25. Training and Alignment of Supports for Local Police Departments for the Investigation of Cybercrimes

Description

Police departments face a broad range of duties in serving their local communities. The innovation of perpetrators, including forms of fraud against the public and especially businesses have increased demands on local police departments. Large, medium size and smaller police departments have identified a number of specialty teams required within their organizations. [1]

Cybercrime is a real and rapidly growing form of crime affecting our communities in which governments, businesses and individual citizens are targeted across Canada.

Municipal and rural police departments are increasingly strained to meet this rising form of crime and threat to the public and business community, both in terms of crime prevention and investigation.

Background

Cyber Crime is a rapidly growing and serious form of crime perpetrated at an alarming rate in communities across our country. Its victims are the people of our communities, local businesses, organizations and governments, and all “often face devasting impacts”. The offenders can range from international to extremely local, and “it often has links to Organized Crime or other criminality”. There are, however, identified actionable items at all levels of policing including increasing calls for “a collaborative approach” and a standardized form of “coordination” which has proven effective. Positive strides protecting our communities from cybercrime and fraud is possible “When police have the knowledge and skills necessary”.[2]

Police departments are faced with allocating time and resources of their already stretched staffing to best address this growing threat to the community. Once actionable items are identified, police departments experience difficulties “hiring, training, and retaining employees who are capable of handling cybercrime investigations”. Even when a department, of any size, identifies the need for such an allocation or specialization, “training programs and qualified trainers must be found.”[3]

The current coordinating body is the Canadian Anti-Fraud Centre, a “central repository for fraud information and intelligence in Canada and is jointly operated by the Royal Canadian Mounted Police (RCMP), the Ontario Provincial Police (OPP) and the Competition of Bureau Canada”.[4] Through its Call Centre and online reporting system, the CAFC amassed nearly 91,000 conventional and cyber fraud reports in 2022, “totaling losses of $530.4 million.” This figure represents a steady yet rapid rise from the total of $383 million in 2021.[5]An increasing method of choice of both domestic and international cybercriminals is the targeting of businesses, governmental and public organizations through a tactic known as spear phishing. [6]Spear phishing “attacks continue to produce larger losses, with fraudsters targeting businesses and organizations with nuanced email pitches and impersonating scams.” [7]

---

[1] Public Safety Canada, “Research Summary, Contemporary Policing Responsibilities,” (2017), (accessed June 3, 2024) https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-s006/2017-s006-en.pdf
[2] Canadian Association of Chiefs of Police, Executive Global Studies Program, CACP Global 2015, “An Action Guide on Cyber Crime for Canadian Policing”, (accessed June 3, 2024), https://www.cacpglobal.ca/images/pdf/CACPGlobal2015CyberActionGuideENFinal.pdf
[3] Police Executive Research Forum, “Critical Issues in Policing Series, The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime,” (2014) (accessed, June 3, 2024), https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf , 27.
[4] Canadian Anti-Fraud Centre “Annual Report 2022”, (2023) (accessed June 3, 2024), https://publications.gc.ca/collections/collection_2024/grc-rcmp/PS61-46-2022-eng.pdf 5
[5] “Annual Report 2022”, 3
[6] “Annual Report 2022”, 31.
[7] “Annual Report 2022”, 14.

Adding to the difficulty of investigations in this area, “Fraud investigations are often spread across multiple jurisdictions and borders, and individual fraud operations can target Canadians in every province and territory.” Currently, the CAFC “provides operational support to assist investigative efforts in collaboration with local police services and other partners in 811 instances.” The CAFC also manages the National Financial Crime Intelligence Sharing Group (FCISG), which “supports information sharing among police services and acts as a central point of contact in coordinating police investigations.” In 2022, the CAFC disseminated 370 articles of intelligence to FCISG members. In 2022 alone, the CAFC assisted in 40 instances of freezing and recovering funds, leading to the recovery of $2.9 million for victims of fraud. [8]

Recommendations

That the Government of Canada:

1. Provide resources to expand the expertise, local experience and data sharing practices of national/regional cybercrime structures.

2. Facilitate professional development opportunities, including specialized/advanced in-service training through the National Cybercrime Coordination Centre (NC3) for businesses and enforcement organizations.

3. Clarify roles and responsibilities of local, provincial and federal police agencies in addressing cross-jurisdictional cybercrime.

[8] “Annual Report 2022”, 13.