Organized Crime Research Brief no. 19

Ways to Measure Cyber-Fraud

BUILDING A **SAFE** AND **RESILIENT CANADA**

Cyber-fraud data is collected by a variety of organizations, including banks, regulatory agencies, and various police agencies. Often it is not collected at all. A study of offender network structures could be applied to methods of identifying hidden populations of cyber-fraud offenders.

Is cyber-fraud, in all of its manifestations, a serious problem in Canada? How does it compare to the frequency and costs of other kinds of crime? While there are many accounts of cyber-fraud documented in the electronic and print media, the frequency with which cyber-fraud occurs and the losses that result are extremely difficult to ascertain with precision. Canada does not have a uniform method of collecting data on cyber-fraud.

The primary goals of this study were to assess the potential for using innovative methodologies to estimate the scope of cyber-fraud, to identify existing data sources and gaps, and to suggest novel sources of data that may help provide an accurate and fulsome picture of the nature and prevalence of cyber-fraud in Canada. To this end, a literature review and interviews with police officers and individuals working in the field of Information Technology were undertaken.

Offender interviews may help uncover the network structure of hidden populations and help the law enforcement community identify key players within groups. Of the options available for researching hidden populations, a truncated Poisson model is suggested as the most effective model. Ideally, this research could help pave the way for data collection and analysis that would better inform law enforcement officials, investigators, and policy makers about the extent of cyber-fraud and cyber-criminal populations in Canada. This research may contribute toward the enhancement of prevention and suppression strategies, as well as the development of an empirical means for evaluating the effectiveness of initiatives, including elements of Canada's Cyber Crime Strategy.

It was suggested that a national data hub could be created to record and measure data relating to cyber-fraud across Canada. This entity might also conduct online surveys or polls of Canadians to gather information about cyber-fraud. A new national cyber-fraud tool could be used to collect data and effectively track cyber-fraud reporting. Effective cyber-fraud information is valuable for both police and policy makers. A central databank of known cyber-fraud offenders and cases across the country could facilitate the identification and tracking of suspects in cyber-fraud cases and could further the understanding regarding when one individual, or group of individuals, is committing fraud across the country. A national databank on cyber-fraud incidents could also give law enforcement officials a better understanding of the types of cyber-fraud being committed in Canada.

In addition to potential ways to measure cyber-fraud, respondents also offered other commentary. Cybercrime can, and often does, transcend national borders. The activities of an offender often result in the commission of a crime in multiple countries simultaneously. To address these complexities, attention could also be paid to: the harmonization of substantive computer offences in national legislation; the harmonization of procedural provisions relating to the investigation and prosecution of computer crimes; the establishment of cooperative relationships to facilitate the exchange of evidence, information and the extradition of suspects; and resources could be dedicated towards ensuring that courts are equipped to deal with complex inter-jurisdictional fraud cases.

Respondents suggested that an online database of best practices could be created that members of the

IT security profession could add to and view. Such a database could be augmented by an online community for IT security professionals that could e used to share advice and tips. Another possibility identified by interview respondents, is that best practice information sessions or conferences within specific industry sectors could be established to proactively respond to cyber-fraud threats, as well as gather information about current threats and vulnerabilities. These initiatives could improve the effectiveness of the IT security industry and police, as well as solidify relationships between police and IT security communities.

Finally, it was suggested that there needs to be more emphasis placed on educating Canadians on how to avoid scams. This could reduce the amount of monetary and other harms experienced by individuals, as well as corporations and insurance entities due to cyber-fraud.

Smyth, Sara and Rebecca Carleton. (2011) *Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources.* Ottawa, ON: Public Safety Canada.

For more information on organized crime research at Public Safety Canada, please contact the Organized Crime Research Unit at ocr-rco@ps-sp.gc.ca.

Organized Crime Research Briefs are produced for Public Safety Canada and the National Coordinating Committee on Organized Crime (NCC). The NCC and its Regional/Provincial Coordinating Committees work at different levels towards a common purpose: creating a link between law enforcement agencies and public policy makers to combat organized crime. *Organized Crime Research Briefs* supports NCC research objectives by highlighting evidence-based information relevant for the consideration of policy-development or operations. The summary herein reflect interpretations of the report authors' findings and do not necessarily reflect those of the Department of Public Safety Canada or the National Coordinating Committee on Organized Crime.