Fear and Paranoia! – Your House Is Unsecure (if you leave the door open!)

A [very provocative article ran in the January 23rd New York Times](#) entitled **"Cameras May Open Up the Board Room to Hackers."**

The subtitle of this article is "Flaws in videoconferencing systems make boardrooms vulnerable."

As I read this article it brought to mind one of my favorite quotes from HL Menken (and I'm paraphrasing here) that 'All complex problems have answers that are clear, simple and wrong.'

Would you call a house design "flawed" because leaving the door unlocked is a security risk? Would you call PC designs "flawed" if the users don't activate a log-in password? Would you call your credit card "flawed" if you leave it lying around so people can see the numbers?

At some point in every life endeavor the responsibility to ensure that we are secure belongs to each of us as individuals. There is no inherent flaw in a technically solid system that has been stupidly implemented.

Video conferencing and conference room multimedia systems have been deployed in bullet-proof, hack-proof condition thousands of times and for many years. I have personally designed rooms with features that many considered to be "over the top" because the application warranted the security. At one large financial services firm I designed a system where ANY incoming call to the room (voice or video) immediately muted all of the microphones and lit up a red beacon to indicate a call had come in. Some users found that experience "jarring" and I took some heat for that (especially when the incoming call was a wrong number) but I slept well at night knowing the kind of intrusion the Times article discussed was just plain impossible.

The video conference device itself (codec) made by most manufacturers is a sophisticated, fully secure device – but only if it is set-up that way. The article tries to blame Polycom for shipping their systems defaulting to auto answer. Car manufacturers' ship their cars with the doors defaulted to the unlocked position – do we blame Ford or Honda for stolen cars or stolen items because we didn't lock the door?

The reason so many video systems were found to be vulnerable is because so many video systems are designed and/or set-up by unqualified people. Many of the manufacturers and mom and pop resellers in our industry do not care about anything past the sale. My career often finds me visiting end-user rooms and systems where there is rampant dissatisfaction with (or low utilization of) video systems. I look at scrambled wires all over the tables and floor, microphones nailed to walls much too far away to pick-up anything and poorly designed and programmed video infrastructures and I try to figure out what the original installer was thinking when they did their work. This is the problem that the industry has to solve – not "flawed" video conference systems but rather flawed thinking in selecting inappropriate partners to design and implement modern, complex and powerful unified communications ecosystems.

End users need to find firms that don't talk about selling products but rather discuss solutions that are designed to meet their specific needs. Before letting any video manufacturer pitch their latest gizmo, organizations should engage a qualified consultant that can design a well thought-out strategic plan and ensure that it gets deployed correctly. Only then can the people in the boardroom relax knowing that not only have they bought the impenetrable door, but that someone has actually made sure that it was closed and locked.

+++

This article was written by David Danto and contains solely his own, personal opinions. David has over 30 years of experience providing problem solving leadership and innovation in media and unified communications technologies for various firms in the corporate, broadcasting and academic worlds including AT&T, Bloomberg LP, FNN, Morgan Stanley, NYU, Lehman Brothers and JP Morgan Chase. He recently joined Dimension Data as their Principal Consultant for the collaboration, multimedia, video and AV disciplines. He is also the IMCCA's Director of Emerging

Technology. David can be reached at David.Danto@Dimensiondata.com or DDanto@imcca.org and his full bio and other blogs and articles can be seen at Danto.info.