**ITSC-309 Social Engineering  
Final Project: Penetration Testing**

D’Artagnan Boocock, Aristotle Bui, Clayton Davidson,  
Jack Chen, Rhean Propp & Coleton Sanheim

Table of Contents

[**Introduction**](#_9okaw5uvb2t1) **2**

[**Target Overview**](#_6iosgvqyt7u3) **2**

[**Information Gathering and Report**](#_2ukdjzaoppfw) **3**

[Objectives](#_fhevdedu8vw5) 3

[Vulnerabilities](#_6868ay4t80yl) 3

[Data Gathering / Investigation](#_xk61trzes4f) 4

[Action Plan](#_le3tqa68fixu) 6

[Examples](#_c8jwdyunixxg) 7

[Discussion](#_95a4tkzh0cdi) 7

[**Conclusion**](#_w5jaqzx5wo2h) **8**

[**References**](#_lq243aum90cc) **9**

# Introduction

This report details a security audit of WestJet. WestJet is a Canadian airline, founded in 1994 and headquartered in Calgary, Alberta. It handles approximately 25 million passengers every year which makes it the second largest Canadian airline compared to Air-Canada.

As a major Canadian airline, it is important that WestJet can ensure security for its passengers and employees. Many Canadians use WestJet on a regular basis. It is important to the public that WestJet has proper security measures set in place that ensure the integrity, confidentiality and security of customer data. This extends beyond data to physical security. Airlines have a responsibility to ensure passengers arrive at their destinations safely. Our team chose WestJet as a target due to its Canadian origin, enabling the alleviation of any potential international liabilities. WestJet employs a bug-hunting policy known as “safe-harbour”, which ensures amnesty for auditors and rewards their findings.

# Target Overview

WestJet faces many security threats. These vulnerabilities threaten to cause financial damages, disruption of service, identity theft, and loss of life. The most common concern airline companies face is the threat of ransomware infecting their secure network and denying service to their customers. Data and credit card information can be compromised and lead to identity theft, fraud and significant collateral damages. Conventional threats still remain prevalent. These include criminal smuggling, human trafficking and terrorist hijacking.

WestJet is a prime target for social engineers. These attacks are often performed with the intent of financial gain. Smuggling and human trafficking share this primary motivation. The most direct threat airlines face is the possibility of a terrorist hijacking directly threatening the life of the passengers and crew of a flight. These kinds of attacks (which often require copious amounts of social engineering to perform) can have a multitude of motivations, from financial gain to political statements. Motivations for terrorist hijackings can vary.

# 

# Information Gathering and Report

## Objectives

We will be staging a pseudo-attack on the WestJet company. This attack will not be executed. Any and all information that is related to real-world data is purely coincidental.

The primary objective for this attack is to transfer money from the WestJet financial department to an offshore bank account. The secondary objective is to obtain account credentials of major IT and senior executive staff to have an effective hold over the company.

Social engineering will be strategized to accomplish these objectives. WestJet is expected to have tight security. This security transcends both computer networks and physical access. Airports are especially armed with rigorous security procedures. Due to this known variable, the attack we will strategize will not take place upon any airport premises. It will be a long and methodical approach to obtaining a powerful grasp over the company’s assets.

## Vulnerabilities

Human beings are the biggest vulnerability for any corporation. They do not often pay attention to their own physical and network security. Their focus is often on convenience and they are prone to trust people, rather than distrust them.

When selecting a target, there are several people to pick from. To achieve the goal of a financial transfer, a spoofing of authority is required. Our primary target is the chief executive officer of the company. When a CEO gives directions to their employees, employees listen. CEOs can be aware of “whaling” attempts to obtain personal information from them. Depending upon the situation, targeting lower level employees and escalating privileges within may be the most advisable strategy. Short-term or disgruntled employees can be an attractive starting target. These people can be used to escalate privileges within the company.This can be performed through verbal persuasion, bribery or stalking.

Public information shared on Social Media sites such as Facebook or LinkedIn can be extremely useful for choosing targets and exploiting social vulnerabilities within WestJet. Information such as job role, length of employment, city/area of residence, certifications, education is all shared publicly by many WestJet employees. Using this information in conjunction with the two pieces of critical information obtained from STEs, many types of attacks could be performed. Using a false identity to gain contact with payroll or HR could lead to more vectors of attack on the main target (CEO).

Once contact with the CEO or other executive has been established, gaining access to their credentials is the next step. This could be an ID number, email or password. Once obtained, pressure can be exerted on WestJet to comply with ransom demands.

## Data Gathering / Investigation

The objective of this project will be to obtain access to WestJet's CEO Alexis von Hoensbroech’s email account. Our group will approach this task through social engineering to obtain information about our target, then use software tools to acquire his login credentials. To accomplish this task, we decided the best method would be to approach lower level employees and move up the ladder, as this method arouses less suspicion. However; we are not closed to the idea of direct confrontation with the CEO if provided the opportunity. To accomplish our primary objective, we will be looking to document the following information: the email addresses of the executive members, any regularly occurring meetings, the physical addresses of any executives, and any ritualistic behaviors of the executives.

There are infinitely many hypothetical approaches to acquire the necessary information. Our group will explore some potential avenues of attack. A quick search of WestJet’s website reveals the names and faces of the entire executive team.

In one possible avenue of attack would be to acquire information about the company through their local head office. Knowing that WestJet’s head office resides in Calgary, it would be possible to stake out the building and follow one of the executives home. Depending on the time scale for the investigation, this task could be broken up to days, weeks or months, with different vehicles following different memberers. Over a period of time, it would be possible to learn the schedule of an executive meeting, specifically which days and times they meet.

Another avenue would be the social engineering of an executive member directly. WestJet’s website reveals Mark Porter, the Executive Vice-President of People and Culture, resides in Calgary. Following him home and staking out his residence would provide useful information, as it would reveal habitual behaviors (such as going to the bar, or attending sports events on a weekly basis). With this knowledge we could then perform social engineering by creating a situation that allows the target to interact with an auditor. The potential for tampering with; or physical material is also a possibility. If the target goes to the gym and leaves their phone or laptop in the locker, it would be possible to steal or extract the sensitive information. Knowing the address and schedule of the target also opens the opportunity for a breaking and entering attack, however; this method should be avoided as it is by far as it includes the most risk. These methods of attack can also be used in the previously discussed avenue of attack and is not strictly limited to Mark Porter. Any executive can be a target, but Porter is the only confirmed Calgarian.

The final possible avenue would be to socially engineer an employee and use them to obtain information. In this scenario, a reasonable target would be a flight attendant or a pilot. After a long day at work it would not be unreasonable to expect one of these individuals at a bar. This provides an opportunity to extract information, after a few beers. In this example the objective would be this access to this employee’s email, with any information regarding executive members as a plus. Through an employee email it would be possible to perform phishing attacks, as it would take a single click of a link to compromise the company's internal network. Phishing attacks are more effective when using an executive email, which means the first two avenues should be prioritized.

Assuming that any scenario is successful and we have physical access to a target’s phone or laptop, we should prioritize data collection, specifically copying the contents of a target’s machine. For PC’s using the tools “DumpIt” and “FTK Imager” can copy the contents of a machine's RAM. Additionally, “FTK Imager” and “Redline” can be used to copy the non-volatile data. A keylogger could be installed on a PC given momentary access and would allow for future data collection. For mobile devices, installing a remote access trojan (RAT) is a quick installation process, and would allow us to gain complete access to the phone. Another tool that can be used during the investigation/social engineering phase is “Maltego”, this tool can be useful for learning more about a target simply by entering an email.

## 

## Action Plan

In order to accomplish the objective of transferring funds to an offshore account, a person of authority needs to be socially engineered. The best candidate for this is the CEO of the company. After the initial data gathering phase, enough information should be collected on who the CEO is, who his primary contacts are and what his habits are. Through this information, we can begin our attack.

Attempting to gain access to the CEO’s local home wifi would be a great start for obtaining credential access. Being able to monitor network traffic would provide a great deal of information. Another avenue of approach would be installing a keylogger on the CEO’s machine. This could be done by paying cleaning staff to insert a USB into the machine on off-hours.

Alternatively, if the CEO cannot be reached directly, socially engineering another executive or a lower level employee is another strategy. The goal in this case would be to obtain credentials by infiltrating their machine and compromising the company network using phishing emails.

Once the credentials for the CEO’s company email address has been obtained, we can use that email to send a phishing attempt to the financial department. A command to transfer funds to an offshore account at a specific time will most likely be followed. If however we want more persistence within the company before we do this, a better plan would be to phish the financial department to upload malware onto their machine that will obtain login credentials.

After the malware has been running for a longer period of time, transactional statements and credentials will have been obtained. With these, a more sophisticated attack can follow that is more covert.

Obtaining the login credentials of IT staff could also be done through the CEO’s email address. It is more risky as the IT department is more aware of social engineering attempts, but if done right, malware can be uploaded and run undetected.

Through these methods, the company’s internal infrastructure can be compromised. With attackers having access to employee emails, financial login credentials and transactions, the amount of damage that can be done has the power to be irrevocable.

## 

## Examples

A similar attack to the one we’re outlining occured at a bank. Hackers were able to obtain the email address credentials of bank executives. Through these emails, the attackers were able to phish other employees and load malware onto their machines. The malware allowed them to see bank transactions and employee credentials. The attack netted hundreds of millions of dollars by transferring funds to offshore accounts and cryptocurrency.

Another notable example of a data theft is when “a Hong Kong-based airline lost 9.4 million passenger records, and a UK-based airline lost 9 million customer records to hackers. More recently, passenger records, including sensitive data such as credit card information and frequent flyer data of about 4.5 million customers of an Indian airline were breached.” (*Cyber resilience in the aviation industry: Sisa Blog,* 2022).

## Discussion

It is not challenging to obtain information about employees. It is shockingly easy. Social media accounts such as LinkedIn, Twitter, Instagram and Facebook provide wealths of knowledge about a person’s social contacts, their habits and personalities. The more information a person puts on the internet about themselves, the easier it is to construct a social engineering attack against that individual. Unless employees are carefully instructed not to post sensitive information online, social engineering will persist as one of the most effective methods for hacking a company.

Mitigation Strategies

Singular individuals are often the most vulnerable targets to attack. A company can only do so much to secure itself, but the individual security of the people who work there varies from person to person. It is often the case that unless an employee works in the information security field, they are not going to have sufficient home network and physical security.

It is the responsibility of WestJet to ensure their employees are well trained against intrusive attacks. Especially because the company is a large target for hackers. An airline has many responsibilities to public safety in both transportation and data security.

Employees should receive regular security training. Within that security training, information on how attackers use phishing to obtain information, spoof themselves as employee personnel and work their way through people to get to an end goal should be emphasized. Mitigations for these types of attacks exist. One of the biggest mitigations is employee education and awareness. Paying attention to things that seem out of the ordinary or abnormal.

# Conclusion

WestJet is an established company that has many good security practices already put into place. However, there is no such thing as one hundred percent security. A company of this size must regularly undergo security reviews and ensure staff are properly trained in security awareness, policy and procedures. In doing so, expensive and irrevocable damage can be avoided. The objective of security isn’t to reach one hundred percent security, but is to make yourself such a challenging target to break, that attackers will conclude it is not worth the effort and move on to another target.

# References

Bugcrowd. (n.d.). *WestJet's vulnerability disclosure program*. Bugcrowd. Retrieved August 7, 2022, from <https://bugcrowd.com/westjet-disclose>

LinkedIn. (n.d.). *WestJet | linkedin*. LinkedIn. Retrieved August 7, 2022, from https://www.linkedin.com/company/westjet

O'Neil, T. (2015, March 26). *How hackers stole millions from Banks all over the world*. Garland Technology. Retrieved August 7, 2022, from <https://www.garlandtechnology.com/blog/how-hackers-stole-millions-from-banks>

SISA. (2022, May 19). *Cyber resilience in the aviation industry: Sisa Blog*. SISA. Retrieved August 7, 2022, from <https://www.sisainfosec.com/blogs/cyber-resilience-in-the-aviation-industry/>

WestJet. (n.d.). *Who we are*. About us | WestJet official site. Retrieved August 7, 2022, from <https://www.westjet.com/en-ca/who-we-are/executive-team>