesday but might not actually be delivered until Friday.

If the message was time sensitive this time delay could have serious consequences and create confusion. It is therefore important to consider using a suitable message validity period.

Obtaining delivery receipt is relatively simple, but having a return path to elicit useful information such as estimated time of arrival is more complex. However, this is achievable and depends on the person receiving the message doing something after the message was received, not always reliable given the situations in which crisis messages are sent.

Flash messages can also be sent that are displayed immediately on the handset's screen but are not retained in memory when read by the recipient.

Cell broadcasting is a part of the GSM specification and allows localised delivery of text messages to all devices in a particular location, but this has not been implemented in the UK, primarily for commercial reasons.

Threats to SMS come mainly from network availability and performance, although communication can sometimes be problematical because of message length limitations.

## Recent Experience

Anecdotal evidence from New York indicated that SMS was the most reliable means of communication in the area although one should bear in mind the low general awareness of SMS at that time in the USA and it is still not as popular as in Europe. In the aftermath of the London bombings, most networks

experienced a significant increase in SMS traffic across the country and there were variable delays in message transmission.

### **Recommendations**

Text messaging is an effective means of communicating in a crisis, but time sensitive messages may not always be delivered in a timely fashion. It is particularly suited to broadcast or one-to-many communication, but having complex response mechanisms, whilst technically feasible, may not be suitable for critical use. Organisations should investigate text messaging transmission options and ensure that all staff are aware how to use these systems.

### **Paging Threats and Issues**

In the UK, pagers have recently fallen out of widespread commercial and public use; most individuals and organisations preferring to use a single device for voice and text messaging, i.e. the mobile telephone. This has resulted in the pager network being used for generally public sector and limited private sector applications.

Pagers are one way devices, at least in the UK, so their ability to enable 'conversations' is limited.

Paging networks are separate from mobiles and very efficient in their use of bandwidth. The message length is dependant on the type of pager and network, but is typically up to 240 alphanumeric characters. Threats to pagers generally come from network availability, although the paging networks are extremely reliable and long term or large scale outages unlikely.

### **Recent Experience**

Recent experience in the aftermath of the London bombings has shown that when public mobile telephone networks became stressed the paging network remained available and a viable means of communication.

This has led many organisations to reconsider pagers as a viable means of

communicating in a crisis, although their use will probably be limited to small teams.

### **Recommendations**

If an organisation wishes to communicate from a single or small number of control centres to a small team, they should investigate paging options as they offer an economical, extremely reliable and effective means of one way communication.

### **Fax Threats and Issues**

Fax messages use simple technology and when delivered are portable, needing no power if delivered to a fax machine, this is becoming less common in large organisations as network fax systems become more widespread. Delivery receipt is very easy to obtain but eliciting confirmation of action or message understanding is difficult.

Given that fax uses similar technology and transport systems as landline telephone systems, the threats of localised damage, power and availability are the same. If traditional fax machines are used, then issues such as paper bin capacity and message receipt notification may impact success. Where more advanced network systems are deployed, the availability of servers, desktop PC and software also adds to vulnerability. Fax is useful where signatures are required.

### **Recent Experience**

There is little evidence available to draw lessons on the practical effectiveness of fax as a means of communication during large scale incidents but fax is a simple and reliable technology that has been proven in many individual incidents.

### **Recommendations**

Fax messaging can be useful when broadcasting to numerous locations such as branch offices, but protocols should be in place at the receiving end to ensure that fax machines or network fax queues are monitored for messages.

Fax message remain an effective means of broadcast communication for small groups or individuals, but organisations should review device checking protocols

to ensure that messages received are actually viewed in a timely fashion and that confirmation of receipt is incorporated into communication protocols. This is especially important as the sender may not know whether the receiving equipment is faulty.

## **Email**

### **Threats and Issues**

Email is suitable for long and detailed messages and can be sent to large groups relatively quickly. Email is a robust means of communication as it is usually delivered over the Internet, an extremely reliable network. There are no delivery guarantees and obtaining return information, whilst appearing simple, is less so when dealing with large numbers, although the tools available for creating marketing email distribution can be used to great effect to track 'opens' and 'click throughs'

Email systems generally require Internet access or access to fixed communications networks and these are vulnerable to local disruption so alternative means of access should be investigated.

### **Recent Experience**

Where Internet access and local systems are available, email has proved a reliable and effective means of communication during all incidents, large scale ones included.

### **Recommendations**

Email is effective for both broadcasting to large groups and for operational communication between smaller groups, but the resilience of access to communications networks should be investigated and appropriate duplicate systems deployed.

## **Mobile Email**

### **Threats and Issues**

Many network providers provide email facilities for modern mobile handsets, Blackberry devices, mobile Exchange for Windows Mobile devices and other software allow individuals to stay connected to their corporate email infrastructure whilst mobile. These devices generally use GPRS (General Packet Radio Service) which is an

extension to the GSM network for data transfer. It is often referred to as 2.5G and can achieve realistic data transfer speeds of between 25 and 40kbs. GPRS has lower priority than voice traffic on the network, so connections may vary.

However, because the nature of connection is packet based, it does not need a continuous link like voice, so in practice it is a relatively resilient system. Mobile email systems often involve extra equipment and/or software at a central location and these may be vulnerable to power and availability issues

Roaming onto different providers' GPRS networks may be used, technical and commercial issues permitting, to achieve a degree of specific network independence. Business class GPRS networks are also available to further improve GPRS availability.

### **Recent Experience**

Blackberry devices were reported as being very effective in New York in the aftermath of the attacks, but only when the damaged mobile networks were restored. Similarly, after the London bombings many reported that Blackberry and similar devices were effective, but their limited deployment, even in many corporate organisations, means that their use for large scale communications will be limited.

### **Recommendations**

Mobile email is an effective means of communication but the transport mechanisms on mobile networks supporting it face the same issues of coverage and resilience in the aftermath of large scale incidents, these limitations should be considered in any planning activity. Systems deployed should also have the required level of resilience at corporate locations.

## **Internet (Web, IM, podcasting, web cams etc.)**

### **Threats and Issues**

The flexibility of the Internet provides a wide variety of communication media including instant messaging, podcasting, web cams, application sharing and others. As long as users are familiar with them, they can all be used

to great effect provided that access to the Internet is available with a reasonable degree of speed and availability. To improve resilience of Internet availability, many techniques can be deployed, from choosing different access methodologies to having simple backup systems and duplication.

Many metropolitan areas are now seeing an increase in free and commercial WiFi hotspot provision and these provide a valuable source of Internet connectivity for individuals and small groups disconnected from their usual 'base', but it is likely that these will become over subscribed at both the local access and network back haul level during a large scale crisis.

The web is a very efficient means of broadcasting communications and the simple addition of a news update on a corporate web site can be read by large numbers of staff, suppliers and other stakeholders. This single point of message origination can also combat misinformation and rumours propagating.

Web sites can therefore be an excellent method for informing staff of the current situation, what to do and other crucial information. Depending on the method used to publish web sites or individual pages, if they are to be used in a crisis management context, the means to amend them should be tested in realistic scenarios.

### **Recent Experience**

The BBC News web site received an estimated 115 million page impressions on the day of the London bombings. Organisations that deal with the public, for example and airlines, may receive a large number of web page hits in the aftermath of an incident.

LINX, the UK's and world's largest Internet exchange point reported no significant operational impact. LINX carries 90% of all UK Internet traffic and the Internet remained steady throughout the day. Instant

messaging was reported to have remained a viable means of communication. Intranets proved a reliable and effective means of communication to organisations' own staff.

### **Recommendations**

Whilst the Internet is a fundamentally resilient network, by design, it does suffer from vulnerability at the local access level. Organisations wishing to take advantage of these many forms of communication should ensure that sufficient attention is given to securing access to the Internet.

If highly skilled web designers are needed, they must be included in the crisis management plan, if content management systems are used, do the crisis management team have the relevant user names, passwords and ability to make changes? Testing of making these changes must be carried out in realistic scenarios.

If the expected audience for a web site in a crisis situation is predicted to create significant extra load, traffic management and capacity issues should be addressed.

### **Satellite Threats and Issues**

Satellite communication systems can be used in both fixed and portable configurations for both voice and data connectivity.

Satellite services provide a very high degree of independence from fixed communication infrastructures; some networks can route satellite to satellite handset calls without using ground based receiving stations, i.e. satellite to satellite. Some systems may be deployed as permanent backup systems that automatically provide connectivity in the event of main circuit failure or in rapid response type services where connectivity is available after a pre agreed period.

These VSAT type services generally use satellite dishes of approximately 1m diameter, although both smaller and larger dishes may be required depending

on location and bandwidth requirements. Although expensive, satellite services do offer excellent capabilities and bandwidth.

Some satellite data systems, typically provided as broadband replacements for rural areas, can also be used but these services are generally contended or shared between multiple users. This makes them vulnerable to unexpected traffic peaks, so organisations should look carefully at contract terms and technical configuration.

Small, hand portable satellite handsets are also available from a number of vendors on a number of different networks such as Iridium, Globalstar, Inmarsat and Thuraya. These typically use low earth orbit satellites to provide voice and data services.

Systems are also available to provide simple voice connectivity using fixed installation satellite equipment that allows satellite networks to be used with conventional telephone equipment, thus providing indoor availability and integration capabilities. Vehicle kits are also available. Interconnection to terrestrial networks and other satellite networks, of course, relies on those networks being available. Some networks provide enhanced data capabilities with VPN and Internet connectivity.

Extremely bad weather can create problems with satellite systems and portable equipment that uses low earth orbit satellite needs to have line of sight which may be difficult to achieve in metropolitan areas. Sunspot activity can also create problems for satellite services.

### **Recent Experience**

Many organisations had equipped themselves with small numbers of satellite handsets and invested in fixed installation systems. It was reported that these systems performed as expected during the aftermath of the London bombings.

### **Recommendations**

Both fixed and portable satellite systems do provide independence from conventional common fixed and mobile networks and therefore are a valid choice for critical applications, but organisations deploying these types of services should carefully investigate contract and technical issues to ensure that they are fit for purpose.

### **Conference Services Threats and Issues**

Audio conference services, self service and operator managed, are available from a number of vendors and provide an excellent means of communication in both the short term and recovery phases of an incident. Conferences can be at regular scheduled times or ad hoc as the need arises.

Conferences can be joined from either fixed, mobile or satellite devices and, as long as calls can be made, access to conference services should be available.

Organisations wishing to use conference services should request that their chosen vendor demonstrates their own network topology and resilience as this will have a bearing on overall service availability.

Conference bridges can also be purchased as a hardware solution and deployed inside the corporate network.

Audio conferences are normally accessed by a non geographic number using a 'room number' and PIN. Those expected to use these services should have ready access to this information.

Video conference services are available but these are generally confined to physical locations, because of connectivity and space requirements, although portable systems are available.

Web conferencing services that allow application sharing, remote desktop control, instant messaging and shared white board capabilities are available from a number of different vendors. Conference services either require Internet or telephone access (mobile or fixed) and, as long as this is available, conference services are reliable.

## Recent Experience

Conference services have proven to be reliable during the course of a number of recent incidents, as long as access to networks is available.

## Recommendations

As long as access to communication networks or Internet access is available conference services, whether audio, video or online, provide organisations with excellent communication tools.

Multiple providers will also provide some degree of protection from individual service loss.

## Summary

It is obvious and well documented that effective communications can mitigate the effects of any incident. Business Continuity and Crisis Management professionals know that their overall goal is to change the outcome of any incident by the use of effective planning, implementation of systems and processes and ultimately carrying through those plans and processes when needed. Underpinning all phases of an effective response is communication. Decisions made are done so on the basis of information. That information is usually communicated to those decision makers using the communication systems described above.

To encapsulate this advice:

Know what means of communication are available;

- Landline telephones
- IP telephony
- Mobile telephones
- Text Messaging (SMS)
- Paging
- Fax
- Email
- Mobile email
- Web (Instant messaging, web pages etc.)
- Satellite
- Conference services.

Know their capabilities and limitations, make sure people are familiar with them;

- Fundamentally, all communications systems are vulnerable to overload or damage, knowing where and how each type of communication system responds to overload and loss will inform the decision on what systems to use
- No one system is any more resilient than another or the universal answer to effective crisis communication
- Under no circumstances have systems that are *only* used in a crisis unless they are familiar to the users.

Use as many means of communication as possible basing those decisions on balanced risk and impact assessments;

- Uncertainty in a crisis is a fact
- Base risk and impact assessments on a degree of uncertainty and the characteristics of the means of communication, as described above
- Know what you want to say or are likely to want to say at all stages of a crisis
- Know who you will want to, or be likely to want to, communicate with
- When you know what you want to say and who you want to say it to, match that message/recipient to the communication media, not the other way around.
- Have diversity in communication resources, this is probably the most important single point.



Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Security
- Continuity
- Managed Services
- Compliance
- Identity Management
- Training

Siemens Insight Consulting subscribes to the ESG Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against BS7799 and are preferred supplier of services to the UK Government and are an accredited Catalist supplier.

If you'd like to find out more about how Insight could help you manage risk in your organisation visit [www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)

### Siemens Insight Consulting

Churchfield House  
5 The Quintet  
Churchfield Road  
Walton on Thames  
Surrey KT12 2TZ  
United Kingdom  
Tel: +44 (0)1932 241000  
Fax: +44 (0)1932 236868