# Researchers explore how cyber-attackers think like regular crooks

November 30 2011, By Missy Corley

In a unique collaboration, an engineer and a criminologist at the University of Maryland are applying criminological concepts and research methods in the study of cybercrime. Their work has produced recommendations for IT managers to use in the prevention of cyber attacks on their networks.

Michel Cukier, associate professor of reliability engineering at the A. James Clark School of Engineering and Institute for Systems Research, and David Maimon, assistant professor of criminology and criminal justice in the College of Behavioral and Social Sciences, are studying cyberattacks from two different angles - that of the user and that of the attacker. Both are members of the Maryland Cybersecurity Center.

Their work is the first look at the relationship between computer-network activity patterns and computer-focused crime trends.

"We believe that criminological insights in the study of cybercrime are important, since they may support the development of concrete security policies that consider not only the technical element of cybercrime but also the human component," Maimon said.

In one study that focused on the victims of cyberattacks, the researchers analyzed data made available by the university's Office of Information Technology, which included instances of computer exploits, illegal computer port scans and Denial of Service (DoS) attacks.

Applying criminological rationale proposed by the "Routine Activities Perspective," Maimon and Cukier analyzed computer focused crime trends between the years 2007-2009 against the university network.

According to this perspective, which is designed to understand criminal victimization trends, successful criminal incidents are the consequence of the convergence in space and time of motivated offenders, suitable victims, and the absence of capable guardians. The researchers hypothesized that the campus would be more likely to be cyberattacked during business hours than during down times like after midnight and on weekends. Their study of the campus data confirmed their theories.

"Our analysis demonstrates that computer-focused crimes are more frequent during times of day that computer users are using their networked computers to engage in their daily working and studying routines," Maimon said.

"Users expose the network to attacks," Cukier said. Simply by browsing sites on the Web, Internet users make their computers' IP addresses and ports visible to possible attackers. So, "the users' behavior does reflect on the entire organization's security."

Maimon, a sociologist, takes the study a step further.

"Your computer network's social composition will determine where your attacks come from," he said. In a similar vein, "the kinds of places you go influence the types of attacks you get. Our study demonstrates that, indeed, network users are clearly linked to observed network attacks and that efficient security solutions should include the human element."

Cukier adds, "The study shows that the human aspect needs to be included in security studies, where humans are already referred as the 'weakest link.'"

Cukier and Maimon said the results of their research point to the following potential solutions:

1) Increased education and awareness of the risks associated with computer-assisted and computer-focused crimes among network users could prevent future attacks;

2) Further defense strategies should rely on predictions regarding the sources of attacks, based on the network users' social backgrounds and online routines.

"Michel and David's research exemplifies the interdisciplinary and comprehensive approach of the Maryland Cybersecurity Center," noted Michael Hicks, director of the Maryland Cybersecurity Center. "Resources are not unlimited, so true solutions must consider the motivations of the actors, both attackers and defenders, as well as the technological means to thwart an attack. Michel, an engineer, and David, a criminologist, are considering both sides of this equation, with the potential for game-changing results."

Provided by University of Maryland