AUDIO VISUAL SCREENS IS SOMEONE WATCHING?

WHITE PAPER - JUNE 2016

Could the videoconferencing camera in your conference room be used to spy on you—even when it isn't supposed to be on?

Could someone potentially be watching and listening to you conduct business via the videoconferencing camera in your conference room—even when it isn't supposed to be on?

SECURITY

The importance of keeping videoconferencing cameras out of the room when not in use is underscored by at least two incidents in recent years.

The first came in January of 2012 when HD Moore—a security officer for the company Rapid7 which looks for security weaknesses in Internet of Things devices—was able to hack into videoconferencing equipment. He was able to control the cameras, panning and zooming all around the room.

According to a New York Times article, Moore found his way into venture capital, oil, law, and pharmaceutical companies. He even got into a courtroom remotely through the camera.

The second warning shot came at the 2013 Black Hat Europe, a security conference. During a presentation at Black Hat, Moritz Jodeit showed how to gain root access to video conferencing devices which could allow, among other things, a remote user to take control of the devices—including cameras and microphones.

DOES IT REALLY MATTER?

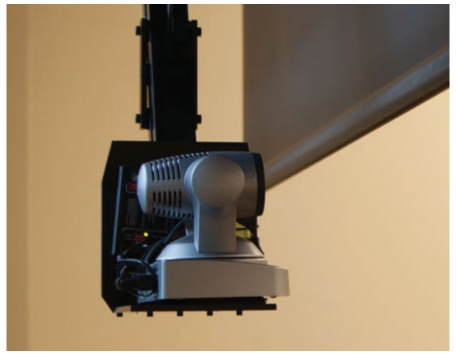
Of course, hijacking a webcam on someone's personal computer and watching in the privacy of a home or office is obviously an intrusion on personal privacy. Even the FBI director and the founder of Facebook are known to put pieces of tape over their laptop webcams for security. But peering into an empty meeting room through a videoconferencing camera isn't that big a deal, you might think. Or is it? Much damage can result from overheard business conversations.

One might also feel the possibility of a hacker gaining control of a video conferencing camera too remote to think about. However, there are many instances where privacy issues mean that any possibility is too much.

For example, by hijacking a videoconferencing camera in a law office, a hacker could eavesdrop on attorney-client conversations, and gain information providing an advantage in litigation. Delicate insider details of pending financial deals—the release of which could be harmful to the stock market—could be gleaned from prying into meetings at a financial institution. Sensitive medical details otherwise protected by HIPAA laws could be overheard and publicized or used as blackmail material.

(continued on next page)

Draper's Video Conferencing Camera Lift-Ceiling keeps the camera safely above the ceiling when not in use, and lowers it to just below the bottom edge of the viewing surface.



The VCCL-Ceiling in operating position.

COMFORT AND PEACE OF MIND

But having videoconferencing cameras in meeting rooms is more than a privacy and security issue. The popularity of video conferencing and the prevalence of cameras all around may make us less sensitive to their presence. For some, however, seeing that camera in the room can create, at the least, an uncomfortable situation and, at worst, trigger a panic attack.

Many people simply don't like the presence of a camera—although it simply causes a low level of discomfort, and perhaps (consciously or subconsciously) makes a person more guarded in her or his words. For some, however, it's more serious. The Social Phobia/Social Anxiety Association says 7% of us are affected by social anxiety at any given time. This can include Scopophobia, which is the fear of being stared at, or seen, or Fotografiki michaniophobia with is a fear of cameras.

WHAT'S THE ANSWER?

There have been a variety of solutions suggested and implemented to reduce the chance of hackers getting into videoconferencing systems. The main piece of advice is to make sure the camera—which resides on the network—is situated behind a firewall. Additional precautions have included making sure the lens cap is on when the camera is not in use, or implementing a software solution to protect the camera.

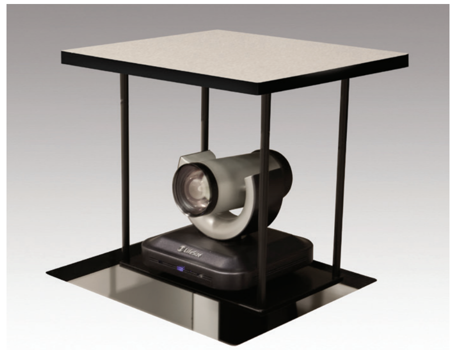
Draper, however, offers another, simpler solution that is effective in dealing with all of the above-mentioned objections to a videoconferencing camera in the room: take it out of the room when it isn't being used. Draper offers three solutions for getting the camera out of sight—and out of mind.

First is our Video Conferencing Camera Lift-Ceiling. The VCCL-Ceiling conceals the camera just above the ceiling, behind a recessed projection screen. When the screen comes down, so does the camera, lowered to the point where the lens can be seen below the screen. When the videoconference is over, both screen and camera return to their respective housings above the ceiling. The VCCL-Ceiling closure shuts once the camera is inside the housing, cutting it off completely from the room.

The Video Conferencing Camera Lift-Credenza provides the same function—keeping the camera out of the room and isolated—but instead conceals the camera below a table top, or in a piece of furniture such as a credenza.

In addition, Draper's Videoconferencing Camera Adapter Bracket lets you use any of our projector lifts to conceal a camera above the ceiling anywhere in the room.

The Draper VCCL-Credenza Lift hides the camera inside a piece of furniture. It can be made to custom fit any camera and blend seamlessly within any enclosure.



Credenza Lift close up.

CAN IT STILL BE HIJACKED?

Of course, since videoconferencing cameras work using IP and thus reside on a network, they can still be hacked into and possibly turned on. Using a Draper Video Conferencing Camera Lift, however, makes this a moot point. Even if the camera is on, it's out of the room, in a dark space.

Even if the VCCL is being controlled via IP, and so resides on the network as well, that doesn't mean a hacker can operate the lifts and bring the cameras into the room. That's because Draper's IP control solution involves translating serial commands to IP. There's currently no known way a hacker could get to the serial side and figure out the commands necessary to operate the lift.

The ultimate safety plan, of course, would be to simply operate the lift with a wall switch or remote control, so it isn't on the network at all.

Either way, the videoconferencing camera—and possibly prying eyes—will be kept away from the action, and people will no longer have to worry and wonder if they're being watched.

For details about Draper's line of videoconferencing camera lifts and other solutions, go to *draperinc.com/go/videoconferencing.htm*.