KAUFMAN | DOLOWICH

Understanding Cyberattack Liabilities, *No Jitters, ft. Marc Voses*

Marc Voses, partner in the Kaufman Dolowich and Voluck New York City office, was quoted in an article by Martha Buyer that was published in *No Jitters on May 23, 2017.*

Be vigilant, and take corrective actions to keep systems up to date… or risk being sued.

Earlier this month cyberattacks dominated the news as 16 health care facilities (mostly major hospitals in the U.K.) lost access to patient data to hackers who demanded payment in exchange for its "return." Rather than simply creating a risk and inconvenience by accessing what was supposed to be secure, confidential information (read: credit card data) as previous hacks have done, in this case, the culprits placed lives in jeopardy because of the critical information they "data-napped." Sadly, in the case of this particular hack, Microsoft warned users of an identified vulnerability and provided a patch to address it two weeks before the attack.

Savvy IT professionals who stay on top of software patches and updates made patch installation a priority, while others, for any number of reasons, did not take those same steps. By not installing recommended software patches, attorneys for hungry and angry plaintiffs can easily make the argument that vulnerable entities were negligent by not taking prompt action. Inaction by IT staffs has created a wide open net for regulatory intervention and litigation, including potentially lethal class action suits, all of which can get very expensive, very quickly. And these costs start adding up only after an organization has already paid the ransom for its data.

And here's another important point. Many enterprises have now secured insurance against hacks and ransomware. While costly, these policies can be effective. However, as is always the case with such policies, knowing what's in the fine print including, most notably, where the exclusions are, is imperative. As is always the case, a network is only as strong as its weakest link. Marc Voses, a partner at Kaufman Dolowich Voluck LLP, warned specifically about this issue in a recent law journal article. In querying him about his statement, Voses shared me with via email: "If a company has told its insurance carrier that the most recent version of Windows is running but the company has terminals running Windows XP and that exposes the entire organization to a cyberattack like this, that's likely to be unacceptable under the insurance policy contract."