Assignment

for

HUM 4741: Business Communication and Law

on

The Digital Security Act 2018
A Case Study

Tasnimul Hasnat

19004113

November 22, 2023

Answer to Question 1

Specific Offences Under the Digital Security Act 2018 Attributed to Cipher's Actions

Cipher's actions can be categorised under several specific offences as per the Digital Security Act 2018. These include:

I **Illegal Access to Critical Information Infrastructure (Section 17):**

Cipher compromised critical sensitive information stored in the government database for citizens which is a clear violation of this provision, which criminalises unauthorised access to any critical information infrastructure.

II **Illegal Access to Computer Systems (Section 18):**

Cipher's unauthorised access to a government database is a clear violation of this provision, which criminalises unauthorised access to any computer system with or without intent to commit further offences.

III **Unauthorised Use of Identity Information (Section 26):**

Since Cipher has gained access to sensitive confidential identity information stored in the government database, it constitutes an unauthorised and illegal collection of data.

IV **Offence Related to Hacking (Section 34):**

Cipher's actions fit the definition of hacking as they involve unauthorised access and potential damage to digital systems, a serious offence under this section.

The categorization of these offences under the Digital Security Act 2018 underscores the Act's comprehensive nature in addressing various forms of cybercrimes.

Answer to Question 2

Potential Punishments for Unauthorised Access and Data Extraction

The potential punishments that Cipher could face for unauthorised access and data extraction based on the relevant sections of the Digital Security Act 2018:

I **Illegal Access to Critical Information Infrastructure (Section 17):**

- If Cipher's actions fall under clause (a) of sub-section (1), he could face imprisonment for a term not exceeding 7 (seven) years, or a fine not exceeding Taka 25 (twenty-five) lac, or both.
- If Cipher's actions fall under clause (b) of sub-section (1), the potential punishment could be imprisonment for a term not exceeding 14 (fourteen) years, or a fine not exceeding Taka 1 (one) crore, or both.

II **Illegal Access to Computer Systems (Section 18):**

- If Cipher's actions fall under clause (a) of sub-section (1), he could face imprisonment for a term not exceeding 6 (six) months, or a fine not exceeding Taka 2 (two) lac, or both.
- If Cipher's actions fall under clause (b) of sub-section (1), the potential punishment could be imprisonment for a term not exceeding 3 (three) years, or a fine not exceeding Taka 10 (ten) lac, or both.

III **Unauthorised Use of Identity Information (Section 26):**

Cipher could face imprisonment for a term not exceeding 5 (five) years, or a fine not exceeding Taka 5 (five) lac, or both.

IV **Offence Related to Hacking (Section 34):**

Cipher could face imprisonment for a term not exceeding 14 (fourteen) years, or a fine not exceeding Taka 1 (one) crore, or both.

In summary, Cipher's actions could lead to charges under multiple sections of the Digital Security Act 2018, and the potential punishments would depend on the specific clauses and sub-sections applicable to each offence.

Answer to Question 3

Addressing Compensation for Victims

The Digital Security Act 2018 addresses compensation for victims of cybercrimes in Section 37. This section grants the Tribunal the power to issue orders for compensation when any person causes financial loss to another person through specific cybercrimes. Here is a breakdown of how Section 37 operates:

- **Scope of Compensation:** Compensation can be sought for financial losses caused by digital or electronic forgery, digital or electronic fraud, and identity fraud or personation.
- **Authority to Issue Orders:** The authority to issue orders for compensation lies with the Tribunal. The Tribunal is empowered to assess the situation and determine the appropriate compensation for the person affected by the cybercrime.
- **Nature of Compensation:** The compensation ordered by the Tribunal is in the form of money equivalent to the loss caused. The Tribunal has the discretion to determine the amount of money it considers sufficient to compensate the victim for the financial losses incurred.

In summary, Section 37 of the Digital Security Act 2018 provides a mechanism for victims of specific cybercrimes, including digital or electronic forgery, digital or electronic fraud, and identity fraud or personation, to seek compensation. The Tribunal has the authority to issue orders for compensation, and the compensation is typically in the form of monetary restitution equivalent to the financial losses suffered by the victim.

Answer to Question 4

Preventive Measures to Avoid Future Incidents

Chapter III of the Digital Security Act 2018 outlines preventive measures that must be adhered to. The government's stance involves taking specific initiatives:

- **Authority to eliminate or obstruct certain data under section 8:** Should Cipher release pilfered sensitive information online, it becomes the Director General's responsibility to request the removal or blocking of this data, citing a potential threat to security and public order as per subsection two under *section 8.*
- **Emergency Response Team under section 9:** In response to Cipher's attack, the mandatory formation of an emergency response team is crucial. Subsections (a), (b), (c), (d), and (e) under *subsection five in section 9* detail the steps this team should take during an incident resembling Cipher's attack. The emergency team is tasked with securing critical information infrastructure, responding to digital attacks, preventing breaches, and collaborating with foreign teams upon government approval, all within the confines of established laws.
- **Establishment of a Digital Forensic Lab under section 10:** Sections one to four under *section 10* advocate for the creation of one or more digital forensic labs supervised by the Agency. These labs are to collaborate and operate under established rules, aiding in gauging the extent of damage caused by Cipher's attacks and devising strategies to counteract such incidents.

- **Assurance of Quality Control (QoC) in Digital Forensic Labs under section 11:**
  Section 10, subsection one, emphasises the Agency's responsibility for ensuring the quality of digital forensic labs. Points (a), (b), (c), (d), and (e) under subsection two outline quality control measures, including ensuring personnel possess proper qualifications and training, maintaining the physical infrastructure, safeguarding data confidentiality, using quality instruments, and adhering to scientific methods. These measures collectively enhance an organisation's capability to analyse cybersecurity attacks akin to those orchestrated by Cipher.

Additional preventive measures from a government perspective encompass continuously updating laws, seeking international cooperation, establishing specialised units to combat cybercrime, and promoting public awareness of cybersecurity. Meanwhile, organisational measures involve employee training, regular updates to security policies and procedures, implementing robust network security, and collaborating with governmental entities.