Cyber Incident Investigation Support – Victim Engagement Questions from Law Enforcement

The following questions are to be provided to the victim companies\complainants regarding a data breach, where an extortion demand has been made for a payment to be made in order to restore encrypted data, or the promise not to leak the stolen data.

Each incident is unique however, the answers to these questions will assist Law Enforcement in their criminal investigation.

The individual providing answers to these questions should have first-hand knowledge of the incident and the steps being taken responding to the incident.

The earlier these questions can be answered and returned to Law Enforcement the better, to try to ascertain the threat actor(s) involved.

Important Note: Context and rationale associated with the information requested through the questions that follow is provided in ANNEX section at the conclusion of the document. This supporting material is intended that both the querying law enforcement official and receiving organization may share a mutual understanding of why the questions are being asked and how provision of information can support law enforcement actions to reduce cybercrime.

PHASE ONE REPORTING INFORMATION (sections can be left blank if required)

A. Information relating to the reporting individual/complainant

1. Are you, as the individual reporting this incident, the primary point of contact for police for future related discussions?

i. If not, who is the primary point of contact for police to follow-up with relating to this reported incident?

2. Key contact information for the primary point of contact

i. Name

ii. Professional role and/or title (if affiliated with the organization impacted by this incident)

iii. Contact phone number and email address

3. Are there any confidentiality concerns you would like to raise relating to your reporting of this incident? (i.e., concerns that would impact you personally, professionally or jeopardize your safety)

4. What is your association to the incident you are reporting?

B. Information relating to the victim of the incident

1. What is the official name of the victim organization impacted by this reported incident?

2. What is the associated corporate address of the victim organization?

3. Where is the physical location of the site where the incident occurred? (Example – where the impacted servers are physically located)

4. Is there a physical presence of the impacted organization in other Canadian and/or international jurisdictions?

C. Key details outlining the incident

1. As you are best able to at this juncture, please provide a high-level description of how the incident has impacted the operations of your organization.

2. Please describe the timeline associated with your (and/or the victim organization's) first awareness of the incident, and any other points in time leading to now, which you feel are noteworthy to provide key context.

3. Are there any significant consequences of impact you feel are important for immediate consideration relating to this incident? (Example – related threat to public safety, financial impacts, downstream supply chain impacts and/or impacts to critical infrastructure and services)

D. Threat vector details (can be left blank if not known at this time)

1. To your knowledge at this time, has there been any contact between a threat actor associated with this incident and any representative(s) – including yourself -from the organization?

2. **If no known contact with the threat actor -** Given the nature of the incident that has occurred, and assuming there has been no known contact to date, if there was an individual or section of the organization that may have encountered or interacted with the threat actor, are you able to provide that person's name and contact information?

3. **If there has been contact with the threat actor:**
   i. How and when was this contact first engaged?

ii. Have there been multiple instances of contact?

iii. Who have the known instances of contact been with?

iv. Are you aware of any upcoming future contacts?

E. Other incident related information not yet provided

1. Is there any other information not yet covered which you feel is important for police to be aware of at this time in relation to this incident?

F. Key contacts information of other parties involved

1. Are you aware of any other external parties to your organization that have been contacted in relation to this incident? (Example – law firm/breach coach, 3rd party cyber incident response provider, Canadian Centre for Cyber Security, insurance company, bank, etc.)