***Business Intelligence tools legal issues involved in the secure exploitation***

**Introduction -**

This report will cover the legal issues involved in the secure exploitation of business intelligence tools. Discuss the impact of business intelligence tools and technologies for effective decision-making purposes and the legal/regulatory context in which they are used.

**Business intelligence and Data Security -**

Market leaders around the world appreciate reduced costs and increased efficiency, allowing them to make better decisions. The new era of business intelligence strategy has begun, focusing on data analysis. While most business leaders anticipate this to help them improve their business operations, very few consider the full ramifications of Business Intelligence.

**Vulnerabilities in exploring BI Security -**

The basic thing about security is that if you leave any data unattended, it will cause you enough damage. If you run enough data and generate it on a large scale, you need to have a system in place to maintain it safe. Market intelligence and data analysis are no longer linked to 1s and 0s, but to sensitive data that have always been prone to cyber-crime attacks.

If the hackers can access the analysed data, consider when they have the key to the whole operation, where they could actually hijack the whole programme. It's like a robber who visits a car garage to rob a few spare parts, swindling the entire car from the dealership shelf.

**Ensure the best Cloud Options -**

The first item that needs to be protected is the very Business Intelligence platform that is in use, and it involves tight security. Almost every company finds cloud to be an important part of its business and strategic approach, given the security concerns it still has.

Business Intelligence, along with blockchain, is a cost-effective way to use data efficiently, but cloud providers need to figure out a proper method that demonstrates how data is safeguarded. If you have an internal audit to look at the safety aspect and, when necessary, provide a secondary layer of security, there will be an added advantage.

**Encrypting Data -**

Understanding that criminals are always monitoring Business Intelligence more than anything else, one should insure the data is secure once it is unravelled. The data must be secured before it is saved or transferred to someone else, so that the intruder can search elsewhere.

The IBM Z Machine is one of those things that allows you to quickly encrypt massive data, nearly 12 billion transactions a day. If this is ignored, you will have to pay a heavy price for the infringement.

If you are capable of segmenting the data storage and network, it could be a strategic move, since solid data can be safe. That way, if a hacker is able to get into one segment, they won't be able to move to the next one, because the access mechanism is not accessible.

**Authenticate Permission and access -**

Business intelligence is a powerful tool, and accountability goes with control, so if power falls into the wrong hands, it can trigger tragedy. It is therefore also good to keep access to a limited number of people, even if you feel it is safe to communicate with all staff or stakeholders. Ensure that items are shared for supervisory or management purposes. Audit the function of each and every consumer who will work on a BI module or segment.

**Data Security and BI -**

Many business leaders agree that business intelligence is about gaining visibility into their companies, but most do not expect that BI can be used for security purposes. Business Intelligence can be used to analyse data that can spot network anomalies, network malfunctions, technological and other problems.

It can be used as a real-time problem solver, and you can track the data as it reaches the system and leave the company behind. So any suspicious conduct can be tracked and corrected thereupon. To translate, we may conclude that the breach of Equifax, which could not be detected by the rules, has culminated in such serious results that the details and personal information of millions of customers have been breached.

Once the core business intelligence target is reached and starts to show performance, never go back to match the old pre-BI techniques. Not only can you bring better outcomes with the legacy system, and it may expose the data to attacks. businesses sustain and become effective by keeping a tight firewall between market intelligence and security.

**Conclusion -**

In conclusion, this report will cover the legal issues involved in the secure exploitation of business intelligence tools. Discuss the impact of business intelligence tools and technologies for effective decision-making purposes and the legal/regulatory context in which they are used.

**References -**

Sowells, J. (2020). *Understanding Business Intelligence and Data Security*. [online] Hackercombat.com. Available at: https://hackercombat.com/understanding-business-intelligence-and-data-security/ [Accessed 26 Jan. 2020].