Hi Dr Nida, this is Ying Chan.

This is the Mid-Module Assignment for the Principles of Digital Forensics and Cyber Law module. I chose the R v. Vachon-Desjardins, 2022 ONCJ 43 case for this assignment.

First, let's look at the summary of the case,

Sebastien Vachon-Desjardins, the defendant, was a member of the NetWalker crime organization, which oversaw supplying ransomware-as-a-service (RaaS).

Developers create, update, and distribute the ransomware and affiliates involved in their RaaS business to rent the ransomware, identify targets, and deploy ransomware.

In exchange for a share of the money made from extorting targets, the NetWalker RaaS allowed affiliates to rent access to the ransomware.

Emergency services, law enforcement, medical facilities, academic institutions, and business entities were the targets of the ransomware.

The defendant was apprehended and arrested in Canada in 2021 because of an American extradition request.

Due to pending drug trafficking claims in Quebec, which were dismissed on January 21, 2022, when he was sentenced to 54 months in prison for five drug trafficking-related offences and possession of the stolen property, the defendant was not turned over to the United States.

On February 1st, 2022, he entered a guilty plea to computer data mischief, unauthorized computer usage, extortion, and participation in criminal organization activities related to his membership in the NetWalker RaaS.

The defendant received a jail term of 6 years and 8 months for his offences. Additionally, the offender was mandated to surrender around two million eight hundred Canadian Dollars in reparation as well as any cryptocurrency or CAD held in Canadian banks or safe deposit boxes.

Point number one. This case, as was noted in the last slide, was prosecuted in Canada.

The reason I chose this case in Canada, is the case was ended recently in 2022 providing the updated cybercrime methodology and technology.

Moreover, this is possibly the first ransomware case on this large scale in Canada.

The other point is the legal system of this case is common law, when there are no written principles of law or applicable legislation, common law is used to guide decision-making in exceptional situations.

Canada’s legal system is based on a combination of common law and civil law.

The Criminal Code is also considered a code, and it is used throughout Canada in reference to Justice Canada 2021.

This case could turn into an important case reference in common law in the future.

Point number two. This cybercrime in this case is Ransomware activities of the criminal groups.

This Ransomware case has Cross-Cutting countries for International Cooperation that involved Bulgaria, Canada, and the USA.

Almost all ransomware cases nowadays are required to pay by cryptocurrency. It enables cybercriminals to accept money while maintaining a high level of anonymity as well as making transactions hard to trace.

Cryptocurrency is perfectly legal in Canada and USA.

The organization within such countries might be targeted since they are able to pay by cryptocurrency.

Nevertheless, there are 9 countries where Bitcoin is banned including Nepal and 8 countries where the use of Bitcoin is legally restricted including China reference to Cryptonews 2022.

On the other hand, this case is participation in activities of the criminal group, NetWalker, which provided a new spreading methodology - Ransomware-as-a-service (RaaS).

To increase members of the criminal group and organise same as a business.

Point number three. The chosen cybercrime, Ransomware, is a type of malicious software, or malware.

It could be spread by Phishing, Exploiting, and Compromising accounts to the target computer. Encrypts and steals the victim's files and denies the victim access to files or systems unless a ransom is paid.

The main nature of ransomware is extortion.

Even if the attacker would threaten to disclose the victim's data to the public or permanently encrypt it if they did not pay quickly, the attacker just wants to be paid, whether the payment is less than the original amount.

They could ask to pay by cryptocurrency like Bitcoin which is highly used by ransomware as it is hard to trace back.

They mainly targeted emergency services, public services, and commercial institutions for a large amount of payment.

The criminal group, NetWalker, in this case, showed well-organized and systematic.

The defendant has increased the group member by hiring between 10 to15 unknown individuals and teaching them the methods.

Point number four. As this case required International Cooperation of Cross-Cutting countries, the case mainly dealt with Canada and USA.

In August 2020, the American FBI provided information to the RCMP in relation to a NetWalker ransomware affiliate operating in Gatineau Quebec.

However, the defendant had outstanding drug trafficking charges in Quebec, the RCMP applied for various court authorizations to further their investigation into the suspected activities of the defendant.

On the right-hand side are the guilty decisions of this case.

All the charges are under Criminal Code, which could be found in the other cybercrime. For example, Section 430(5), which was also found in R. v. Geller, [2003] O.J. No. 357 case about hacking after obtaining 400 credit card numbers.

Similar cybercriminals in the U.S.A would be using the 18 U.S. Code instead. For example, 18 U.S. Code § 1030 - Fraud and related activity in connection with computers and 18 U.S. Code § 873 - Blackmail and extortion laws.

No forensics technology should be necessary since the defendant chose to cooperate with Canadian law enforcement.

Point number five.

For the costs of this crime, it could refer to the NetWalker behaviour Analysis by McAfee, 2020.

They might require the Email server for the phishing attack.

The target hardware or software cost for scanning and preparing the exploit attack.

The expense of social engineering on the target user for the compromised accounts.

Hosting the servers for ransomware-as-a-service.

Share the payment from victims to the hiring members.

Although these points involved the cost to perform those actions, the amount could be very low or even free for the hackers themselves. The main cost should be the workforce to develop the ransomware which is incalculable.

For the affecting investigation factors, data could be encrypted in the victim’s system, the log might be unable to be read.

The attack source address might be routed to many places which are hard to trace back.

The compromised account should be owned by the victim, the account information might not be related to the attacker.

The ransomware-as-a-service does not require expert hackers, the attackers could be many and with a clean criminal background.

The investigation might not be able to catch up to the speed of the rapidly spread ransomware far and wide.

Point number six is about the gathering of evidence.

Regarding the Canadian Legal Information Institute, the defendant was identified by the Canadian authorities using information obtained from the U.S. based on IP addresses. Investigations into multiple Apple, Google, Microsoft, and Mega.nz accounts, aliases, and email addresses. As well as the personal information disclosed on social media sites.

In January 2021, the police searched the defendant’s home and bank accounts. Search warrants and general warrants to seize cryptocurrency resulted in many devices seized with approximately 20TB of data contained therein. If printed, it would fill an entire hockey arena.

During an application to extend the detention of items seized, in the absence of any charges

The defendant even improved upon the ransom messages and convinced the creator of NetWalker to use “mixing services” to disguise funds paid for ransoms in Bitcoin.

Defendant’s decision to cooperate with Canadian authorities, the police would not have charged the defendant for several years while they sifted through the mountain of data to identify victims and searched for proof to mount a successful prosecution.

Point number seven is about the critical examination of public and social perception generally in Canada.

Reference to the Canadian Enterprise Communications 2021 survey by IDC, 2021.

67% of the 460 firms questioned and reported that they had been victimized by ransomware in 2021.

On paying a ransom, 44% of respondents admitted that their company has done so.

In contrast, slightly under half of those that paid stated access to their encrypted data was only partially recovered, while 42% said that their business was able to fully restore its data using the decryptor offered.

Demonstrating that more than half of the Canadian companies have this belief or try their luck on paying a ransom for the restoration of their system or rescue of their information. Furthermore, it indicated that their system lacked a proper backup solution or file security against this type of malware attack.

With reference to the State of Ransomware 2022 report from Sophos.

The Average Ransom Payments over the 31 countries, Canada is ranked 26 with US$ one hundred twenty-three thousand just after the US.

The average cost to organizations to Rectify the Attack has been decreased by US$1.27 Million which is 66% less in 2021.

The figure showed that Canadian public and social perception is above average compared to other countries. Moreover, there are significate improvements in last year.

On 14 June 2022, the Government of Canada introduced Bill C-26, ARCS to strengthen Canada's cybersecurity.

The Telecommunications Act is being amended by the proposed legislation to make security a priority. This will give the government the power to impose any measures required for Canada's telecom system to be secure.

In addition, including this law in the CCSPA establishes the framework for safeguarding Canada's key infrastructure.

This will enhance cyber security in the banking, telecommunications, transportation and energy sectors, and this proposed law will safeguard Canadians.

Organizations will be better able to prepare, mitigate, and handle cyber threats with it.

This is the reference list including the figures and images used. That is the end of my presentation, thank you so much for your interest and listening.