## Benefits and Traps of Data Exchange

By Vijay Mookerjee, Dengan Liu and Yonghua Ji

*Dr. Mookerjee, the Charles and Nancy Davidson Distinguished Professor of Information Systems and Operations Management, and co-authors Dengan Liu of the University of Alabama and Dr. Yonghua Ji of the University of Alberta pose the question: Is it better for firms cooperate with one another in a bid to secure sensitive customer information? The answer: It depends. Theirs is a working paper under review. For a copy, e-mail Dr. Mookerjee at* vijaym@utdallas.edu.

To explore the question, the relationship between the data stored at the two firms needs to be examined. When the data at two firms is *complementary*, a hacker needs to steal data from both firms so that it can be combined and sold in the black market. On the other hand, when the data is *substitutable*, stealing information from any one firm is sufficient.

In the complementary case, the firms have a natural incentive to share. However, in this case, the firms also *under-invest* in security technologies. Because each party benefits from the other's investment, the situation leads to the so-called "tragedy of commons."

In the substitutable case, the firms fall into a "prisoners' dilemma trap," in which they do not share despite the fact that it is beneficial for them to do so. Here, the beneficial role of a policy maker to encourage the firms to share is indicated. However, even when the firms share in accordance with the recommendations of a policy maker, they sometimes enter into an "arms race" by over-investing in security technologies. This is similar to two neighboring gas stations: if one makes its security tighter, the other automatically becomes an easier target for break-ins.

The research has useful implications for information security vendors to build products that can facilitate security knowledge sharing among firms. Policy makers also need to intervene with regulatory changes (for example, by providing tax incentives for sharing) so that firms make socially optimal investments (that is, neither under- nor over-investing) in security technologies.

***