New model of cybercrime factors in perishability of stolen data

March 10 2015

A new model examining cybercrimes adds an important way of examining the perishable value of stolen data so policy makers can plan against future hacks like the recent Anthem data breach, according to a study in the Articles in Advance section of *Service Science*, a journal published by the Institute for Operations Research and the Management Sciences (INFORMS).

INFORMS is the leading professional association for professionals in advanced analytics.

A Multiproduct Network Economic Model of Cybercrime in Financial Services is by Anna Nagurney, the John F. Smith Memorial Professor of Operations Management at the Isenberg School of Management at the University of Massachusetts Amherst. Professor Nagurney is an INFORMS Fellow. It describes a computer-based model that captures the network economics of cybercrime activity and permits the policy evaluation of interventions.

A novel feature of the model is its inclusion of the critical time element and perishability of stolen cyber financial products with, as in the case of fresh produce, the value (and, hence, the black market price) decreasing over time. It also identifies different demand prices for different financial products, with certain credit cards being more valuable because of credit limit, expiration date, and continent of origin.

Cybercrime exacts billions of dollars from businesses across the globe annually in theft and loss of revenue, as well as damage to reputation, opportunity cost, and disclosure of proprietary information. The financial services sector, in particular, has been a major target of cybercriminals, with cybercrime now the second most commonly reported economic crime affecting such firms. Through new Internet pathways, cybercriminals can attack remotely and remain undetected for months.

The new model includes the sources of financial products (the supply points) and the destinations (the demand points) in a powerful visual representation as a network, accompanied by the associated costs of illicitly acquiring the financial products, the transaction costs associated with finding consumers of such illicit products, and the prices at which they can be sold.

It models cybercriminals as economic agents who evaluate targets by the difference between the demand prices that the products (such as credit and debit cards) command versus the associated costs of stealing and transacting them. Financial service firms are modeled as prey and the hackers as predators. The underlying methodology used to capture such asymmetric interactions is "variational inequality theory," which examines multiple interacting agents on the supply and demand sides.

The network economic framework permits quantifiable evaluation of various policy interventions investigated in the study:

1. Determining the impact of strategies that make it harder to attack financial products' source locations (computer servers)

2. Evaluating ways that make it harder for cybercriminals to make transactions through the common technique of increasing transaction costs

3. Exploring changes in the demand price to evaluate greater or lesser interest in criminal products at demand markets

In addition, the study shows improved graphical network representation that makes it possible to quantify the addition or removal of demand markets and sources of financial products.

In subsequent research, the author is investigating extensions to this framework that include cybersecurity investments using game theory. These identify not only an individual firm's vulnerability but that of the industry as well. She is also studying supply chain networks' vulnerability to cyberattacks.

Provided by Institute for Operations Research and the Management Sciences

Citation: New model of cybercrime factors in perishability of stolen data (2015, March 10) retrieved 2 May 2024 from
https://phys.org/news/2015-03-cybercrime-factors-perishability-stolen.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.