How Not to Respond to Hackers

We are seeing played out in public an excellent example of how companies should NOT behave when told about potential vulnerabilities by vulnerability assessors or hackers. Hackers have claimed that medical products made by St. Jude Medical, Inc. have serious security vulnerabilities. See http://www.krcrtv.com/news/national/st-jude-pacemaker-hacking-claims-absolutely-untrue/58974682.

St. Jude categorically denies there are any problems. I've seen this before. It is a foolish way to respond. Whether correct or not, a company's denial never seems believable even if the company is right (which it often isn't). A knee-jerk denial just enrages the original and other hackers, and eggs them on to further exploits. Moreover, claiming that there are no economic incentives for attacking medical devices is disingenuous and not a satisfactory reason to ignore potential security problems in any medical device.

Whatever the facts, a public accusation of serious security vulnerabilities in its products is not the time for the manufacturer or vendor to go into cognitive dissonance mode, nor is it the time for Public Relations Amateur Hour. Hackers, the public, the news media, and the relevant security issues have to be handled with a certain degree of sophistication, intelligence, and understanding of the culture and psychology of hackers. The response should be planned in advance, before the hack! Better yet, figure out your own vulnerabilities before others do!