

**Table of Contents**

[Part A - Overview of the Target Organization](#_rg6ngq2j628z) **3**

[Introduction](#_f28is4wdtnir) 3

[Common Vulnerabilities and Criminal Threats](#_k1xqihrtjovx) 4

[Part B - Information Gathering and Report](#_b1st66j36mu) **5**

[Online Target Research](#_dmrux3tdhsk5) **6**

[Examples](#_tcu4xpi0dmu) 12

[Vishing](#_okssxz2kl7nq) 12

[Pretext Example Scenario](#_fc23mvelpa2l) 12

[Phishing](#_9c90kzepjn1g) **14**

[Pretext Example - Direct (employee targeted)](#_6fcu9n2rs6xh) 15

[Pretext Example - Indirect (not targeted, generic)](#_83y0iijvq3h9) 15

[Identify Specific Organizational Vulnerabilities](#_j70nczoc07xl) 16

[Discussion](#_s9mpjvrrbp5q) 21

[Conclusion](#_5jfsxikbeje1) 25

[References](#_s6emx0v2akkg) **27**

In the following paper, we will be accessing and evaluating Canadian Natural Resources Limited (CNRL) in order to identify vulnerabilities that might expose the organization to social engineering attacks and threats. The paper will be divided into three section. The first section will discuss details as to why the following organization was chosen for the following project. Secondly, through research and other means of information collection, we will be assessing the vulnerabilities of the organization. Finally, our team will propose mitigation strategies to protect the organization and staff from attacks that may be initiated by exploiting the vulnerabilities discussed previously.

# **Part A - Overview of the Target Organization**

## **Introduction**

Canadian Natural Resources Limited (CNRL) is an oil and gas exploration, development and production company. It’s head office is located in Calgary, Alberta and employs approximately 10,000 individuals. CNRL is known to be Canada’s “single biggest conventional heavy oil producer” with 121,000 barrels of oil produced per day [1]. CNRL was also ranked number 251 on the Forbes Global 2000 list in 2009 [2]. CNRL is known to be the largest producer of heavy crude oil in Canada. Companies like CNRL make future plans for development - from new methods of extraction, to discovering land and producing petroleum products. Obtaining information regarding future exploration plans and extraction methods can be beneficial for other companies. With the vast amount of information that the company holds, the company can easily be targeted for many types of attacks including data theft regarding operations, technology compromisation and social engineering attacks. CNRL was chosen as target due to the large revenue generated by the company and its reputation in Canada and around the world. Furthermore, the head offices of the company is situated in Calgary, making it easier for us to gain information regarding the company, its employees and their operations within the city and nearby locations.

## **Common Vulnerabilities and Criminal Threats**

Common vulnerabilities for these type of industries are stealing field data, corporate espionage and sabotage. These vulnerabilities exist due to the lack of security awareness/training, outdated updates, software vulnerabilities and poor physical security. Social engineers may target the industry because these companies hold information about ongoing trade secrets, wealthy people and potential industry competitors may hire hacker mercenaries to sabotage other companies. An example, there has been reports about Russian hackers shutting down Natural gas Pipelines, Chinese hackers hacked Exxon, Shell and Baker Huges; and also there public attempts in which the hacker organization “Anonymous” attacked TransCanada. These case studies shows sabotage and stolen trade secrets that occured.

Most common vulnerability in the oil and gas company is industrial control systems. As it's a big role in the upstream oil and gas companies as there been terrible sabotages like December 2002 Venezuela state oil company which access the Programmable logic controller in which it cut Venezuela’s oil state production down by 81 percent in one day.

Another common vulnerability to this industry is the anti-petroleum and anti-oil movement. In recent years, there has been a growing number of individuals that are concerned about the long-term effects of the energy, oil, and petroleum industries. These groups are concerned about fracking, pollution, and the First Nations land that it falls on or goes through. An internal document by the RCMP that was leaked in 2015 showed their concerns about these movements and if they got out of hand (extremist/criminal activity that traced back to these campaigns).

In the petroleum industry, many of the marketers are victims of ransomware attacks, where data is held onto by attackers by malicious software until they are paid the ransom they demand. Human error results in clicking on malicious URLs. URLs are also used by applications to update data, which occurs in real-time. Attacks take advantage of this- benign applications which go to these malicious URLs. These oil marketers are using mobile technology which has its own set of concerns.

These industries are also a huge target for cyberattacks. Deloitte in 2016 reported that the energy industry was the second most popular target for these attacks, with almost half of them being overlooked. This is also applicable and expanded to the petroleum industry. These industries have sensitive information in relation to consumers and use computer access for many of the tools and equipment. Therefore there could be devastating effects if hackers get a hold of these (billions of dollars worth), especially since the offshore physical areas, with databases present on them are vulnerable if they are not secured properly. These locations act as access points to confidential information. Well-flow data could be retained which is needed to stop fluid eruption for blowout preventers, cement slurry data from a development well could be changed up by these attackers and they could suppress drilling views, both offshore by attackers. Most of these attacks (around 90%) start with email phishing, and due to this many employees are choosing to use SMS services instead, with 80% of employees doing this for business activities.

Technology plays a substantial role in these corporations, so the risk of phishing attacks (and their variants) go up. Comparatively, a company belonging to the same industry, BP Oil was a victim of email scam and spear phishing appearing to come from the Canadian Bar Association with a legal request. Spear phishing is phishing that seems to come from a known or trusted sender.

Since this time, our target is much larger (with around 10,000 employees), this increases the risk of there being more lower ranking employees that may have not had the right security training. These employees may not feel as much of a bond with the company and have malicious intent or will not care as much about giving information out in regards to the company and its operations. The more employees there are, the harder it is to trace responsibility of an action or activity and accountability, especially if there is not a proper procedure in place to address the consequences of such actions. This becomes more complex with outsourcing of services and third party company involvement. In CNRL, the headquarters location primarily has geologists and researchers, whereas the employees are the ones that go out to the sites.

# **Part B - Information Gathering and Report**

Information gathering about the company and the individuals is vital for social engineers. Learning about the company and how it operates is the starting point which tells us how information is being transmitted for an example who talk to who, as well who has more authority and what technology is being used. By knowing who talks to who, social engineering use methods to intercept this information an example is taping a phone or even hacking an individual email. Social engineers figures out there targets by the hierarchy sometimes starting from the lower and carefully moving up. Figuring out what technology CNRL is using can make social engineering check any vulnerabilities. Information gathering on individuals in the company is usually how social engineers find vulnerabilities. By vulnerabilities they use this information to manipulate people's decisions plus the pontiental of leaking sensitive information on the company. Information like interest, how they wear, how they talk and past accomplishments and where they live. By knowing this information social engineering attacks like phishing, vishing and impersonation.

# **Online Target Research**

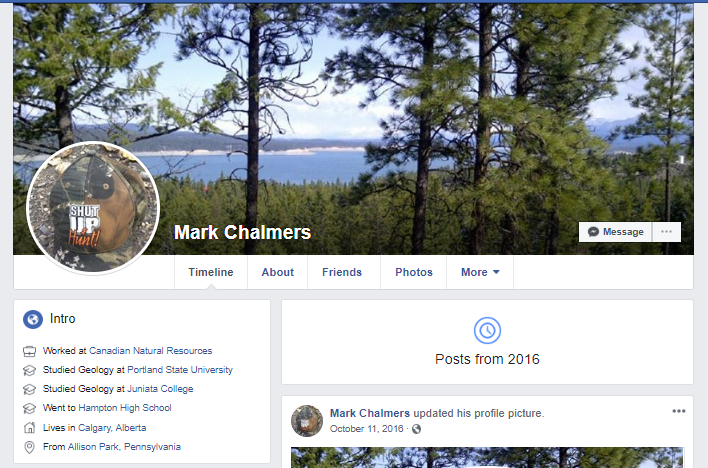
Canadian Natural Resources Limited, or CNRL or Canadian Natural, is a Canadian oil and gas exploration and production company. Its main head office is located in Calgary Alberta at 855 2 Street Southwest #2100, Calgary, AB T2P 4J8. Mr. Timothy Shawn McKay or “Tom” has been appointed as the President and Director of Canadian Natural Resources Limited since March 01, 2018 and February 2018 respectively. As described above, the company consists of approximately 10,000 employees.

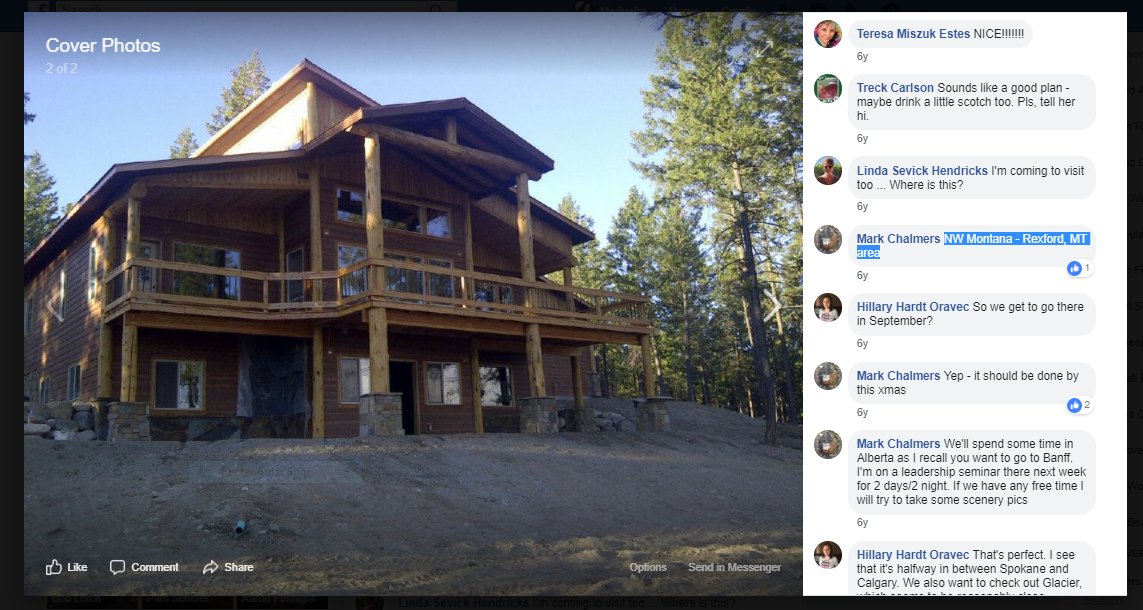
Information about the organization chart are on the official company website. Figuring personal information about a specific target in the company can be found through websites such as pipl, zoominfo, LinkedIn and other social media sites like Facebook and Twitter. From a social engineering perspective, figuring out details about which person works in a department isn't a challenge as they can be discovered through these websites. Digital footprints on the internet open doors for social engineering to create possible attacks like vishing (voice phishing), phishing, SMiShing (SMS phishing) and Impersonation.

For the purpose of the following assignment, we conducted searches on specific employees within the organization. Social media has become a vital part of people’s lives, making it extremely easy for attackers to retrieve this information and use it to target the individual or the company itself. Although extensive searches were done on multiple employees, a couple were chosen to demonstrate how easily, targets can be chosen, exploited or even impersonated. Below are the information we were able to obtain regarding Vice-President of Exploration (Central) Mr. Mark S. Chalmers.

**Example: Mark S. Chalmers**

Mr. Chalmers is from Allison Park, Pennsylvania but lives in Calgary, Alberta. He attended Hampton High School located in Hampton Township a northern suburb of Pittsburgh, Pennsylvania, USA (2929 McCully Rd, Allison Park, PA 15101, USA). He was in the graduating class of 1977. Then he obtained his Bachelor's of Science in Geology in Juniata College located in Huntingdon, Pennsylvania and graduated in the class of 1981. He continued to get his Master of Science in Geology at Port State University. Mr. Chalmers enjoys the outdoors. He had a house build in “Northwest Montana - Rexford, MT” area. The house was planned to finish renovation by Christmas of 2013. According to his facebook comments, he wished to move into the house once he retired. We also found multiple family members that may be related to Mr. Chalmers. This includes Christie Chalmers and Zach Chalmers. It was quite clear that Mr. Chalmers was into hunting from his facebook profile. This also become clear as many friends in his friend list also shared the same interest in hunting. We were also able to find that he was into hockey and baseball and supported the Pittsburgh Penguins and the Pittsburgh Pirates. He’s been working for CNRL for 13 years and 9 months. He first started as a Exploration Manager in August of 2015 then was promoted to Vice President Exploration Central District in January 2015.





Information regarding his hometown, where he lives and education can be found on his online profiles and accounts. He also has images of his home and comments mentioning the location of his home, details about renovation and his plans after retirement. This information can be further verified through is LinkedIn profile.

We were also able to find Mr. Chalmers on a webpage made for Hamptons High School Class of 1977 where you can find photographs of reunions, other classmates of the graduating class, profiles of each classmate (including Mr. Chalmers - which has been updated by himself), locations of where each classmate lived, etc.



It may not be clear as to why this information may be beneficial to anyone but for a social engineer, this information will pave the way for a carefully planned out attack. The intention of presenting the following information was to demonstrate how easy it is for an attacker to find information regarding employees within the organization. With the amount if information online any employee is prone to social engineering. Although we did not personally know or contact Mr. Chalmers, we were able to retrieve information from 42 years before. We were able to retrieve such information on many individuals that work in the organization including individuals that have retired. An attacker may use the information to impersonate a classmate or plan out an attack based on personal interest or their love for a sports team. In the sections below, we will discuss how the following information can be used in different types of attacks such as phishing, smishing etc. and further discuss methods and techniques that can be used to protect and educate employees about how the information they post online can be used in an attack.

**Additional Target Research**

The organization chart for CNRL can easily be found through a simple Google search. Due to the large size of the organization, we decided to focus on the Exploration and Exploitation Departments. Below is a screenshot of a organization chart we were able to find on the internet that clearly outlines the names of individuals and their position within the organization. It is important to note that this information is publicly available for anyone to find. Furthermore, for most individuals on the chart, the information can be verified through their LinkedIn accounts. For our purposes and records a screenshot was taken capturing the specific departments that we were interested in. The chart can be seen below.



In order to test the front-end security of the organization, we called the headquarters located in Calgary, Alberta using the company reception line found online (403-517-6700). The intention of the call was to ask generic questions regarding the company and the types of security controls CNRL has put in place. We were able to talk to Reem Ahmed who was a representative. The conversation was as follows:

Reem: Good morning. Canadian Natural

A: Hi, my name is Ahmed and I'm an Information Systems Security Student at SAIT. I'm doing a project on CNRL, is there anyone I can talk to about the company?

Reem: Can you please hold for a moment Ahmed?

A: Yes.

Reem: Alright. Thank you.

Reem: Thank you for holding. What is your project on? Is it just the company or a specific department?

A: It is just a couple of general questions.

Reem: Let me see who can help you. What I would do is send an email to [student.jobs@cnrl.com](mailto:student.jobs@cnrl.com) That email is generally for employment or internship. Because this is a school project and you are a student, they might be able to help you or guide you to who to speak to. It is not everyday that we receive calls like this. So they should be able to direct you.

A: Is there any chance we could talk to you?

Reem: Oh no, I won't be able to help you. I’m here to direct calls so I will not be able to help you.

A: That's okay. Thank you.

## 

We were able to talk to Reem Ahmed in person as well and she was quite clear that she will not help and stated that it is against policy for her to answer any questions. She also mentioned that if we wanted to discuss any information regarding the organization a formal meeting must be set up with an authorized individual. We approached her stating that we were here to gather information school project to which she responded saying that you had to know someone within the organization in order for someone to help you for a school project or assignment.

As seen from the conversation, Reem Ahmed took action to follow company policies. She stated clearly that no information will be given out unless one had access to a individual within the organization or was given special access to the facility. She did not give out any information regarding the organization. She simply refused saying that it was not her duty to answer question and how it was against company policies. In the incidence of an attack, the following scenario will cause the attacks to deviate to another plan and use other means to access the facility or the information as the front end security is high. It is important to ensure that the front end staff follow company policies strictly to ensure the security of the company, its information and employees.

## **Examples**

In the second assignment we used the social engineering techniques of vishing and phishing. We found individuals that we wanted to target and created a pretext so we could go through with these techniques. Some of these are the same pretexts from the first assignment with alterations done to fit with this company instead. This is described below.

### Vishing

Vishing (voice phishing) is a type of an attack that happens through the phone. The objective of this attack is to gain information or use manipulation to change the victim decision making, using social engineering.The attacker will pretend to be a person that you would trust, using tone of voice, talking patterns, and framing. The Vishing attacker would spoof their caller ID making it hard to trace back and also that make it seem legitimate or a localized sourced, making the victim be familiar, which increases the possibly picking up the phone.

Vishing attacks can be performed to CNRL by calling the company directly, specific people involved with the company or companies that are contracted with CNRL. When performing a vishing scheme, the attacker will have to gather phone numbers and understand who talks to who, and what information is usually exchanged. By understanding the information exchange, the attacker can intercept using social engineering. Targeting a third party that is involved with CNRL is a good strategy because there is a less of a risk of getting caught by the main target.

#### Pretext Example Scenario

In the petroleum industry, before they decide to lease the land that they are interested in (which may be owned by the provincial government or First Nations), they look at core samples first for the lithology. These core samples are obtained from third parties who do drilling with special drills into the rock. The Geologist is the one that make the arrangements with the third parties.

In this scenario will show an example how an attacker may find out a target, pretending to be a person that works at CNRL. The objective is to find out what locations that CNRL are focusing on, which could be potential exploration on the land development. Hence, obtaining this information is sensitive because if an attacker were to gain this information about the land leased before CNRL makes the buy, the sensitive data could be sold to another company and the other company can lease the land to make the production.

A pretext is planned out for this scenario as well as potential responses that can be given by him. The target will be called and he or she is told that the geologist they usually talk to is not capable to work because he or she chosen (the attacker) to fill in the position for the time being. The target will leak the location that CNRL was looking at for drilling. Thus, the objective is complete. For this hospitalized and is in critical condition, and through management this employee was his strategy, planning possible responses, using sympathy (emotion), having a casual demeanour but also expressing urgency, and having a strong pretext is the key to be successful.

Example Pretext

Attacker: Hi, this is Reem from CNRL.

Victim: Hey how's it going, what can I do for you?

Attacker: I’m calling because Jonathan Rowe is not able to work right now, as he is in the hospital. I was told by my VP to replace him for the time being.

Victim: I’m sorry to hear that, what happened to him?

Attacker: He got into a car accident on the highway and he is in critical condition at the moment.

Victim: Oh my god.

Attacker: Sorry I’m in a bit of a rush right now. Since this incident occurred, he didn't tell us the plans for quotes and location of cores samples and I don't have access to his email password or I don't see anything he wrote on her desk. Can you provide that information? I have to report everything in like 10 to 15 minutes.

Victim: Definitely, the prices are \_\_\_\_ and locations are \_\_\_\_\_.

Attacker: Thanks a lot, I really appreciate it! Have a nice day.

# Phishing and SMiShing

Phishing is a type of attack that happens through email. The objective is to lure computer users to expose sensitive information or to trick the person to click a hyperlink or even download a malicious attachment that could compromise the computer. Attackers will use methods like spoofing the same domain for the email or even something almost similar and having a believable pretext. Phishing may be spear phishing, and may use direct you to customer service websites with company logos that seem legitimate, and claim to come from a financial institution, the government, or a social networking website. In these scenarios it will require you to give away personal information.

In this scenario, it is basically the same idea as vishing, where the objective is to find out what locations CNRL are focusing on, which could be potential exploration on the land development.

For this attack, Alberta Core Research Centre is selected as a target for the attack. This is another effective method because core samples are sent there after being observed or companies get core samples to look at from nearby locations where that core sample was obtained from. Alberta Core Research Centre is chosen as the target because they record which core samples have been taken and which company gave them the cores. Obtaining this information will let the attacker know the location that CNRL was looking at and what time they were doing so. Phishing will use pretexting and spoofing of the email address to make it seem that it is being sent from CNRL. The pretext will mention that the Geologist that was assigned to this project has been laid off and a lot of data been lost, allowing us to ask for an update of what she was looking at, what cores has been borrowed and has been submitted.

## Pretext Example - Direct (employee targeted)

To: CRC.ServiceDesk@aer.ca

From: JohnDoe@CNRLcom

Dear Service Desk,

Jonathan Rowe, the geologist in charge of observing the core samples, has been laid off. We’ve lost the information regarding which core samples were borrowed from your organization and which samples have already been submitted.

Please update me on the borrowed and submitted samples with locations and the due dates.

Thanks,

John Doe

Geologist

Canadian Natural Resources Limited.

## Pretext Example - Indirect (not targeted, generic)

As mobile technology is growing, the use of mobile intrusions also continue to grow, with both phishing emails, websites and SMiShing. According to IBM Research, users of cell phones are 3x more likely to be victims of phishing. SMiShing is also called SMS phishing and is done by deceiving a person into downloading some form of malware onto their phone. A user is sent a text or SMS (on the default texting app or messaging app) which may urge the user to download something via a link that is given. Verizon’s 2018 Data Breach Investigations report wrote that common malware that can affect IOS and Android are Adware (that look like advertisements), Chargeware (charging for a certain service and asking to enter credentials), Trojan Horse or Trojan (that reside in the background of the phone or pretend to be an application), Spyware (which spies on the user and collects information for a third party), and Riskware (which use certain code that can affect the device altogether).

The user may also be asked to provide credentials and login data (like 2FA information) which will be stolen by the attacker, or extorted into revealing secrets that may or may not be related to the corporation. Mobile devices are far more vulnerable to attacks than traditional devices, as they are outside of firewalls without endpoint security, and have a number of messaging applications that desktops do not have, including social media platforms like Facebook (Messenger), Whatsapp, Instagram, Snapchat, Viber, etc with their SMS and MMS capabilities (useful for malicious attachments). There is far less detail on the interface for mobiles, and limitations such as not being able to hover over hyperlinks to know where it may redirect to. The screen sizes are smaller, which means it may be more difficult to read the details such as grammatical errors on a mobile.

For our assignment, the phone number of the individuals can be obtained through zoominfo.com (after registering for an account). We obtained the direct phones of individuals Kendall W. Stagg (4037166318) and Jeffrey J Bergeson (2194731516).

Since these are direct numbers and not HQ (which is 4035176700 of the corporation), it is easier to perform SMiShing since it is likely it will not go to landline and may be a number with SMS and texting functionalities implemented in them.

Pretext Example - Direct (employee targeted)

Hi Kendall,

Can you go over this invoice before I submit it?

[link]

Hi Jeffrey,

Can you go over this invoice before I submit it?

[link]

Pretext Example - Indirect (not targeted, generic text)

Have you taken a look at this year’s annual report? You can find it at [https://www.cnrl.com/upload/report/113/02/cnq-2018-annual-report\_t\_r.pdf](https://www.cnrl.com/upload/report/113/02/cnq-2018-annual-report_t_w.pdf)

[spoofed URL]

Impersonation

Impersonation is type of social engineer attack in which in person used to play a role of someone you would trust allowing to access your premisses. The objective would convince a person to allow access to network infrastructure to plant a ioT device which could perform man in the middle attack which intercepts and transmit network packets, or even the office to get sensitive data. An example would be a person can impersonate as a internet provider claiming that they came in to replace or fix a router in the office.

## **Identify Specific Organizational Vulnerabilities**

In order to access the physical security of the facility, we paid a visit to the company headquarters in Bankers Hall Retail (located at 855 2 Street Southwest #2100, Calgary, AB T2P 4J8). The intention of the visit was to observe the types of physical security put in place to prevent social engineering or any vulnerabilities that an attacker might take advantage of.

The office was located on the 21st floor of Bankers Hall. The main floor of Bankers Hall itself is extremely busy especially during the lunch hour. It is important to note that during these hours the security is quite low as the building is busy with employees from surrounding offices heading out to take their lunch break. We were able to get the 21st floor and did not encounter any security guards.



The 21st floor was all offices for CNRL. There are 2 sets of elevators that can take you up to the floor, one on each side of the building. It was extremely quiet. We did not observe anyone in the hallways of the entire floor except for a janitor. We were able to walk around the entire floor without any questions being asked. We did not see any security guards. We were able to locate a staff kitchen, meeting rooms and washroom. All these areas were locked and only could be accessed using key cards. It is important to not that if you had a key card in your possession, these areas could be accessed quite easily as there is no security guards to protect the area. The area did have multiple security cameras. We were within the facility for about 15 - 20 minutes walking around without any questions being asked.

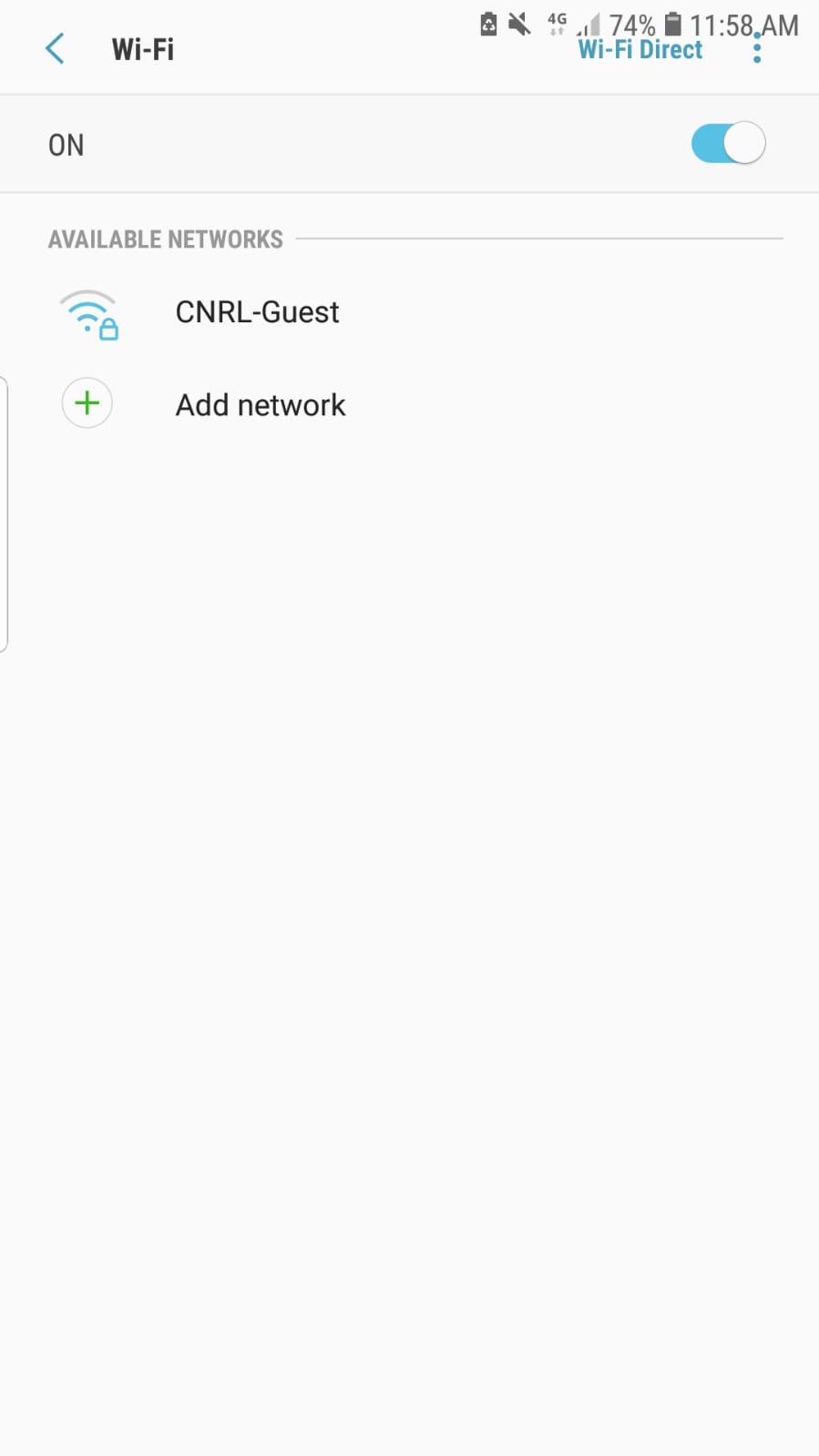


Once we made our way to the reception area, which was clearly labeled “Floor 21 Main Reception” we noticed the only individual within the office was a receptionist. There were offices inside the area which can only be accessed once the receptionist checks you in. It was quite surprising to us that were was no security available on the floor and that anyone can come up to the floor and walk around without being questioned. We did come across multiple signs reminding employers of security and contact information of building security. It is important to note that just reminding employees of security is not enough. The physical security of employees and others within the facility must be considered. It is quite easy to come into the building and up to the 21st floor, walk around the facility without any complications. Although phone number of building security is posted across the floor, it times of urgency one may not have the chance to contact security or take the necessary action to protect themselves.



We also noticed that the company did not use a WiFi connection. The only WiFi that was available for the facility was the guest WiFi connection. The guest WiFi password was printed on business cards that were placed on the front desk and can be easily accessible to anyone. We ourselves were able to retrieve the password during our short visit. It was clear to us that the company used wired connections in the office places but this did raise some concerns when it came to mobile devices and tablets. To ensure that no other WiFi connections were available we did scan for nearby WiFi networks using our mobile devices as seen below. Without a staff WiFi network available, the staff most likely connect their mobile devices to the guest WiFi. As we know, we do everything on our phones including checking our emails, banking etc. This in itself is a major security concern. Staff members may log into their company email or other accounts with confidential information using their mobiles phones which is connected to the guest WiFi as there is no other connection available. Furthermore, it is convenient for employees to log into the guest WiFi because it is available from anywhere in the office. A wired connection is not convenient when employees move from meeting to meeting and different parts of the facility. It is a good security measure to implement wired connections but people prefer convenience and connecting and disconnecting your device from time to time is not convenient and it not likely to be followed. It may be beneficial to implement a staff WiFi network to ensure that no staff devices are connected to the guest WiFi.

From an attackers point of view, one can easily monitor the traffic to determine which sites are being opened and gain information regarding the daily functions of the company. If the communication is not secure the attacker will also be able to interfere the network traffic to access unauthorized data (man-in-the-middle). Therefore, this is a major security concern that can be exploited and the necessary actions must be taken to ensure that the company is protected against eavesdropping and other forms of network attacks.



## Discussion

There were certain pieces of information regarding the company that were easy to find. This includes the number of employees and locations of offices, phone numbers and revenue. Details regarding daily processes within the organization were hard to find as the information is not publically available. Multiple articles were found online discussing when certain employees were appointed and withdrew from positions. This information can help an attacker when planning out attacks as small changes in employment causes some adjusting within the organization. This can be exploited by an attacker.

When it came go gathering information regarding positions higher up in the organizational chart, it became quite easy as the information is publically available on the internet for anyone to view and access. There were multiple organization charts available online along with annual reports which not only included employee’s positions but also their age. We were also able to find websites that contained information regarding their income, news articles and many other sources of information. It was also easy to find personal social media accounts containing pictures and a vast amount of information regarding their family, home, personal interests etc. Note that with personal information such as income being online, these employees and families may be targeted personally and are the individuals within the company that are most likely to be targeted.

To illustrate this, we will be using the example discussed above of Vice-President of Exploration (Central), Mr. Mark Chalmers. Through a site called Bloomberg we found that Mr. Chalmers makes an annual income of $298,606. The following value may not be accurate but to an attacker this is all the information that is needed to launch an attack. With the information that we were able to collect on Mr. Chalmers would be a good target. The attacker might target him for money and use the information we discovered regarding him to launch an attack. For example: an attacker might impersonate one of his classmates, or befriend him by pretending to be a Pittsburgh Pirates fan.

For employees lower down the organizational chart, there is little to no information on. These employees were not mentioned in organizational charts nor were they mentioned in annual reports or websites. To test if we could find any information regarding individuals lower we tried looking for details of representatives in the headquarters. Nothing was found online. Once we talked to Reem, we decided to do a couple searches on her to find a method that we could use to best approach her and to get more of an understanding regarding her position in the organization but we were not able to find any details on her. No LinkedIn, Facebook or any other social media accounts were found,

**Part C - Mitigation Strategies**

It is important to provide the right training and have a plan in place to minimize security risks and vulnerabilities. A training plan that is set in place for employees can ensure that they are taught to recognize some of these risks and be vigilant or wary of anything suspicious. This security training, which include workshops, will help employees use the internet in the appropriate manner and for the purposes it is intended for in the organization. The training will outline potential motivations of hackers and attackers (such as the ones discussed in this report) and the consequences of these attacks or employee carelessness in regards to protected information (and leaking). Employees will be taught ways to protect their private information and credentials as well as company data (such as how the representative Reem Ahmad did not disclose information)..

This training should help employees learn about other phishing techniques as well like vishing, smishing, spear phishing, and impersonation tactics and strategies as well. This could include seeing the signs of a phishing email like the grammar used, the domain it comes from/email service they use (could be one that is gibberish), links, attachments, possible english translation due to being written in a different language, and the tone used (urgency, threatening, emotional, etc). Another indicator would be if it comes from a contact that they have not been talking to recently, or is contradictory to a policy that is usually in place (like asking for confidential information over the email that is usually not sent that way). For SMiShing, there is usually a link at the bottom of the message for an offer or alert and the sender is some supposed company. The tone in these text messages too might written with a sense of urgency or threatening and induces panic and may seem like it comes from a legitimate source, like someone you trust. A closer inspection reveals a number that is fake.

To be precise a SCAM check can be conducted to identify fraudulent content in emails and SMS. S for Sender to see if the email it is being sent from is recognizable (look at the email address instead of the name that is displayed in it as well as the email content. The sender might use a personal email address. C for Confidential, where the email is requesting data that is considered confidential (credit card or/and bank info, SIN). A for Addressee where the sender may be using a general way to address you, rather than your name (like Sir or Madam, “to whom it may concern”). If your name is used, it may be misspelled. The M is for Message where again, the contents of the email are inspected and grammatical errors, spelling mistakes, and inconsistencies in these things are noticeable. If the scammer is coming from another country, translating services like Google Translate will show errors in these things when translated to English. The email content may not contain any contact information like an address, or work/cell phone number. It is important to use email services that may be already able to detect if any email is scam or display a message of suspicious, as well as detect fake accounts, and move it to the spam or junk folder as this will help to make an employee more conscious. However, since many SMSing and messaging apps cannot do this yet, it is easier for targets to use these. A company-wide platform like Vaporstream can be used in place of personal SMSing and email apps to ensure consistent security and communication with other employees related to business matters. Through these platforms, only certain senders that are whitelisted are allowed into the domain, which prevents man-in-the-middle interference, especially with unencrypted SMS texts on open networks. If an employee is connected to their guest WiFi, an open network, and using a secure messaging platform, then it mitigates the risk of interference. These platforms capture and archive messages so the organization stores them to meet compliance and business needs and is useful for incident response, where notifications are sent out. This also prevents surveillance or/and third party leaks. System administrators could also suppress hyperlinks from all the emails that come in so that employees can only copy paste it into the address bar, but not click on them.

Using different and complex passwords for all your accounts, including social media, banking, and email with password managers like Dashlane and 1Password - with 2FA can help protect them. When receiving an alert that claims to be from your financial institution or an employee, it is better to follow up with them and call, rather than clicking anything in the message.

A phone call may be indicative of a scam if it comes from a source that is not viable or doesn’t seem legitimate and they are asking for disclosed data. If an employee is very prying and persistent of information that is on the verge of getting confidential, that could also be a warning sign - especially if it is not their place to be seeking it out. Making sure that employees feel a connection and attachment to the corporation is also crucial so that will not have thoughts of doing anything malicious to the company. Once spotted, the employees should know who to report it to.

Social engineering drills in which mock phishing email or SMiShing messages are sent out can help understand the effectiveness of this security training within the corporation.

Before employees are hired, they should be screened to make sure they don’t have a history of hacking in their background or anything that may be deemed suspicious or make the company at risk. Screening should be done not just for employees working within the company, but also outsourcing and third parties (like contract work) as well as vendor services that come into contact with CNRL network and assets or other forms of information related to them.

In terms of the anti-oil, anti-petroleum, and anti-energy movements, it is important to educate employees on how to deal with individuals or groups that may target the company and that they might come across with these sets of ideologies. They should be outspoken about addressing the concerns of these groups and the different policies or/and actions that are being taken to address climate change, pollution, fracking, and First Nations land that it falls on. With this reassurance that plans are in place to tackle these issues, it helps to mitigate any action taken against them.

Since social engineering isn’t just technical, it is important that there is physical security in place to insure that unauthorized individuals do not access the premises. There should be proper surveillance and CCTV cameras in place, as well as security guards. At the CNRL HQ, we didn’t see any cameras or security guards to prevent individuals from roaming around on their floor. On the other hand, all of the doors (except for the main one, where the receptionist was), were locked with what seemed to be RFID locks. It is important to remove individuals from access control systems after they leave the organization, as they are no longer part of the company. It is also crucial that individuals do not have more access than they need, based on their role and they only know the information that is necessary for them to know (this prevents privilege escalation). An information classification and management policy can be effective so that employees are aware of what they are allowed to know and not know, be aware of the sensitivity of certain data, and know what they are allowed and not allowed to do with information (like viewing, editing, distributing, etc.). However, when they sign this document, the guidelines for each category should be clear and detailed to prevent arbitrary information and multiple interpretations. Any leak of confidential information should be investigated promptly and thoroughly.

## Conclusion

In conclusion there are potential threats within CNRL. Common vulnerabilities in CNRL are the footprints on individuals on the internet and lack of physical security. The motivation of attackers could be competitors or even people that dislike the oil and gas industry.

Information gathering about the employers and employees was not difficult.The hierarchy was easily found on CNRL official website . We found information on Vice-President of Exploration (Central), Mark S. Chalmers from several sites like linkedin, facebook and ect . This information contains interest , education ,address, relatives and accomplishments. With that information a social engineer can create attack vectors like phishing or even impersonation to expose vulnerabilities.

In addition we called CNRL attempted to ask question about there security and we found out that they have a policy of how to answer question over the phone and also in person regarding the company. Further we then checked there headquarter and checked there physical security with potential vulnerabilities like lack of security on there floor and ioT devices that opens the doors for the rooms in which it could be exploited.

Knowing risk and vulnerabilities about the company is important to create a security training plan. Every department should have a level of security training. But every depart should have a baseline understanding what is social engineering and what attacks could occur. Also how to reduce risk plus how to spot the attacks as well. Without security awareness CNRL would be in risk, from ransomware, sensitive data or money stolen, and sabotage in the technology systems in the field.

Penetration testing are important in big corporate companies. Penetration testers reveal weaknesses before a hackers does. It shows which parts are vulnerable and what parts you should invest in. As well how to implement security controls and enforce strategy.

When a Penetration tester reveals the weaknesses of a company, the person will pretend to be a real hacker but don't actually steal or sabotage anything. Uncovering security policy that the company are lacking and help focus how to detect them. This will prepare a company risk factors and how to mitigate the risk.

Penetration testing reports will also show what vendors have potential vulnerabilities and how hackers can break through. The report will help security education and avoid future attacks by creating strategy and layers of security to slow down a future hacker and prepare to mitigate the situation.

# **References**

[1] P. McKenzie-Brown, “The big five: Canada's top conventional heavy oil producers in profile”, Language Matters, 2011. [Online]

Available: <https://languageinstinct.blogspot.com/2011/04/big-five.html> [Accessed: Apr 03, 2019]

[2] "The Global 2000". *Forbes*. [Online]

Available:<https://www.forbes.com/lists/2009/18/global-09_The-Global-2000_Rank_3.html> [Accessed: Apr 03, 2019]

[3] “Don’t Be a Victim of Fake Job Offers – Run the SCAM Check, *Vista Projects*  [Online] Available: <https://www.vistaprojects.com/blog/identify-fake-job-offers/> [Accessed: Apr 07, 2019]

[4] A. Mittal, A. Slaughter & P. Zonneveld, “Protecting the connected barrels

Cybersecurity for upstream oil and gas”

Available:<https://www2.deloitte.com/insights/us/en/industry/oil-and-gas/cybersecurity-in-oil-and-gas-upstream-sector.html> [Accessed: Apr 07, 2019]

[5] Y. Schulz, “Reducing the risk of phishing attacks”, IT World Canada, 2016 [Online]

Available: <https://www.itworldcanada.com/blog/reducing-the-risk-of-phishing-attacks/388062> [Accessed: Apr 07, 2019]

[6] “FRAUD ALERT: BP Global Oil email scam and “spear phishing”, Lawyers' Insurance Association of Nova Scotia [Online]

Available:<http://www.lians.ca/sites/default/files/documents/FraudAlert-BP%20Global%20Oil%20email%20scam%20and%20spear%20phishing.pdf> [Accessed: Apr 07, 2019]

[7] J. Wagner, “The Threat of Cyberattack is Real For Oil And Gas Industry ”, The IT Team, 2017 [Online] Available: <https://theiteam.ca/energy-it/oil-and-gas-industry-cybersecurity/>

[Accessed: Apr 07, 2019]

[8] L. Segarra, “'Smishing' Is Internet Scammers' New Favorite Trick. Here's How to Avoid It”, Fortune, 2017 [Online].

Available: <http://fortune.com/2017/07/07/smishing-scam/> [Accessed: Apr 07, 2019]

[9] “Phishing Smishing - Can we trust any ecommunication?”, *Vaporstream Secure*  [Online] Available:<https://www.vaporstream.com/blog/phishing-smishing-ecommunication/> [Accessed: Apr 07, 2019]

[10] D. Harris, “'What Petroleum Marketers Need to Know About Mobile Device Fraud”, OPIS, 2018 [Online].

Available: <https://blog.opisnet.com/mobile-device-fraud> [Accessed: Apr 07, 2019]

[11] C. Linnitt, “Leaked: Internal RCMP Document Names “Violent Anti-Petroleum Extremists” Threat to Government and Industry, The Narwhal, 2015. [Online]

Available:<https://thenarwhal.ca/leaked-internal-rcmp-document-names-anti-petroleum-extremists-threat-government-industry/> [Accessed: Apr 07, 2019]

[12] S. Mccarthy, “‘Anti-petroleum’ movement a growing security threat to Canada, RCMP say”

The Globe And Mail, 2015. [Online]

Available:<https://www.theglobeandmail.com/news/politics/anti-petroleum-movement-a-growing-security-threat-to-canada-rcmp-say/article23019252/> [Accessed: Apr 07, 2019]

[13] I. Slav, “Catastrophic Cyberattacks Threaten Big Oil”, Oil Price, 2018. [Online]

Available:<https://oilprice.com/Energy/Energy-General/Catastrophic-Cyberattacks-Threaten-Big-Oil.html> [Accessed: Apr 07, 2019]

[14] “Social Engineering in Oil and Gas: Criminals are no longer hacking your firewalls and antivirus, they’re hacking your employees – Startech Business Systems”, *Energy Now*  [Online] Available:<https://energynow.ca/2018/07/social-engineering-in-oil-and-gas-criminals-are-no-longer-hacking-your-firewalls-and-antivirus-theyre-hacking-your-employees-startech-business-systems/> [Accessed: Apr 07, 2019]

[15] M. AlGhazal and M. AlJubran, “Cybersecurity for Upstream Operations”, Journal of Petroleum Technology, 2018. [Online]

Available: <https://www.spe.org/en/jpt/jpt-article-detail/?art=3748> [Accessed: Apr 07, 2019]

[16] C. Cooper, “What’s fueling cybersecurity concerns in the oil and gas industry?”, CSO Online, 2017 [Online]

Available:<https://www.csoonline.com/article/3191226/whats-fueling-cybersecurity-concerns-in-the-oil-and-gas-industry.html> [Accessed: Apr 07, 2019]

[17] J. Williams, “Six cybersecurity issues for oil and gas companies”, EY Global Oil & Gas, 2019 [Online]

Available:<https://www.ey.com/en_gl/oil-gas/six-cybersecurity-issues-for-oil-and-gas-companies> [Accessed: Apr 07, 2019]

[18] “Phishing Attacks In The Energy Industry”, *Infosec Institute* [Online] Available:<https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-attacks-in-the-energy-industry/#gref>

[Accessed: Apr 07, 2019]

[19] “Oil and Gas Industry Increasingly Hit by Cyber-Attacks: Report”, *Security Week* [Online] Available:<https://www.securityweek.com/oil-and-gas-industry-increasingly-hit-cyber-attacks-report> [Accessed: Apr 07, 2019]

[20] K. Boman, “The State of Cybersecurity in Today's Oil, Gas Industry”, Rigzone, 2016 [Online]

Available: <https://www.rigzone.com/news/oil_gas/a/147332/the_state_of_cybersecurity_in_todays_oil_gas_industry/> [Accessed: Apr 07, 2019]

[21] B. Rossi, “The oil and gas industry: prime target for email security threats”, Information Age, 2015 [Online]

Available:<https://www.information-age.com/oil-and-gas-industry-prime-target-email-security-threats-123460572/> [Accessed: Apr 07, 2019]

[22] W. Sizemore, “Drilling for Answers: Cyberattacks on the Rise in the Oil and Gas Industry”, IBM, 2017 [Online]

Available:<https://securityintelligence.com/drilling-for-answers-cyberattacks-on-the-rise-in-the-oil-and-gas-industry/> [Accessed: Apr 07, 2019]

[23] “Targeted Attacks Against the Energy Sector,” Symantec [online] Available:<https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf> [Accessed: Apr 07, 2019]