Eavesdropping Protection Systems

Sound masking solutions to protect sensitive and confidential conversations

For more information, visit **www.biamp.com/eavesdropping**

THREAT ANALYSIS

When the area of concern is viewed as a six sided enclosure, the breach points can be easily identified; windows, walls, doors, ducts and utility penetrations. A properly designed audio security system protects against inadvertent and deliberate eavesdropping attempts.

- Laser listening devices are sometimes used to capture conversations from vibrations on window surfaces.
- Ductwork can be used to listen-in on conversations from several offices away or to hide listening devices.
- Doors are an obvious point of vulnerability for eavesdroppers or passers-by.
- Ceiling plenums and open return-air grills allow conversations to travel between rooms.
- Electrical conduit is a possible sound path exiting the secure space.
- Raised access floors are highly reverberant environments that can easily transmit sound between offices.

THE SOLUTION

Eavesdropping protection systems from Biamp prevent deliberate attempts to intercept private and confidential conversations. These solutions are regularly used to protect corporate intellectual property, mission-critical conversations, and national security.

TYPICAL BREACH POINTS PROTECTED

Doors: Door maskers provide protection from intentional eavesdroppers by applying low-level sound masking to the door surface, filling the gaps around the door and door frame with protective sound.

Windows: Windows present both visual and acoustical breach points. With only visual access to the facility, sensitive laser devices and parabolic microphones can capture conversations at great distances.

HVAC ducts: Metal ductwork creates a highly reverberant path that carries conversations far beyond the intended perimeter. Dynasound's duct masking devices are installed without any penetration into the duct it's self, masking conversation without impeding air flow.

Walls and Wall penetrations: Any utility penetration creates a breach point. Pipes and conduits may transmit sound from the secured space. Even without utility penetrations an unmasked wall can be vulnerable to contact microphones and listening devices.

Perimeter areas: In many cases the most effective way to prevent unintentional or accidental eavesdropping is to add conventional sound masking to the perimeter area surrounding the secured space.

Ceiling plenums and Raised access floors: Reverberant cavities above and below office walls can easily transmit sound from one space to another.

EAVESDROPPING SOLUTIONS

The breach points of most rooms can be easily identified. Windows are vulnerable to laser listening devices, ductwork can easily channel sound to adjacent areas and doors form an obvious weak point. Sound transmission through utility penetrations, access floor cavities, and above suspended ceilings can create a lack of confidential privacy.

Biamp sound masking products help safeguard those potential breach points.

DS1390 and DS1398

The DS1390 (70v) and DS1398 (networked) use dual, horizontally opposed speakers to produce uniform sound dispersion ideally suited for reverberant under floor cavities and shallow ceiling plenums.

DS2400 and DS2408

The DS2400 (70v) and DS2408 (networked) pipe, duct, and wall sound maskers are used to protect pipes, ducts, and walls against human and electronic eavesdropping by filling them with full bandwidth sound masking.

DS2500, DS2508, and DS2530

The DS2500 (70v), DS2530 (70v) and DS2508 (networked) protect windows, walls, and doors against human and electronic eavesdropping. DS2530 includes volume control and retractable cord.

9300 SW Gemini Drive
Beaverton, OR 97008 USA
Phone: +1 503.641.7287

biamp.com/eavesdropping