|  |
| --- |
| ProAktive News » Terrorism – what does it mean? |
| Individual Practical Assignment:  (Word count: 3706)  Jeremiyah Mathew Peter (222632529) |
| |  |  |  | | --- | --- | --- | |  | MIS781 Business Intelligence and Database | Practical Assignment | |

Table of content

[1. Introduction 2](#_Toc49946704)

[1.1 Objectives of BI Dashboards 2](#_Toc49946705)

[1.2 Benefits/Advantages of BI Dashboards 2](#_Toc49946706)

[1.3 Assumptions 3](#_Toc49946707)

[1.4 Description of business rules and of variables used in this report 3](#_Toc49946708)

[2. BI Dashboards) 5](#_Toc49946709)

[2.1 Dashboard 1: Attackers’ list For INTERPOL 5](#_Toc49946710)

[Chart 1-Identity 6](#_Toc49946711)

[Chart 2-Date 6](#_Toc49946712)

[Chart 3-Location 7](#_Toc49946713)

Chart 4-Pay……………………………………………………………………………………………………………………………………………………………………7

Chart 5-Offence count…………………………………………………………………………………………………………………………………………………..8

[2.2 Dashboard 2: Proprietary Organizations’ list 10](#_Toc49946714)

[Chart 1-Groups & Number of Members 10](#_Toc49946715)

Chart 2-Location………………………………………………………………………………………………………………………………………………………….11

Chart 3-Arrested v/s Killed………………………………………………………………………………………………………………………………………….12

Chart 4-Impact on victims……………………………………………………………………………………………………………………………………………12

Chart 5-Rating…………………………………………………………………………………………………………………………………………………………….13

[2.3 Dashboard 3: Victims’ List 14](#_Toc49946716)

[Chart 1-Companies & Purpose of Attack 15](#_Toc49946717)

Chart 2-Location………………………………………………………………………………………………………………………………………………………….15

Chart 3-Money owed……………………………………………………………………………………………………………………………………………….…16

Chart 4-Liquidation probability……………………………………………………………………………………………………………………………………16

Chart 5-Loss & Recovered money……………………………………………………………………………………………………………………………….18

[3. Recommendation 20](#_Toc49946718)

[4. Reference 20](#_Toc49946719)

5. Appendix (Certificate of Completion for Power BI Essential & Dataset) …………………..………………………………………………..21

# Introduction

This assignment is based on the severe attacks that happened to major companies in Australia. The master table of the attacks and its details are given in the Appendix 2. The attackers and their details are given in the dashboard 1, the proprietary groups the attackers were in, and their information are given in the dashboard 2 and the 3rd dashboard contains the details of the victims that were attacked. Dashboard 1 describes the identity of the attackers, date of attack, the pay they got from their proprietary groups, Number of cyberattacks they have in their record, and their location. Dashboard 2 contains names of organizations and their locations, the impact they had on their victims, their rating globally, their total number of members, number of members arrested and killed. Dashboard 3 contains information on victims and their locations, purpose of attacks, financial loss occurred, loss recovered, money owed to the stakeholders and their probability to go into liquidation.

## 1.1 Objectives of BI Dashboards

* **Objective 1 (For Dashboard 1-for INTERPOL)**

The primary aim is to find the attackers on the list who are still not caught. Dashboard 1 gives an overall description of each attacker and their background. The country locations and their IP addresses are enough to track their locations. They are visualised in a fashion in which they are easy to comprehend. The dashboard will give an overall idea about the cybercriminals to the Police.

* **Objective 2 (for Dashboard 2-for UN Counterterrorism Centre)**

Dashboard 2 represents the data on proprietary organizations from the attackers mentioned in Dashboard 1 come from. It gives the UN counterterrorism centre an idea about the terrorist groups aiming at each country’s economy. The centre can take necessary actions to eradicate these organizations and bring world peace.

* **Objective 3 (for Dashboard 3-for Australian re-insurance pool corporation)**

ARPC is a corporation in Australia which takes care of the recovery of companies from terrorist attacks. They insure companies against terrorist attacks. They help the company with the financial loss they suffer. This dashboard will advise the corporation on the financial status such as loss, loss recovered, money owed to stakeholders, and liquidation probability of each company so that the corporation can make swift actions to recover the loss and prevent companies from liquidation.

## 1.2 Benefits/Advantages of BI Dashboards

* Benefit 1 (for Dashboard 1)

Dashboard 1 will benefit the INTERPOL to recognise the pattern of crimes, finding the responsible one for attacks and convict them. The visualisation is done in a way to easily comprehend the criminal background, identity, locations, and seasonal background of attacks.

* Benefit 2 (for Dashboard 2)

Dashboard 2 will give the counterterrorism centre information regarding the level of threat each proprietary organization possess and details about the number of members yet to be caught and removed.

* Benefit 3 (for Dashboard 3)

Dashboard 3 gives the whole idea about the financial status of each company after the attack. It will give the insurance corporation complete data to take swift actions to recover the companies from their losses and prevent liquidation.

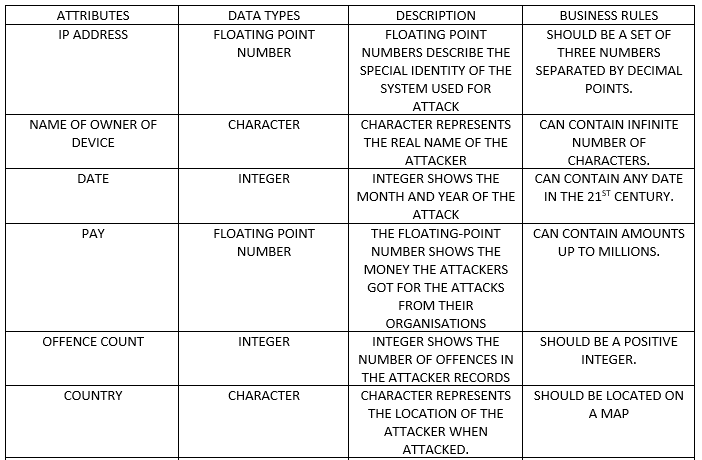
## 1.3 Assumptions

The findings and analyses identified by the dashboard are derived from an amalgamation of publicly available data sources identified in Table x.

**Table 1 Assumptions**

|  |
| --- |
| Assumption 1: The systems they used for attack are not destroyed yet and is with the owner |
| Assumption 2: The names of the owners are real which were found based on face recognition and fingerprints. |
| Assumption 3: Number of members, number of arrested and killed members of proprietary organisations are accurate according to the recent data. |
| Assumption 4: Money owed to stakeholders are separate from financial loss which should be recovered by the insurance corporation along with a part of recovered amount of loss |

## Description of business rules and of variables used in this report.



# A picture containing text, screenshot, number, font Description automatically generated

A picture containing text, screenshot, number, font

Description automatically generated

# 2. BI Dashboards

## 2.1 Dashboard 1: Attackers’ list For Interpol

This dashboard demonstrates the list of attackers who focused their attack on major companies and organizations in Australia whose details are provided in Appendix 2 – Master table and Appendix 3 – Attackers list. This dashboard will help the World police i.e., Interpol to have a clear picture of the attackers and investigate into these unsolved cybercrimes. Their location is provided so that Interpol can connect and cooperate with the corresponding countries to inquire and find the given attackers. Furthermore, the IP Addresses of the attackers can be used to track their moves, given it is not destroyed yet. The month and year they attacked denotes the companies’ financial seasons they aimed and the pattern and give a further outlook their further moves of attacks.

Figure 2.1

A screenshot of a computer

Description automatically generated with low confidence

|  |
| --- |
| 2 |
|  |

## Chart 1 (Identity)

The Table (figure 2.1(a)) Shows the IP Addresses of the systems the attackers used for cyberattacking, although it was registered under an alias name. A table was selected to represent the IP addresses and their corresponding names as a list. They had duplicate IDs with other names. But we were able to track down their real names matching their IDs (fingerprints included) in their country’s database. These real names along with their System addresses are given here to track them down using their system location, given, they possess their systems with them.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 2.1(a)

## Chart 2 (Date)

The month and year they selected for cyberattack are given in figure 2.1(b). Here also, a table was selected to show the dates in an order. After careful research, it was found that the time and month they used for attack were the peak time of financial gain and the time when their security systems were being reconfigured and updated for more security during the peak time. If we carefully watch the next targeted companies’ financial peak time and system reconfiguration time, we can calculate the time the attacks might occur and warn them before. We can also create a firewall in their systems and track down attacker’s location using a feature in firewall.

A screenshot of a calendar

Description automatically generated with medium confidence

Figure 2.1(b)

## Chart 3 (Location)

These were the countries they are from and the countries they were in for the attacks (figure 2.1(c)). Map visualisation is best for showing locations. Jane Doe and Litty Perrera are from Switzerland, although Litty Perrera is born in Portugal. Sarigama is from India, Sruthi Bala is from Sweden, born in India. Will smith attacked the target from Mexico to deviate his location from the police. He is from Texas, US. Jingle bells is from England, Jacob Gonzalez is located from Philippines. Jenovah Max is from Iraq while Manilla Barren is from Malaysia. All of them are members of international proprietary organizations and were equipped by their organizations.

## A map of the world Description automatically generated with medium confidence

*Figure 2.1(c)*

**Chart 4 (Pay)**

This bar chart (figure 2.1(d)) shows the pay the attackers got from their organization to do these attacks. A bar graph is chosen to represent the money in comparison with each other. Sarigama got the highest pay of $200,000. Sruthi Bala and Litty Perrera got the same pay of $160,000. Jacob Gonzalez got slightly less pay of $140,000. Manilla Barren got $120,000 and Jane Doe got $100,000. Jenovah Max’s, Jingle Bell’s and Will Smith’s Pay was low, it was below $50,000 ($50,000, $29,000 and $10,000 respectively). Jenovah Max’s and Jingle Bell’s attack caused a huge amount of loss for the companies in contrast with their pay.

A picture containing screenshot, diagram, font, plot

Description automatically generated

*Figure 2.1(d)*

**Chart 5 (Offence count)**

This doughnut chart demonstrates the number of times they were registered for the cybercrimes (figure.2.1(e)) The chart was chosen as it was a simple chart to show small numbers. Jingle Bells is the inexperienced one among the attackers in the list with only two times, although the second one caused a huge loss for the company. Sarigama and Litty Perrera are top of the notorious list with 8 offence count. Jenovah Max and Sruthi Bala comes right behind with 7 offences. Following them, Jane Doe, Jacob Gonzalez, Will Smith and Manilla Barren comes with 1 less count each respectively.

A picture containing text, screenshot, circle, colorfulness

Description automatically generated

*Figure 2.1(e)*

## 2.2 Dashboard 2: proprietary organizations’ list For UN counter-Terrorism Centre

This Dashboard includes every information of the Proprietary organizations the attackers were supported and equipped by. The proprietary organizations which are among the top 10 dangerous terrorist organization are being grown with a lot of people joining them each day. Most of the members are from poor background and are called upon for supporting their families. These Organizations send their members in various fields as target attackers, hackers, Bombshells and so on. The attackers from the master table (Appendix 1) are members of the corresponding organizations and they are professional hackers resourced by the groups to cause destructions to major companies and their countries’ economy. The dashboard contains information such as Number of members, Organization headquarters, Impact they had on the victim organizations (refer to master table), Number of members killed by the number of members arrested and finally the rating of danger level given by the START terrorism database.

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Figure 2.2 Dashboard 2

## Chart 1 (Groups & Number of members)

The major terrorist organisations have a lot of members joining them each day. Some are trained to kill, some are trained to cause financial destruction, some are trained for destroying national security such as taking control of their nuclear weapons. Altogether, the table (figure 2.2(a)) show the number of members joined them so far. It is shown in a table to show it as a simple list in order. Al-Qaeda has the highest number of members with 5500 in total while Sher-khan, a newly formed group has the least members. Hispan comes second with 5000 members, Ganchat and ISIS has the same number of members 4500 and NCS and OSC has 2400 members each. Santacruz, although new, grew up fast with 3000 members. PWZ has half of the number of members in Santacruz.

A screenshot of a table

Description automatically generated with low confidence

*Figure 2.2(a)*

**Chart 2 (Location)**

The world map shows the location of the headquarters of these organizations (figure 2.2(b)). Map is best for visualisation of locations. One important factor is that Hispan is an organization growing in Australia attacking the same country, if Australia takes necessary measures, it would be easy to phase off the organization within few years. NCS and Santacruz are from Brazil, two of the few organizations Brazil has. Sher-khan and PWZ are groups grown up in different parts of Indonesia. Ganchat is the only terrorist organization generated in India. ISIS and Al Qaeda are groups from neighbouring countries Iran and Iraq. OSC is a budding organization from Malaysia.

A map of the world

Description automatically generated with medium confidence

*Figure 2.2(b)*

**Chart 3 (Arrested vs Killed)**

This bar chart shows the details of number of members arrested v/s the number killed (figure 2.2(c)). We used a bar chart to represent both variables together. These members were arrested on their site or tracked down using their GPS locations and others killed on their site or given death penalty. These number includes virtual terrorists. Members from ISIS were the highest number who were arrested (900) while Hispan members were the most killed (200). Brazil groups NCS and Santacruz were among the most secured groups with same number of arrests and killed (250 and 76 respectively). Even though Al Qaeda is one of the oldest terrorist groups with 600 arrested, it has the second least number of killed (40). The least killed members’ group is OSC from Malaysia (30) and it was second least in arrested (260). Ganchat from India has 540 members arrested and 50 members killed. Though Sher-khan’s members are low, their arrested and killed numbers are high, showing that the intelligence group in Indonesia and Interpol have been successful in eradicating them. The other Indonesian group PWC has 500 members arrested and 45 killed. 109 members of ISIS were killed and 670 members of Hispan were arrested.

A picture containing text, screenshot, diagram, font

Description automatically generated

*Figure 2.2(c)*

**Chart 4 (Impact on victims)**

The pie chart shows the rate of impact they had on victim companies when they sent corresponding attackers to cyberattack (figure 2.2(d). Pie charts are best for showing variables in percentages. PWZ was most successful in destroying their victim. The company suffered destruction of 78% including capital and other resources. Hispan was 67% successful while Al Qaeda was 65% successful. Santacruz was the least successful with only 10% and OSC second least with 12%. NCS and ISIS was successful in destroying the network between the departments of their victim countries throughout Australia. However, they could not affect their financial ability, which is huge, as hard as their network. Their impact was 56% and 45% respectively. Sher-khan had an impact of 39%, They destroyed the cybersecurity of the company completely. The company might have had other attacks during this period which is not in this report as their firewall was down. Ganchat had an impact of 34% on their victim.

A colorful pie chart with numbers

Description automatically generated with medium confidence

*Figure 2.2(d)*

**Chart 5 (Rating)**

The Doughnut chart illustrates the global rating of danger level reported by the START terrorism database (figure 2.2(e)). This chart is used as it is easy to comprehend. According to the records, ISIS has the highest rating of 9/10. ISIS was able to create fear among all people of the world by brutal attacks on different parts of the world. They even trained children from a young age to cause fear among people. Al Qaeda has the second rating of 8. ISIS and Al Qaeda were the oldest and fiercest group people has known. NCS and Santacruz has a rating of 7 while OSC and Sher-khan has a rating of 5. PWZ obtained a rating of 6. Hispan and Ganchat have the least rating of the selected list with 3 and 2 respectively.

A picture containing screenshot, text, colorfulness, circle

Description automatically generated

*Figure 2.2(e)*

**2.3 Dashboard 3: Victims’ list For ARPC (Australian Reinsurance Pool Cooperation)**

The victims’ details from the master table are given to ARPC, the official Board of Australia which covers the insurance of the loss from terrorist attacks. It is given to cover the losses suffered by the companies as they are not fully able to come back to its operational stage without the Government supporting them. The companies have already recovered a part of their losses through pooling their assets and profits. This dashboard contains the details of purpose of attacks, loss they suffered, loss recovered by the companies and the money they owe to their investors and stakeholders. It also shows the probability of the companies going into liquidation. The list only consists of companies located in Australia.

A close-up of a graph

Description automatically generated with low confidence

Figure 2.3

## Chart 1 (Companies & Purpose of attack)

The Table shows the list of victims who were attacked by the attackers and organizations represented in the previous dashboards. It also contains details regarding purpose of attacks(figure 2.3(a). Table is used to understand easily. ANZ bank was attacked for financial robbery. By robbery, it was not meant an actual robbery of theft. It meant the security of the bank was penetrated through network and finance was leaked. Herald sun and Soman Group were attacked for taking control of their business and activities and malfunctioning it. Jay group LTD and Queensland university were asked for ransom after possessing the leverage data. The data of Queensland metro transport and Victorian metro transport such as its metro map and time stamps were obtained for creating havoc among the passengers in public. Sasi Group LTD was the victim of cyberterrorism and Tasmania Government confidential data were leaked for passing it to their rival territory.

A screenshot of a computer

Description automatically generated with medium confidence*Figure 2.3(a)*

**Chart 2 (Location)**

The Card shows the attacked location country which was Australia (figure 2.3(b). As there is only one variable shown, we chose a card. This database was selected for focusing on the few Global attacks Australia faced in the 21st century.

A black text on a white background

Description automatically generated with medium confidence

*Figure 2.3(b)*

**Chart 3 (Money owed)**

This bar chart contains the information regarding the money each company owes to their stakeholders (figure 2.3(c). Bar chart shows the comparison of the owed money. This money is around the money the companies look for their insurance board to cover. The owed money is around $200,000 for almost all companies except Herald sun who did not suffer much loss. The highest amount owed to investors and shareholders is $260,000 by Queensland university and Sasi Group LTD. Second comes ANZ bank with $240,000. Queensland metro Transport and Soman Group LTD incurred a loss of $220,000 owing to their stakeholders. Jay group LTD, Tasmania Government and Victorian metro Transport owes $200,000 each to their stakeholders. Herald sun has relatively a very low amount owed to the shareholders which is $20,000.

A picture containing text, screenshot, font, plot

Description automatically generated *Figure 2.3(c)*

**Chart 4 (Liquidation Probability)**

This pie chart shows the liquidation probability of each company which means the probability the company might see its end after the huge cyberattack they faced (figure 2.3(d). Pie chart is used to represent Percentages. Although, it might be nearly impossible to be liquidated because Victorian metro and Queensland Metro transport are an integral part of Australia’s Transport system, Their Probability to be end is 73% and 71% respectively due to the disrupt in causing fear among passengers which in turn means less revenue. Jay group LTD has the probability of 67% to be liquidated while its 54% probability for Queensland university because of the money they owe to their stakeholders. Sasi Group LTD, Tasmania Government and Soman Group LTD have a liquidation probability of 45%, 38%, and 34% respectively. ANZ Bank and Herald Sun have the least probability of 23% and 18% respectively.

A colorful pie chart with numbers

Description automatically generated with medium confidence

*Figure 2.3(d)*

**Chart 5 ( Loss & Recovered money)**

This Double stacked bar chart shows the loss each company suffered and how much they covered by their own money for which a part of the loss they expect the insurance to cover(figure 2.3(e).This chart is good when comparing two variables of the same cateogory, like here, loss and recovered amount is compared with each other of every company. From the graph, Victorian metro transport, Jay Group LTD and Sasi Group LTD has the highest difference in loss incurred and loss covered. Victorian Metro transport has the difference of $130,000 to cover for which loss was $700,000 and recovered amount was $570,000 and Jay group and Sasi Group each has $120,000 to cover. Jay group’s loss was $400,000 and the recovered amount was $280,000. Sasi Group had a loss of $260,000 and a recovered amount of $180,000. Queensland Metro Transport had a loss of $520,000 and recovered the amount of $500,000. They have only an amount of $20,000 to be recovered. Herald Sun suffered a loss of $50,000 and $36,000 was shown in records as recovered, they await for the insurance to recover the rest. ANZ has a loss of $340,000 and a recovered amount of $320,000. The difference is just $20,000. Queensland University’s amount yet to recover is $25,000 with $560,000 as a loss and $535,000 as the recovered amount. Tasmania Government had a loss of $300,000 and recovered the amount of $280,000, with only $20,000 more to recover. Finally, the Soman group has a difference of $20,000 to recover with a loss of $120,000 and a recovered amount of $100,000.

A picture containing text, screenshot, plot, diagram

Description automatically generated

*Figure 2.3(e)*

# 3. Recommendations

# 3.1 For INTERPOL

* Once a cybercriminal’s identity is caught, it would be beneficial to keep track of the systems he uses and the IDs he forms to arrest as soon as possible.
* A cybercriminal is as dangerous as any other criminal; therefore, Police must produce notices on them worldwide through virtual media.
* A cybercriminal’s accounts like bank accounts, social media accounts, license, should be frozen immediately when his identity is found.
* A cybercriminal can mask his identity and migrate to other countries, to prevent this, every airport must have a security system to identify them through facial recognition and fingerprints.

These additional precautions would aid in finding the responsible one and convicting them.

3.2 For UN COUNTER-TERRORISM CENTRE

* UN must gather every country to fight against these anti-social groups and eradicate them completely from the world.
* The centre should be informed about every group including newly bud groups by creating special anti-terrorism forces in every country which answer directly to the UN.
* The centre should supervise providing education and job opportunities to people to not let people from poor backgrounds get lured into these organizations.
* There should be additional security in nuclear weapons in each country as these groups’ primary aim is to destroy humanity and it can be done through nuclear weapons.

These would help in eradicating of anti-social groups and save humanity.

3.3 For ARPC

* There should be an immediate and quick assessment of the financial loss of an attacked company so that a company does not go into liquidation, it finally affects the economy of the country.
* Make sure every major company in Australia is a customer of ARPC.
* Thorough assessment to be done to detect fraud in financial status data and avoid overcompensation.
* As Australia’s cybersecurity is weak, Frequent attacks are expected, so additional backup funds should be availed from the Government for casualties.

These ideas wouldn’t help in erasing cyberattacks but will help in taking healthy measures of healing after an attack. ARPC would be the backbone of the companies for every casualties.

# 4. Reference

*Annual Reports*. (n.d.). ARPC. Retrieved May 17, 2023, from <https://arpc.gov.au/news-resources-arpc/annual-reports/>

*Get a competitive edge in business analysis with Power BI - Power BI Video Tutorial | LinkedIn Learning, formerly Lynda.com*. (2023, March 15). LinkedIn. <https://www.linkedin.com/learning/power-bi-essential-training-17362720/get-a-competitive-edge-in-business-analysis-with-power-bi?u=2104084>

# 5. Appendix (Certificate of Completion for Power BI & Dataset)

Appendix 1 – Certification of Completion

A picture containing text, screenshot, font

Description automatically generated

Appendix 2 - Master Table

A picture containing text, screenshot, number, line

Description automatically generated

Appendix 3 – Attackers List Dataset

A screenshot of a table

Description automatically generated with low confidence

Appendix 4 – Proprietors List

A screenshot of a table

Description automatically generated with low confidence

Appendix 5 – Victims List

A picture containing text, screenshot, number, parallel

Description automatically generated