BUSINESS CASE

Cybercrime Officer

10/13/2021

Prepared by Karen Hira
Approved by DCC Laidman

Table of Contents

The Strategic Context

Problem Statement

The Victoria Police Department is unable to reliably allocate resources to cybercrime investigations or deliver targeted cybercrime prevention programs to effectively reduce the threat and impact of cybercrime, and reduce victimization by cybercrime in the jurisdictions it serves.

Business Need Summary

A coordinated response at the local level is essential to an effective cybercrime response. Based on the five strategic pillars outlined in the *Cybercrime Strategy* of awareness and education, enforcement, partnerships and collaboration, capacity building, and continuous learning, the VicPD proposes the development and implementation of a cybercrime unit to allow for the sharing of expertise and best practices to better protect the public interest, and to be proactive in the fight against cybercrime.

Background

Currently, cybercrime is broken into two primary categories: (1) technology as the target or (2) technology as the instrument. These are further broken down into different types of crime, as shown in the graphic below.

Cybercrime:

- ✓ New crimes leveraging new technology (e.g. ransomware, botnets, cybercrime as a service, crypto-jacking)
- ✓ Old crimes done in new ways (e.g. fraud, identity theft)

In 2016, a cyber-attack occurred (on average) every 39 seconds and was the second most reported crime around the world, accounting for more than 50% of all crimes globally (Cook, 2017). The World Economic Forum's (WEF) 2018 Global Risks Report includes cybersecurity threats as one of its four key areas. It predicts that cyberattacks will constitute the third largest global threat in 2018 and increase in priority over the coming years, with projected costs to reach $ 2 trillion annually (WEF, 2018; (Morgan, 2016).

As a result of a national Cyber Review, the development of the National Cybercrime Coordination (NC3)

Unit was announced to centralize cybercrime resources (Public Safety Canada, 2018). There maintains a need to develop regional and local units to ensure a collaborative multi-level response with varying degrees of responsibility at each tier, reflective of the resources and capacity available. Many municipal law enforcement agencies in Canada (Calgary PD, Edmonton PD, Vancouver PD, etc.) have developed and implemented internal cybercrime units to act as a supportive unit to various sections within their Department and informally liaise with provincial and national law enforcement and public/private agencies such as: Canadian Anti-Fraud Centre, National Child Exploitation Coordination Centre, Canadian Centre for Child Protection, BC Integrated Child Exploitation Unit, etc. These units are not formally coordinated with other municipal law enforcement agencies when completing cyber related investigations. These units may also perform Forensic Computer Analysis on seized computers, assist officers with capturing and editing digital video and still surveillance images; and assist officers with capturing IP addresses and social media information.

Current State

At VicPD, cybercrimes are currently investigated within the following divisions:

A. Investigative Services Division

I. Computer Forensics Unit

The CF Unit includes two Forensic Investigators who work with Investigators to assist in investigations related to child pornography, homicide, fraud, robbery etc. which involve a digital exhibit or digital item (cell phone, computer, etc.) that was seized, and subsequently a warrant was received. CF Investigators conduct mobile device and computer forensics to search the device to find evidence to corroborate a crime or confirm that a crime occurred.

II. Financial Crime Unit (FCU)

Although not dedicated completely to cybercrime, the FCU handles a number of cybercrimes related to frauds. The FCU includes three Investigators. The most common types of cyber-fraud complaints received by the FCU include: virtual kidnapping, identity-theft and credit card fraud, ransomware or cyber-extortion, crypto currency scams, and e-banking fraud. Currently, the FCU investigates few cyber-fraud incidents, as the Unit is only able to attempt to: freeze accounts, attain basic information, and track emails.

III. Special Victims Unit (SVU)

Currently there is one Internet Child Exploitation (ICE) Investigator within the SVU who collaborates with provincial and national partner agencies to investigate REDACTED in the Victoria area engaged in online child exploitation. ICE files are received from multiple points and may be generated in the following ways:

a. The National Centre for Missing and Exploited Children will send a file to the National Centre if the file is Canadian. From there, REDACTED the file is sent to the ICE unit within the corresponding province, and then to the corresponding city.
b. A direct report may be received from the front counter (i.e. complaint of sextortion). In these instances, a file is generated in Patrol and then sent to SVU for investigation.

c. [redacted]

d. [redacted]

e. [redacted]

B. Patrol Division

At the Patrol level, common cyber complaints include cyber-bullying, cyber-domestic violence, identity theft, threats on social media, fraud, extortion, and fraud via online photo check deposits. However, few files are investigated at the patrol level due to a lack of capacity and resources. Patrol members may engage in the following activities when confronted with a cyber-related incident:

a. Prevention and Awareness: Victims or Complainants are given information to better protect themselves in the future from similar incidents;
b. If exigent circumstances exist (fear of injury or death threats, suicide, etc.), Patrol members may access the Facebook law enforcement portal, query IP addresses, and seek a Law Enforcement Agency Exigent Circumstances Request from Shaw to acquire a GPS tracking location of a cellular device being used; and
c. Generate a file and forward it to the corresponding Unit (SVU, CFU, FCU).

Drivers for Business Need

Fragmented Service Delivery (within the VicPD and across jurisdictions): presents a significant barrier to effective cybercrime response. Municipalities are currently operating in silos and there are no processes or point personnel to engage with at local or national levels when cooperation or additional information is required for files that go beyond jurisdictional boundaries.

Impact of Technological Change and Capacity for Criminals to Adapt: New types of cybercrimes are constantly surfacing, and old technologies are quickly unable to address emerging trends and threats. For CFU Investigators, the software required varies depending on the device, and with the consistent introduction of new devices or updated devices, the unit is unable to successfully keep up technologically or financially to upgrade software and equipment on an ongoing basis. Perpetrators that engage in online child exploitation are also very adaptable to software being used to identify them. They are effectively able to protect their devices, and/or operate on 'darknets', increasing resources, capacity, and personnel required to identify them.

Inability to Keep-up with Scope and Prevalence: According to CPS - the Child Protection System, there were 84 unique IP addresses seen on the system downloading and sharing Child Pornography files that geo-located to the Victoria area in 2018. The ICE Investigator was only able to investigate two of these IP addresses (amounting to roughly 2%). As a result of increased use of mobile and computer devices among all demographics for a wide variety of purposes and the introduction of new internet communication devices (i.e. smart watches), more and more investigations require mobile and computer forensics and/or have a cyber component causing a significant workload for Forensic Investigators. Additionally, FCU investigators are dealing with more and more frauds that affect thousands of consumers and are rapidly increasing in prevalence, complexity, and reach. Currently, the FCU is barely scratching the surface while the scope and prevalence of cyber-fraud and the economic losses of cyber-fraud continue to increase at an exponential rate.

Lack of Capacity: The CFU and FCU do not currently investigate a significant number of cybercrimes, as these units simply do not have the capability, experience, or training to do so. While the CFU Forensic Investigators conduct mobile device and computer forensics, they do not have the software or training to search the internet. This presents a significant barrier to investigating cybercrimes. At the Patrol level, files are being closed without investigation because many members struggle to navigate these files. There is a steep learning curve as a result of significant discrepancy in capacity among frontline members due to a lack of knowledge and training related to cybercrime.

Lack of Clarity Regarding Responsibilities: There is currently a lack of clarity regarding responsibilities at the local, regional, national, and international level making it difficult to navigate files, leverage local and national resources, and develop a coordinated approach. A lack of policies and regulations also inhibits the development of clearly defined roles and responsibilities. Departmentally, VicPD lacks coordinated internal processes that aid members in navigating complaints based on what they can realistically accomplish, taking into consideration capacity, resources, and time at various levels.

Resource Restraints: The majority of cybercrime files are time consuming due to the fact that they are complex, span jurisdictional boundaries, and require ongoing collaboration with local police agencies and provincial, national, and international centres causing an extensive investment of time per file. In addition, most files require Production Orders and search warrants which can take from days to months to acquire. Competing priorities and limited resources also restrict the time that can be spent on cybercrime cases, as other high-risk files must be prioritized.

Lack of Public Awareness and Prevention Efforts: Research indicates that 80% of cybercrimes are preventable and targeted interventions aimed at behavioural change and education of risks is paramount (Airmic, 2018). However, the majority of VicPD's efforts are currently focused on reactive policing of cybercrimes rather than prevention. In addition, VicPD does not currently have dedicated personnel or a dedicated unit and resources to deal with cybercrimes, and as such there has been limited public awareness and prevention efforts to target vulnerable populations.

Administrative Barriers: Administrative barriers related to court processes, case law that impacts how evidence is investigated and seized, process and time required to obtain Production Orders and search warrants, disclosure and digital evidence protocols, etc. do not align with the speed and adaptability of cybercrime. Many of these processes are also attempting to catch up to the scope and prevalence of cybercrime, and as such have not adapted their processes to respond to the needs of law enforcement to be effective in their investigation of cybercrimes.

Risk Assessment

The risks of not establishing a cybercrime unit include:

- Scope and prevalence will continue to expand
- Inability to deliver targeted prevention efforts
- Burnout and risk to employee wellness
- Ineffective investigative responses to public complaints
- Increased local financial losses
- Inability to share knowledge and leverage resources

Risks associated with the establishment of a cybercrime unit include:

Risk	Description	Mitigation Strategy
Scope of Work is Unpredictable	As cybercrime is an emerging trend, it is difficult to estimate the scope of work that the unit will be inundated with once it is up and running.	• Establishing a clear unit mandate; • Clarifying the scope that can be handled by the unit at a local level; • Clarifying responsibilities of unit members; and, • Reducing unit liabilities through the development of a comprehensive SOP. • Phased in approach to a Cybercrime Strategy.
Increased Financial Commitment	Ongoing training and infrastructure costs are unknown. These costs may also fluctuate depending on the various types of cybercrimes that are trending and prevalent in the jurisdictions served.	• Re-allocating internal resources; • Coordinating training with area departments; • Diversifying funding through various provincial and federal grants; and, • Pooling infrastructure.
Taking on Files Without Appropriate Resources	Despite the establishment of a cybercrime unit, the unit will still not have the capacity to take on certain types of files unless the unit is able to join a greater regional or provincial unit.	• Strengthening relationships with outside agencies; • Developing clear communication lines and communication processes with stakeholders; • Engaging in resource and knowledge sharing at all levels; • Developing clear processes to coordinate files across jurisdictional boundaries; and, • Clearly defining reasonable scope at municipal level in SOP.
Assuming Risk Beyond Municipal Level	Cybercrimes and cyber-threats often impact multiple jurisdictions. The risk of duplication or jurisdictional overstep can occur if the correct communication	• Clearly defining reasonable scope at municipal level in SOP; • Building MOU's with other law enforcement agencies to ensure

	channels and areas of responsibility are not established	responsibilities are clearly defined; and, • Establishing collaborative relationships to share knowledge and information.
Increased Public Expectations	The establishment of a cybercrime unit may increase the public's expectations of VicPD in regards to cybercrime investigations. The public may perceive that the development of such a unit indicates capacity to investigate all forms of cybercrimes regardless of their complexity and scope, resulting in unrealistic expectations.	• Consistent and coordinated public messaging; • Targeted prevention and awareness presentations to individuals and businesses; • Clear communication on unit mandate, priorities, resources, etc.; • Ongoing and mutual dialogue; and, • Monitor, evaluate, and report achievements, barriers, and outcomes to public.

Recommendation and Resource Requirements

Recommended Option

Create a fully integrated cybercrime unit, phased in over two years with the following structure: Integration of Computer Forensics Unit (CFU) & Internet Child Exploitation (ICE) unit. Addition of a Cybercrime Sergeant, Cybercrime Constable, one ICE Investigator, and one CFU Investigator. Currently, CFU is in place with two Forensic Investigators and we have one ICE Constable in the Special Victims Unit.

This model would provide baseline cybercrime capacity at a regional level with the participation of municipal police agencies only. The model would also create a workable integrated unit structure, add some capacity in areas where there is currently little or no capacity, and provide additional CFU capacity that will be needed to support the additional investigators. While we believe this model is a good start, the plan will be updated as needed in response to changing conditions.

Resource Requirements

Short Term: Addition of a Cybercrime Officer

	2022 Impact				Full Year Impact (2023 On)	
Estimated Date	One-Time[1]	Ongoing (prorated)	Total	% Impact on Budget	Ongoing	% Impact on Budget
May-22	10,000	117,560	127,560	0.22%	176,333	0.30%

The role of the officer would, in the first year, be to focus on prevention and capacity building. This would be achieved through the development of partnerships and collaboration at the national, regional and local levels with various stakeholder groups to increase awareness and education.

Additionally, the officer would perform a full assessment of current and potential capacity to determine the resource needs, level of integration, and strategic priorities for the unit.

Long Term: Establish an Integrated Cybercrime Unit

The longer-term strategy is to develop an integrated Cybercrime Unit with other police departments in the region. Specifically, any remaining staff positions left outstanding after year one will be filled in year two. The benefits of a regional approach include better knowledge-sharing, increased capacity and the ability to establish centres of expertise. It should be noted that, with or without the establishment of an integrated cybercrime unit, the position has a direct benefit for VicPD in being able to focus on prevention of, rather than reaction to, cybercrime in our municipalities.