Company Security Report

Name: Christopher Luddy

Student Id: R00214236

Class: B-Y

Assigned Company Name: Fresnillo PLC

Student Gmail: [Christopher.luddy@mycit.ie](mailto:Christopher.luddy@mycit.ie)

Summary

Cyber risks for Fresnillo Plc and other companies have increased significantly due to the recent covid-19 pandemic and the advancements in new digital technologies. Since the mining company created a website, we can see there is an interest from cyber attackers due to the number of times the company has been saved from attacks since 2008. Throughout my research I found that the “crown jewels” of the company are their financial statements, client and internal communications, property such as machinery intellectual property and any investments that the company owns including physical buildings land and also in the stock market.

Icon

Description automatically generated

Table of Contents

[Summary 1](#_Toc86327555)

[**Task 1 (34 marks)** 2](#_Toc86327556)

[Company Overview 2](#_Toc86327557)

[Crown jewels/Assets 3](#_Toc86327558)

[Four Websites for Cybersecurity Awareness 3](#_Toc86327559)

[Eight Identified Malware 4](#_Toc86327560)

[Ransomware Overview 6](#_Toc86327561)

[**Task 2 (33 marks)** 7](#_Toc86327562)

[Digital Footprinting, Methods and How Employed 7](#_Toc86327563)

[Identified Company Weaknesses 7](#_Toc86327564)

[Solution To Identified Weaknesses 7](#_Toc86327565)

[Extending Company Policy to Social Networking 7](#_Toc86327566)

[**Task 3 (33 marks)** 8](#_Toc86327567)

[Social Engineering Overview and Effects on Assigned Company 8](#_Toc86327568)

[Physical and Digital Authentication Against Physical Access 8](#_Toc86327569)

[**References** 9](#_Toc86327570)

# **Task 1 (34 marks)**

# Company Overview

[Fresnillo plc](http://www.fresnilloplc.com/) is an UK domiciled Mexican precious metals mining company embodied in the United Kingdom. Fresnillo’s company headquarters is in Mexico City. Fresnillo is the world's largest silver producer from ore and the second-largest gold miner in Mexico. The mining company is located all over the world including London, Spain, Peru, and Mexico. The mining company launched their website in 2008 and still currently has a website. The companies’ competitors include [Pan American Silver Corp. (PAAS)](https://www.panamericansilver.com/company/) and also [Industrias Penoles SAB de CV (IPOAF).](https://www.penoles.com.mx/)

Throughout my research I found that the “crown jewels” of the company are there:

* Client and employee data. Client and employee data is valuable to Fresnillo plc if this data was stolen or leaked it would anger the employees and clients would put a bad name on the company leading to less sales in the long term.
* Property such as machinery/operating. Physical property such as machinery is also very valuable for the company. If the operating machinery gets damaged or stolen it can lead to a loss of a lot of money as mining and transport vehicles are highly expensive.
* Any investments that the company owns including physical buildings. In the stock market businesses have shares in a portfolio and so do retail investors. Retail investors who purchase Fresnillo plc stock are buying shares of the company in the hope of the company succeeding and making a profit. Fresnillo plc have their own shares of the company at a very high value and if the stock market was to crash then their shares would plumet and this would lead Fresnillo to lose a lot of capital and value not just from the shares but as a stock on the stock market.
* Land and also the capital in the stock market. Land is a long-term asset and can be sold as a fixed asset for capital, since Fresnillo plc is a mining company expanding and selling the land after it has been used to extract ore such as silver and gold id a crucial element to the company.

A picture containing sky, outdoor

Description automatically generated

# Four Websites for Cybersecurity Awareness

1. <https://www.shodan.io/search?query=http%3A%2F%2Fwww.fresnilloplc.com> I found that the Fresnillo web browser was issued by the server Apache, which has recently had an emergency update to fix incomplete patch for exploited bug.
2. <https://www.securitymagazine.com/> I found that Malware is using PowerShell tools to bypass powerful protections.
3. <https://www.webroot.com/ie/en/business/security-awareness> This website explains what security awareness training is and why businesses need security awareness training.
4. <https://portswigger.net/daily-swig/twitch-breach-leads-to-leak-of-source-code-and-streamer-earnings-data> Twitch breach leads to leak of source code and streamer earnings data.

# Eight Identified Malware

1. **Phishing**

Phishing is the psychological manipulation of people into leaking sensitive data or confidential information. This can differ from personal information to company confidential information. It is a technique used by criminals and cyber attackers to trick or con users into revealing the information. This type of threat would be dangerous for Fresnillo plc as human error would play a massive role and this would be seen as a disadvantage for the company phishing is the psychological manipulation of people into leaking sensitive data or confidential information. This can differ from personal information to company confidential information. It is a technique used by criminals and cyber attackers to trick or con users into revealing the information. This type of threat would be dangerous for Fresnillo plc as human error would play a massive role and this would be seen as a disadvantage for the company.

Examples include:

**Phishing**: These tactics include deceptive emails, websites, and text messages to steal the user’s information without the user knowing. Once a user interacts with the suspicious email, website, or text message then cyber criminals can steal the information.

To limit the risk of Phishing employees and personal working with and working for Fresnillo plc need to be trained not to open suspicious messages, emails, and website links. If something doesn’t look secure, then do not open it!

1. **Zeus**

Zeus or Zbot is a well-known banking Trojan horse program meaning this type of program is designed to breach the security of a computer system while ostensibly performing some innocuous function. This trojan bot steals important data from the users infected computer via web browsers and protected storage. Once infected, the computer sends stolen data to a bot command and control sever, where the data is stolen. Zeus is known as crimeware and is exchanged in the criminal underground as a kit for approximately $3,000-$4,000. It is likely one malware most utilized by criminals specializing in financial fraud. This would be very hazardous to Fresnillo plc as they are a company that deals in vast amounts of capital.

To remove Zeus from your device, follow these steps:

Step 1: The first step to removing Zeus is to use Rkill to terminate the Zeus Fake Windows Process.

Step 2: Use Malwarebytes to remove Zeus malware.

Step 3: Use the software HitmanPro to scan for the Zeus virus to see if the virus is still there.

Step 4: Use Zemana antimalware free to remove potentially unwanted programs.

1. **Nanocore RAT**

Nanocore is a high-risk RAT that provides the hackers with details on the device name and OS. This information is used to carry out various attacks such as manipulating confidential files, hijacking webcam, and microphone, stealing login credentials and more. This malware is very dangerous to companies as files, login details and confidential documents can get into the hackers’ hands. Fresnillo plc’ most important information such as confidential files including passwords, employee data, client lists and salaries.

Examples of Nanocore malware:

**Business email compromise:** Hackers calledkeyloggers are used to steal Office 365 credentials such as passwords and pins to gain access to financial information and other business critical data.

**Payload deployment:** This is when the user clicks the attachment that is sent to them and the trojan is uploaded on the device without any detection once the file is opened.

To remove malware like this manually is a very complicated task and can be done but usually it is best to allow antivirus or anti-malware programs to do this automatically. For best practise to avoid malware like Nanocore it is also advised not to interact with suspicious files or emails.

1. **Agent Tesla**

Agent Tesla was first discovered in late 2014, is it known as spyware focused on stealing sensitive information from a victim’s device, such as keyboard inputs (keylogger), saved application credentials, etc. The price varies between $25 to $65 based on the monthly or yearly subscription. This malware is also used to hijack bitcoin address information. The affected platform is Microsoft windows and impacted potential parties such as window users. This is a high risk for Fresnillo plc as hosting history shows us that the company was hosted on windows servers since 19-Feb-2017.

The removal of agent tesla is tough like any other virus and can leave you puzzled as it does too many modifications to the devices internal system. Complete removal of the malware is never fully ensured when removing manually. Thus, it is advised to scan the infected computer with reliable anti-malware programs to detect and remove the Agent tesla virus. SpyHunter use advanced threat detection technology to remove any sort of threat as it provides 24/7 protection from any unsolicited programs, vulnerability, or rootkit attacks.

1. **Ursnif**

Ursnif is a trojan malware is one of the most active variants of Gozi malware. It is spread by exploit kits, email attachments, and malicious links sent to manipulate the user of the system. Ursnif has been spread out by email and messages throughout 2016 and targeted vulnerable users in the United States, Australia, Canada, Italy, Poland, Switzerland, and also the United Kingdom. The attackers use Microsoft Word attachments with malicious macros to distribute Ursnif to USA victims, this if a giant threat for Fresnillo plc as they use Microsoft servers. This virus is designed to infiltrate systems without permission by using spam email campaigns. Removal of this malware is best left to anti malware programs and antivirus programs to do this automatically.

1. **Jupyter**

Jupyter trojian is a newly discovered malware stealthily steals usernames and passwords. The malware Jupyter is a campaign that targets businesses in an effort to steal usernames and passwords. The Jupyter installer is disguised in a zipped file, often using Microsoft Word icons and file names that look like they need to be opened urgently usually being pay rises or other important documents. This would be highly destructive for Fresnillo plc as the companies netblock owner is [Microsoft limited UK](https://www.microsoft.com/en-ie/default.aspx) leading me to believe that the company would be at risk as the stolen data could be sold or used to further attack the company. Hackers that attack the company using Jupyter would have access to passwords and usernames enabling then to steal sensitive data with ease. It is recommended that you eliminate possible malware infection, scan the computer system with legitimate antivirus software to remove the threat. To avoid catching this malware it is suggested to be wary of infected email attachments, malicious online advertisements, and also social engineering.

1. **Pushdo**

Pushdo is a downloader trojan meaning it main focus is to download and install additional malicious software. When the malware is executed into the computer system Pushdo reports back to one of several control IP addresses embedded in it its code. Then it pretends to be an Apache webserver. The malware keeps track of the victims IP address, steals passwords and banking information. To avoid catching this malware it is suggested that any unknown link or emails are to be ignored and any instant messaging chats are not to be interacted with. It is also recommended like other removals of malware that you eliminate possible malware infection, scan the computer system with legitimate antivirus software to remove the threat from the system.

1. **Dridex**

Dridex is a banking trojan spread by using emails containing malicious Excel documents. This trojan malware specialises in stealing bank credentials through a system that utilises macros from Microsoft Word. Excel documents are given exiting names such as “Invoice”, “Outstanding”, “Payment” or “Statement”. Fresnillo Plc is at risk due to banking information and passwords being lost a stolen by the Dridex malware. These banking credentials can be used to further gain access to the company’s capital. Removal of the malware is suggested that the user removes all possible malware infections and uses anti malware scans to eliminate the malware. Preventions of the malware is best done by not clicking into emails that have links on them and not interacting with excel documents with attractive names on them.

# Ransomware Overview

Ransome is a type of malware that attack that steals user data and holds the data hostage unless a ransom is paid. If not caught fast ransomware attacks can damage the company extremely as data that is stolen is sold on the Dark Web, leaking sensitive information public, and also destroying the stolen data completely. Although the data is returned when the ransom is paid off, it is still a risk to the company as attackers can save the data and publish or sell it later on. According to a report in 2020 by Cybersecurity insiders, 82% of cybersecurity professionals were most concerned about ransomware out of any other typical malware.

Crypto Wall is a type of ransom ware that can be very dangerous for Fresnillo. It is a ransomware that encrypts the files of infected computers in an effort to extract money for the decryption key. This means that the attacker will give the decryption key to the user once they pay up the ransom. After they pay, the user is allowed to download and run a file or application to clear the device from the threat. Removal of ransomware is very challenging and sometimes impossible to eliminate the malware from the system. The key is to minimize the likely hood that it penetrates the system. To prevent this ransomware from accessing the system in the first place it is advised that you do not click into any unknown suspicious emails and stay away from unsecured websites that may pass on the virus. Fresnillo plc once infected with ransomware would more than likely have to pay a large sum of money to the attacker which would slow down operations and damage the business.

Text

Description automatically generated

# **Task 2 (33 marks)**

# Digital Footprinting, Methods and How Employed

Digital foot printing is when the traceable digital activities, actions, communications, and contributions on the internet or on digital devices. All information and activities are stored as cookies. Businesses, organizations, and companies have a digital footprint. Digital footprint can be both positive and negative for users. On the positive side it is a great way to get personalised and targeted advertisements. The disadvantage of using cookies on websites is that strangers can piece together information about that individual very easily by only using search engines. **Passive** digital footprints can be stored and tracks the IP address. In an offline circumstance, administrators can access and view the machines actions without seeing who performed them. **Active** digital footprints can also be stored, and logs can show what actions the machine did and who preformed them. The owner of the system uses a keylogger to monitor the clipboard for and changes. This may be problematic as the keylogger may copy and save passwords or take screenshots of sensitive information. Removal is not as easy as clicking a button as the system has to be cleaned the files have to be deleted and a scan of the computer has to be done. It is recommended that an antimalware scan is used to securely double check that all the malware has been removed after an attack has been implemented.

# Identified Company Weaknesses

[https://pentest-tools.com/website-vulnerability-scanning/website-scanner#](https://pentest-tools.com/website-vulnerability-scanning/website-scanner)

I found that the overall risk rating for Fresnillo was a medium, which for a company like this dealing in such volumes of valuable metals and currency was quite concerning to me. The URL for Fresnillo plc’s webpage picked up evidence that the communication is made over unsecure, unencrypted HTTP. Once the communication from the server to the web browser is infiltrated then the attacker would be able to read and modify the data transmitted including credit card information, passwords, and other sensitive data. Have I been pwned has picked up breaches for the companies email ([IR@fresnilloplc.com](mailto:IR@fresnilloplc.com)), the most resent breach was in February 2019. This data can lead to compromised data such as Job titles, IP addresses, phone numbers, employers, emails, and physical addresses. <https://haveibeenpwned.com/> . The pentest website scanner picked up on the website that the communication is made over unsecure, unencrypted HTTP. This can lead to leaking of passwords and sensitive data and also credit card information.

# Solution To Identified Weaknesses

Communication served over HTTP is not encrypted which means that if someone is able to intercept it through an attack, they are able to see all the communication between your browser and the site you are visiting. They can even change the information that is going to your browser. Switching to HTTPS will secure and encrypt the server to make attacking it much more difficult for attackers. To secure the company’s website with HTTPS, It is recommended to reconfigure the website sever to use HTTPS which encrypts the communication between the web browser and the server.

# Extending Company Policy to Social Networking

Social networking uses social media and communication software to communicate with people across the internet. These conversations can be with colleagues, customers, clients, friends, and family. Social networking can be both for a social purpose and a business purpose through social media sites. These sites include Twitter, Snapchat, Instagram, Twitter, and Facebook. In a business environment this can be seen as a disadvantage as some social media activity can lead to bullying, negative feedback, damage to the company’s reputation and malware attacks such as phishing. It is however an advantage for the business too as data can be spread fast and easy, the company can extend its audience, have access to paid advertising and have a direct connection to the audience online through the company’s page. Threats include loss of IP address and sensitive data, reputation loss, effect of human resources such as bullying or explicit messages being spread and leaking of sensitive data. I would suggest the company Fresnillo plc to extend to social networking as bullying, sexual harassment, leaking of confidential information and other threats can ruin the reputation of a company. To prevent this, employees and personal in the company need to be aware of the dangers of the activities they do online. They need to be aware of social engineering and how to avoid falling for a scam or a phishing attack. They need to also be aware that bullying and spreading of false information about other employees is unacceptable and will be met with serious consequences.

# **Task 3 (33 marks)**

# Social Engineering Overview and Effects on Assigned Company

Social engineering is the psychological manipulation of people into leaking sensitive data or confidential information. This can differ from personal information to company confidential information. It is a technique used by criminals and cyber attackers to trick or con users into revealing the information. This type of threat would be dangerous for Fresnillo plc as human error would play a massive role and this would be seen as a disadvantage for the company.

Examples of social engineering are:

**Phishing**: tactics include deceptive emails, websites, and text messages to steal the user’s information. Once a user opens or even interacts with the suspicious email, website, or text message then cyber criminals can steal the information.

**Baiting:** these types of attacks use a false promise to manipulate the victim. They lure users into a trap that steals sensitive information or inflicts their systems with malware.

To limit the risk of social engineering employees and personal working with and working for Fresnillo plc need to be trained not to open suspicious messages, emails, and website links. If something doesn’t look secure, then do not open it. With the Covid-19 pandemic, this risk of attacks has increased mainly due to ‘phishing’ attacks and the increase in home working. Also, the total number of cyber security incidents affecting the Company has increased dramatically since the pandemic has started. A number of media mentions related to cyber security issues affecting the mining industry has also increased as hackers and keyloggers scramble to find the various valuable pieces of information to steal.

# Physical and Digital Authentication Against Physical Access

Several attacks have taken place recently from organised crime gangs, jeopardising the continuity of mining operations and the physical integrity of workers. The Security at mining facilities should be heavily increased for the safety and protections of employees and machinery. Pass codes and key cards can be used to control who has access to certain area of the building and access to files in the company. This allow keeps the employees, clients that are on site and staff safe physically and it also keeps their data safe as only employees have access to the data and not any casual civilian or attacker looking to breach and steal information. Digital this is harder to do but with biometric scanning and face id this allows authentication of staff through digital means. This also makes it harder for attackers to breach the system. Adding firewalls and encrypting servers helps. Cameras on site are essential to secure staff and employees. In the event of an accident, it can prove or disprove an argument it also can reveal the identity or any trespassers looking to damage the company’s property such as machinery or buildings.

# **References**

# 

[1] Apache released Apache HTTP 2.4.50 <https://www.bleepingcomputer.com/news/security/apache-emergency-update-fixes-incomplete-patch-for-exploited-bug/>

[2] Stock data history for Fresnillo plc <https://finance.yahoo.com/quote/FRES.L?p=FRES.L&.tsrc=fin-srch>

[3] Top ten malware 2021 <https://www.cisecurity.org/blog/top-10-malware-january-2021/>

[4] Phishing information <https://www.phishing.org/what-is-phishing>

[5] Zeus research <https://www.secureworks.com/research/zeus>

[6] Nanocore RAT malware of the month <https://spanning.com/blog/nanocore-rat-malware-of-the-month/>

[7] Agent Tesla analysis <https://www.riskiq.com/blog/external-threat-management/agent-tesla-trend-analysis/>

[8] Ursnif the new variant <https://www.fortinet.com/blog/threat-research/new-variant-of-ursnif-continuously-targeting-italy>

[9] Jupyter malware analysis <https://www.pcrisk.com/removal-guides/19483-jupyter-malware>

[10] PushDo <https://blog.trendmicro.com/trendlabs-security-intelligence/latest-pushdo-variants-challenge-antimalware-solution/>

[11] Dridex <https://redcanary.com/threat-detection-report/threats/dridex/>

[12] Removal of virus <https://www.pcrisk.com/removal-guides/13751-ursnif-trojan>

[13] Net craft site report <https://sitereport.netcraft.com/?url=http%3A%2F%2Fwww.fresnilloplc.com%2F>

[14] Way back machine: [https://web.archive.org/web/\*/http://www.fresnilloplc.com](https://web.archive.org/web/*/http://www.fresnilloplc.com)

[15] Why physical security matters <https://protectivesecurity.govt.nz/physical-security/why-physical-security-matters/>

[16] Social engineering <https://www.csoonline.com/article/2124681/what-is-social-engineering.html>

[17] Have I been pwned has picked up breaches for the companies email <https://haveibeenpwned.com/> using [IR@fresnilloplc.com](mailto:IR@fresnilloplc.com)

[18] Pentest scanner [https://pentest-tools.com/website-vulnerability-scanning/website-scanner#](https://pentest-tools.com/website-vulnerability-scanning/website-scanner) for the website <http://www.fresnilloplc.com/>