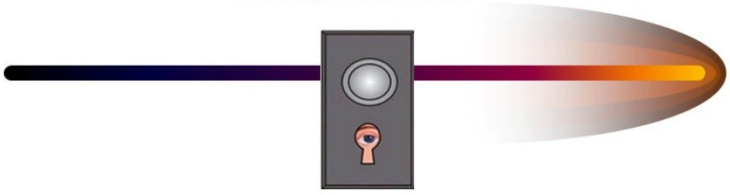
FullBlast technologies Inc.

Getting to know you



June 13, 2014

Accoustic Isolation and Electronic Interdiction.

There are two strategies generally employed to defeat hostile audio or video. The effectiveness of either strategy depends on the company's willingness to practice security and utilize tools and procedures designed to interdict or detect audio or video penetration.

Effective deterrence can be defensive or offensive.

Defensive. A defensive posture assumes mischievous penetration is possible and should be located and removed as soon after installation as practicable. This philosophy is classic and has been practiced for decades in government and private organizations. In decades past, listening devices and recorders were large in size. Infiltration of a bug required considerable expertise and technology. Very few actors had the funding or expertise to make corporate espionage viable. In the decades that introduced cell phones, miniature cameras and lithium batteries- things have changed dramatically. Cost is low relative to the past. Size has gone down considerably and features abound. Manufacturers produce spy gear because there is a market. Access to product has made corporate espionage a business option among companies with a low moral threshold.

The Defensive posture requires that security counter measures be conducted daily. Radio scans must be run to identify the presence of clandestine audio or video devices. Audio masking devices must run, during working hours in conference rooms and senior executive office spaces to render speech unintelligible, just in case listening devices were missed. Employees must be vigilant in the use of metal detectors, to interdict the introduction of cell phones, cameras, or recorders. Periodic checks of walls and ceilings must be conducted to scan for radio devices or non-radio recorders that may be brought in and later removed.

Procedures, which are not technical, but administrative ,also need to be a part of any defensive strategy. A security officer, responsible for policy adherence must ensure no one brings cell phones into the business offices spaces, particularly conference rooms or meeting rooms. The repair of computers, printers, air conditioners and office equipment generally, must be supervised by a security principal. Cleaning crews similarly must be escorted when working in the office space. Finally, office spaces need to be locked after hours and visitors during the day must be checked-in and escorted during their visits.

The final necessary measure involves periodic involvement of a security professional. This review involves a complete survey of the processes, a full technical sweep and an employee briefing on Security Awareness. Visits, twice yearly are recommended. Once a year is the minimum advisable.

Offensive. When technology made corporate espionage possible, executives began to look for ways to defeat hostile penetration with less disruption to operations. Counter measures were developed that reduced much of the overhead described in the defensive strategies above.

Security professionals offered that hostile penetration needed an objective. One wouldn't spend the time and money or accept the risks if there was nothing of value to obtain. Corporate Executives, capitalizing on this concept, turned the requirement around and Security went from defensive to offensive- ways were crafted to relocate "valued assets" into compartments that could be more easily secured. Rather than defend large floor spaces with considerable resource, many companies chose to install sound proof enclosures with proportional counter measures. The resources to manage a 100 sq. ft. enclosure is significantly less than the resources to manage a 5000 sq. ft. office space.

Offensive strategy is not without impact. This strategy makes it necessary to squeeze all sensitive discussion into the enclosure. For this to work, no one can discuss sensitive information in the remaining office space. For employees unaccustomed to this practice there is some pain initially. There is also the enclosure to consider. Some offices are too small and can't give up 100 sq. Finally, there is the expense of this enclosure. They are not inexpensive but neither is the compromise of sensitive information.

On the positive side. An enclosure is easy to inspect. It is easy to secure. It is easy to monitor and it forces participants to stay on task when they use the space. When properly used, a separate enclosure provides considerably less access and opportunity to those intent upon hostile penetration. Less vulnerability translates into greater security.

This implementation requires that sensitive information be compartmented and denies access to all but the few who have a need-to-know. Unlike the "open" philosophy of the Defensive Strategy, this technique is more restrictive. This implementation restricts sensitive discussion to a room that is not available to employees or residents, generally. The space is small and therefore manageable. This space is soundproof. This space is easy to scan for audio or video devices and its small size makes it easy to inspect. It is a stand-alone compartment that is electrically isolated and does not connect to any communications networks. What are we offering? A controlled environment. Inside this environment any classified or sensitive

discussions can be held without fear of electronic penetration because radio devices cannot get inside the enclosure. There is nothing inside the enclosure to tap or modify because there are no business machines inside the enclosure to manipulate. Employees carrying devices into the enclosure are caught at the sensors in the door that detect metal and radio signals. The enclosure is sound proof so only those inside the enclosure can hear what is being said.

What do you give up to make this discipline work?

a. Access to the enclosure will be restricted. When not in use, the enclosure will be locked. An alarm will be set to ensure there is no entry without authorization.
b. The enclosure can only be cleaned by authorized employees. Better still, let the employees do cleaning when necessary. The biggest source of compromise to any facility is listening devices "put down" by the cleaning force.
c. Participants may not take cell phones, cameras, or any electronic devices into the enclosure. Cell telephones are poison. They can be easily manipulated and with malicious software they can transmit or record audio and video. They can be used as beacons to identify your physical location and they can be hacked, revealing any personal information or corporate data that should remain private.
d. Laptop or desktop computers cannot be taken inside the enclosure unless they are dedicated to this mission, and, if so, they are fixtures in the enclosure and are never removed. For this to work the computers may be stand alone. There must be no signal continuity outside the box with any network such as with the Internet, servers, routers, etc. Files, drawings, photos, messages, etc will need to be copied to media and taken physically out of the enclosure. All media must be controlled.
e. There can be no telephones, fax machines, or appliances such as coffee pots, pencil sharpeners, shredders, etc. inside the enclosure. Any of these appliances can be manipulated. Work-arounds can be implemented so that capability is not interdicted but the technology needs discipline in order to work.
f. Regular inspections must be performed. The space is relatively small so inspections will be manageable. There will be meters to identify radio devices. The enclosure will also be assembled in a manner that makes physical inspection of all 6 surfaces possible. The absence of wires leading from the enclosure ensure there is no path for information exfiltration.

What is the cost? These numbers assume an enclosure 8'W x 10L'x 8'H. Size can change. Space should be sufficient to accommodate the number of employees that might be present at a meeting, briefing, etc.

1	enclosure	$	14,799.50
2	audio masking	$	231.95
3	RF sensor	$	195.00
	Sub total	$	15,226.45
	Fee 20%	$	3,045.29
4	shipping	$	2,474.00
	Total	**$**	**20,745.74**

Installation cost?

Transportation, Lodging, Expenses, Two days labor @ $80/hr.

What service do you get?

a. Functional enclosure
b. Setup, Testing, Training.
c. Help setting up procedures and process.

Not included?

Furniture, Unforeseeable necessities such as steps, ramps, locks, extra lighting.

Recommendation:

Purchase one or two units to test the concept. Work out the kinks and then purchase more as necessary.

Please contact the undersigned if questions persist.

Dennis Carroll

President, FullBlast Technologies, Inc.

dennis@fullblasttech.com