Mobile Adventures LLC

Christine Baxter

DeVry University, Keller Graduate School of Management

BIAM 530 – Week 7 Homework

Dr. Robert Burdwell

August 21, 2021

# Table of Contents

[Table of Contents 2](#_Toc80568784)

[Objective 3](#_Toc80568785)

[Player Data 3](#_Toc80568786)

[Valuable Asset 3](#_Toc80568787)

[Monetization of Data 4](#_Toc80568788)

[Major Threats against Data 5](#_Toc80568789)

[Policies and Procedures for Mitigating Threats 5](#_Toc80568790)

[Conclusion 6](#_Toc80568791)

# Objective

With the development and distribution of three popular games and two more on the horizon, Mobile Adventures LLC (MAL) executives want to explore how they can realize additional value from their collected player data and how that data should be managed and protected (DeVry University, 2021). This paper will first advise the leadership team on how to turn their player data into a valuable business asset, presenting several examples on how to monetize the collected data. Next, major threats will be identified. Lastly, policies and procedures will be recommended to manage and protect the company’s customer-specific data as well as their proprietary data (e.g., program code). Let’s start by reviewing what data is collected and then move to understanding how that collected data becomes a business asset.

# Player Data

MAL collects a variety of data on each player (or customer), including the player's e-mail address, type of mobile device, frequency and duration of game play, and highest level reached within each game. Customers pay an initial fee to download a game plus an annual subscription fee for continued access. In addition, MAL uses mobile advertising (ad) within the games for an additional revenue stream. The company also records each time a user views or clicks on an in-game ad. So, you might be wondering, how is this data converted into a valuable asset?

# Valuable Asset

Let’s start with discussing key performance indicators (KPIs). There are several KPIs for the gaming industry that can be used to determine game health and monetization metrics (Parmenter, 2021) which can guide the company on the popularity/revenue of the games it develops and distributes. The health metrics can assist the company in determining a game’s potential, its player retention and engagement, and gameplay time; whereas the monetization metrics can show the company various details like average revenue per paying user (ARPPU), daily active user (ARPDAU), monthly active user (ARPMAU), percentage of users who made a purchase that day (Conversion Rate), and average revenue per paying user across games on platform (ARPPU) (GameAnalytics, 2021).

MAL is already capturing the needed data to produce the metrics listed above. As an example, to determine a game’s potential, the frequency game play data will show how many players returned after 1 day of playing. If the day 1 retention is low, the game may need many improvements or a decision made to move onto next project/game (GameAnalytics, 2019). The frequency field can also be used for determining player retention and engagement with duration field being used for determining gameplay time. In addition, the DAU-to-MAU ratio can provide how many monthly users play each day.

To take the data even further, you can calculate an effective cost per mile (eCPM) metric which is the amount an advertiser pays another game/publisher per one thousand visitors (GameAnalytics, 2021). The views of in-game ads or clicks on in-game ads fields can be used to calculate click-through-rate (CTR) and cost-per-install (CPI) metrics (De Vries, 2021). With CTR, the company can measure the amount of clicks an ad receives against their total traffic and CPI calculates how much is paid for every user that installs your game. As you can see, the collected user data can be converted into information that the business can use for many informed, effective decisions. This brings us to a few examples of monetizing the collected data.

# Monetization of Data

When contemplating ways to monetize the collected data, several options come to mind. First recommendation is to strive for an understanding of user preference and their behavior, assisting in selection of which ad a user should get, when it should be presented, or which in-app virtual item/subscription plan to present for purchase (Freeman, 2021). For the second recommendation, MAL can use a player’s pursuit of status and recognition or achievement systems compelling players to stay with a given game. Another option is to encourage players to invest in a booster that will allow them to finish the current level instead of losing all progress. Now that we have reviewed recommendations for monetizing player data, let’s move onto discussing major threats to MALs data.

# Major Threats against Data

For any company that collects and stores customer data, it is imperative that proper systems and controls are in place for the many cyber threats in the world today. Threats such as malicious hackers using a cyberattack to compromise gaming company’s systems, hacking in-game valuables, and information-stealing malware are very real and policies/procedures should be put in place to combat or prevent such items (Rodriguez, 2021). These hacks can include customer/employee personal information but also confidential proprietary developer project code. Companies also need to ensure privacy laws/regulations are being followed appropriately. As an example, the European Union’s General Data Protection Regulation (GDPR) now classifies digital cookies as online identifiers which means they are subject to regulations where websites are required to gain consent prior to placement of those cookies on browsers (Germain, 2021). For a long time, digital cookies have been a default tracking mechanism and used to generate revenue through free advertising. As a result of the new regulations, many web browser companies are now turning off cookies by default. Threats are real and can be very damaging to a company’s reputation and overall business; however, there are policies and procedures that can significantly help ward off attacks on company and customer information.

# Policies and Procedures for Mitigating Threats

All the possibilities of being hacked can be overwhelming for companies There are a multitude of steps companies can take to protect themselves and their customer from the various threats. MAL will need to ensure their networks are monitored for abnormal traffic, implement security solutions that will help authenticate legitimate users and keep malicious activity out, keep users informed of known threats, and not only reporting on inappropriate bot or content behavior but also identify methods of detection and prevention (Roddie, 2020). For any financial transactions, it is imperative the company invests in/provides a secure online environment. Lastly, the company should consider cyber insurance for protecting the business and be sure to keep up with latest security risks and scams.

# Conclusion

In conclusion, when data is treated as an asset, an organization not only has improved decision-making abilities but also makes better judgement calls as well as produces more meaningful user insights (Duhe et al., 2019). For a quick recap, we have reviewed what data is collected, discussed why/how collected data becomes a business asset, provided recommendations to monetize player data, discussed major threats to MALs data, and wrapped up our discussion with policies and procedures that can be implemented to mitigate major threats.

References

De Vries, S. (2021). *CPI or CTR? how to best measure your game’s marketability.*

DeVry University. (2021). *Week 7 lab overview : Developing and managing databases for business intelligence - 61183 | week 7 lab scenario summary.*

Duhe, M., Gracie, M., Maroon, C. & Webre, T. (2019). *Data as an asset.*

Freeman, W. (2021). *Understanding player motivations – and how to harness their power.* Insights Hub

GameAnalytics. (2019). *Mobile gaming industry analysis for H1 2019.*

GameAnalytics. (2021). *GameIntel | benchmarks+.*

Germain, J. M. (2021). *Marketers need new strategies to parry cookieless advertising.*

Parmenter, S. (2021). *The metrics behind hyper-casual games (industry report).*

Roddie, M. (2020, -03-16). Player vs. hacker: Cyberthreats to gaming companies and gamers. <https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/>

Rodriguez, N. (2021). *Steam patches unlimited wallet funds exploit.*