



VCME (Virtual Crisis Management Environment) Security

MissionMode is a Virtual system that utilizes the Internet, Mobile networks, VOIP networks and legacy telephony infrastructures across the globe. It is a Ready-to-Go system which is not the same as other crisis management systems as it is highly secure from *both* the (a) electronic and (b) physical security viewpoint in comparison to others. This is especially true if other systems are Microsoft-based and not protected by hardened data centers.

The following criterion distinguishes the MissionMode security from a BCM viewpoint without providing significant IP or security information. Full details are provided with non-disclosure agreement signed.

MissionMode	Competition
A Mass notification system with customers having members ranging from 2 to 5 figures in numbers.	Most are not mass notification and unproven or must be used with other systems to achieve results.
Multi-channel Alerts with global customers have many different device types for each member. Customers geared for 6 figures in devices.	Most are not global and multi-channels are unproven in major alert circumstances across the globe or in Australia. They cannot meet professional BCM Service Level Agreements.
Bandwidth is greater and Overseas Internet speeds are much faster than Australian. The Thin Client at the user PC end produces only a Thin Thread of information to go to the MissionMode server to fire-off Alerts. It has minimal bandwidth requirements at the user end. The MissionMode Server is the Thick Thread that produces the bulk of the data processing and sending out of Alerts under the very fast bandwidth. There is no overhead at the Thin Thread user end.	Mostly 256 or 512KBS uploads and 1.5mb download speeds. The upload speed is paramount to send out Alerts when the emergency system is in-house. Sending out an Alert always has the Thick Thread at the PC-user end and always open to a single-point-of-failure (e.g. to 100 people with 400 devices requires a serious processing and Internet power). If hosting in Australia there are restrictions with the bulk of the data processing operations at the Thick Client Server end with very limited upload speeds. You always have a bottleneck with narrow broadband.

Test your own site now, click on the url:

<http://resources.broadbandguide.com.au/speedtest> & Click Begin

What are your Download and Upload speeds? _____

<p>Guaranteed Service Level Agreements 24 x 7 deliveries of alerts, messages, rapid content uploads no system downtime.</p> <ul style="list-style-type: none"> • Meets all corporate electronic and physical BCM requirements. 	<p>Competition</p> <ul style="list-style-type: none"> • Only a Yes or No? • If Yes, to what degree? • Is it good enough for corporate standards?
--	--

<p>Physically secure Hosted site</p> <ul style="list-style-type: none"> • Fully redundant • Hardened • Fail safe facilities <p>Data center in high security, hardened environment with redundant systems at the hardware, software, database, data and power levels.</p>	<p>Competition</p> <ul style="list-style-type: none"> • Only a Yes or No? • If Yes, to what degree? • Is it good enough for corporate standards? <p>Does it meet:</p> <ul style="list-style-type: none"> • ITC security requirements? • BC backup facilities if system goes down due to failure, power cut, bucket of water over it, etc. • Unsecured and sometimes shared data centre. <p>Unacceptable as a corporate standard.</p>
<p>Multiple high-speed internet backbone connections</p> <ul style="list-style-type: none"> • Ensures speed and SLA's are achieved 	<p>Competition</p> <ul style="list-style-type: none"> • Only a Yes, or no? • If Yes, to what degree? • Is it good enough for corporate standards?
<p>Highly secure non-MS operating systems</p> <ul style="list-style-type: none"> • Contractually Guaranteed 99.9% up time 	<p>Microsoft Windows Operating Systems technology</p> <ul style="list-style-type: none"> • Definitely unsafe and prone to many types of electronic attacks. • Attacked much more than any other system around. • Will not guarantee an exact up time. <p>Does not meet risk or BCM requirements</p>
<p>Operating Software upgrades are transparent to users</p> <ul style="list-style-type: none"> • OS upgrades are performed by MissionMode with zero electronic security risks • There is no concern for the users to be concerned with upgrades provided in a transparent manner • No extra costs 	<p>MS Windows Operating System now requires external software upgrades</p> <ul style="list-style-type: none"> • Automated updates by external downloads leaving the system wide open to electronic attack by Viruses, Spam, Spyware, Trojan horses and much more. <p>Product Upgrades are costly and time consuming</p> <ul style="list-style-type: none"> • Require professional services
<p>Extensive auditing recorded to meet:</p> <ul style="list-style-type: none"> • EU/US/AUS data privacy regulations • Legal corporate • Securities • Governance • Insurance requirements <p>Meeting Corporate Risk and BCM</p>	<p>Competition</p> <p>?</p>