



Secure Hosted Unified Communications Business Benefits Summary

Introduction Summary:-

Cybercrime cost the global economy an estimated \$445bn last year. It also estimated by the report that 150,000 European jobs were affected by cybercrime in the year, as well as 200,000 from the US.

Researchers collated estimates of both indirect and direct costs from governments and security firms, including loss of intellectual property, financial assets, and sensitive information, as well as missed opportunity, and the costs of protecting and recovering from cyber-attacks.

Financial losses are growing. David Burg, PwC's Global Cybersecurity Leader said cyber criminals evolve their tactics very rapidly and the repercussions of cybercrime are overwhelming for any single organisation to combat alone. The survey found that the US organisations are more worried about cybercrime compared to their global peers with 69% of US respondents reported they were worried about the impact of cyber threats to their growth prospects, compared with 49% of global CEOs.

Still Cyber Security has to be compliant and assured, it must also be delivered fast and implemented across technology platforms, and in this it must deliver both mobile and fixed security.

The UM Labs Security Software Platform as a Service (SSPaaS) combines a complete set of real-time communication applications with a high degree of assured and compliant security tasks (tested and certified this year by the Dutch/European Financial and Telecom authorities). The features needed include:

- Encrypted Voice and Video calls from mobile devices (smart-phones, tablets)
- Service implemented using proven protocols and security standards
- Encrypted calls from suitable fixed-line IP phones linked to a corporate phone system
- Ability to support encrypted calls between fixed-line and mobile devices
- Secure conference calls for fixed-line and mobile devices
- Secure Voicemail with encrypted access
- Encrypted text messaging
- Encrypted presence updates (providing ability to view colleague's availability status)
- Ability to interconnect with other UC services, for example Microsoft Lync.
- Optional call capture under the control of the end-user organisation
- Proven security controls to protect against denial of service and other cyber attacks

- Organisations must use the encryption services for highly sensitive information and can choose an in-house private cloud deployment, or a public cloud service operated by a trusted service provider. The opportunity for Government, Oil & Gas and financial institutions to gain cost savings with compliant security reduces the risk taken by the boards of these major corporates. This flexibility of running this all as a Hybrid cloud service will for example offer a hosted service based in a country where there is a risk of government sponsored call monitoring and need to protect against hacking.
- The ‘Encrypted’ communication spanning both mobile and fixed-line devices increases the service value by allowing mobile users to make secure calls to office based workers and allowing secure calls between offices in geographically separated locations. As this can be an emotive subject, one challenged by government subpoena or warrants, will need legal intercept ability and in this UM-labs compliance makes the grade.



Features for Inter-operation between technology:-

- The UM Labs service is not limited to secure voice calls. The service also provided secure video, instant messaging and presence between devices supporting those applications. The wider range of applications increases the value of the service. Most other services cannot deliver the full range of UC applications.
- The UM Labs solution includes mechanisms for enhanced integration with Microsoft's Lync. UC Platform. Lync is widely adopted by large organisations, mostly for presence and IM as the telephony features are difficult to integrate with other systems. The enhanced integration from UM Labs enables users of both mobile and fixed line devices to make calls to and receive calls from Lync users. All calls have end-to-end encryption. This feature adds value to the UM Labs solution by extending the secure reach to Lync users and helps organisations gain additional benefits from their investment in Microsoft Lync.
- Many organisations need the ability to capture and record selected calls. This can be for internal reasons, to meet local compliance and auditing requirements or to enable legal intercept. The UM Labs solution has this capability, but places it in the control of the organisation operating the services. Most other call encryption services do not provide this flexibility. Some services, in an effort to ensure call confidentiality, make it impossible to capture and record calls. This makes the service unsuitable for commercial use and may even raise legal problems for organisations using it.
- The UM Labs solution is unique in including security measures specifically designed to defend against the growing number of security threats that target Unified Communication applications running on IP networks. This is essential as systems lacking this protection are vulnerable to denial of service attacks which could leave the service inoperable or penetration attacks which could compromise call security and circumvent the encryption mechanism.

InformationWeek's 2014 Unified Communications Survey shows a revitalized market; 77% of respondents have deployed UC or plan to within 24 months. 81% plan to deploy security specifically for UC systems. 46% will use media encryption for voice, 54% say attackers accessing data network via UC is a big threat, so cost savings in reduced business risk, compliance with insurers so that corporate policies pay out and loss of trade or national intellectual property all add up to why UM-Labs Innovation in Cyber Security is a 21st century secure deployment, designed to secure all UC solutions and in this secure Inter-op between legacy IPPBX and new wave applications such as Microsoft Lync