Subject line: Stay ahead of hackers to keep AV systems safe for all

Headline: Don’t let your classes get hacked – secure your AV and IT

Just as technology changes rapidly, so do the skills of those who would wreak havoc on your classroom or lecture room automation system. With a click of a mouse, a hacker can upload malicious code to initiate Denial of Service attacks, record audio and visual streams, establish new sessions for eavesdropping, even unleash a virus that could cripple a university’s entire network.

And access can result from something as simple as a student forgetting to log off a classroom computer or a professor not purging proprietary files or browsing history. Then there’s always the risk of some joker coed commandeering a camera or lights during a lecture.

The good news: There’s state-of-the-art technology, equipment and know-how to give you the upper hand. From using smaller controllers that can be locked away to reconfiguring AV equipment, your educational institution can limit exposure to internal and external hackers.

Learn how to stay a step ahead.