Skynet
Security

Threat Risk Analysis

Money Bags Wealth Management

Project Lead: Patrick Murphy
Asset & Security Analyst: Israt Karim
Risk Analyst: Khandker Hasan

Table of Contents

Executive Summary

Skynet Security (SNS) has been contracted by Money Bags Wealth Management (MBWM) to perform a Threat Risk Analysis (TRA) on their new Market Prediction Initiative (MPI). The following report is a detailed account of the TRA Team's finding related to the MPI, related infrastructure, policies, procedures, and integrations as authorized by MBWM's CISO to be presented to all MBWM key stakeholders.

As a financial institution, the current security situation of MBWM has been assessed as inadequate. With respect to the MPI, there are critical risks and vulnerabilities present that are threats to the valuable assets which extends to MBWM business practices and reputation. The identified risks should be addressed to improve the security posture of MBWMs corporate infrastructure in order to pave the way for the esteemed success for the new MPI.

This report outlines the following with respect to the MPI at a high level: tangible and intangible assets, issues, key threats, remediation, risk reduction strategy, and risk register. Once the TRA has been completed and provided by all parties, it is highly recommended that MBWM begin an internal risk remediation process to action identified risk and vulnerabilities.

Recommendations can be categorized into three areas:

Web Application Vulnerability Remediations

- The web application should be moved to the cloud to take advantage of Microsoft Azure's built-in security controls. This enables Money Bags Wealth Management to increase the security of their application, as well as makes the scalability of the application better as their user base increases. Azure also offers a web application firewall to protect from many common application attacks.
- If the cloud is not your desired solution, the current web application code can be audited for any security risks and corrected to be as safe and secure as possible.

Administrative Controls

- A new password policy that complies with or exceeds the PCI DSS criteria should be implemented. Details of this can be found in the Remediation Options section of this document.
- Measures to ensure employee satisfaction should be taken to reduce the likelihood of a disgruntled employee leaking sensitive information or attacking the infrastructure themselves.
- Policy documents that define regular audit and inspection practices should be drafted to continually ensure the secure operation of the technological infrastructure of the company.

Server Configuration

- If MBWM does not want to migrate to the cloud, the configuration of the servers should be inspected for vulnerabilities and any that are found should be fixed to the latest recommendations.
- Servers should always have their software kept up to date with the latest updates and patches to avoid any known attack vectors.

Threat Risk Assessment

Identify Assets

Tangible Assets

TABLE 1: MBWM TANGIBLE ASSETS

Asset ID	Asset Name	Asset Type	Asset Owner
00001	Market Protection Initiative	Software	CEO
00002	Web Application Server	Server	Networking Team
00003	Web API	Software	Operations Team
00004	Production Server	Server	Production Team
00005	Development Server	Server	Development Team
00006	User End-point Terminals	Workstations/Laptops	Operations Team
00007	Firewall	Network Device	Networking Team
00008	Routers	Network Device	Networking Team
00009	Switches	Network Device	Networking Team
00010	Wi-Fi Access points	Network Device	Networking Team
00011	Email Server	SaaS	Operations Team
00012	FTP Server	Service	Operations Team
00013	Corporate Website	Service	Operations Team
00014	E-Business Platform	SaaS	COO
00015	Hand-held Devices	Smart Phones	CSO

Intangible Assets

- Employees/Personnel
  - Developers
  - Users
  - Managers
  - Contractors
- Intellectual Properties
- Industry Reputation
- Public Trust
- Investor Confidence
- Relationships with Global Stock Exchanges
- Relationships with Financial Institutions

Identify Issues

TABLE 2: MBWM KEY IDENTIFIED ISSUES

Issue ID	Issue Name	Issue Details
0001	Password Policy	The password policy does not require strong passwords and it is left to the individual user to create a strong password.
0002	No Firewall for Web Application	Because there is no dedicated firewall to protect the web application, this can allow internal and external threats to access through the single firewall. In case this firewall fails, the entire network could be exposed to multiple threats.
0003	Phishing attack	Employees aren't sufficiently trained against phishing attacks. General awareness against phishing attack is found to be poor.
0004	SQL injection	Web API and Web App are not properly configured with type-safe parameters for data access for which code inspection doesn't look for SQL injection. It leads to compromise database server and leak sensitive information.
0005	DoS/DDoS attack on Web API	There is no load balancer to protect the web App and web API from DoS or DDoS. No monitoring or filtering system also implemented which might be the weak point in favor of the potential attacker.
0006	Brute-force attack	Because of the weakness in the password policy and weak implementations of the web API, the website is vulnerable to brute-force attack.
0007	Server Misconfigurations	Web server software contains default user accounts enabled that a cybercriminal could utilize to access the system. Because of the misconfigurations of the server an adversary can fingerprint web application by leveraging server header information.

0008	Cross-site request forgery	There is no protection implemented against CSRF attack in the API. In Cross-Site Request Forgery (CSRF) an attacker forces a user to execute unwanted actions on a web application in which the user currently authenticated.
0009	Information theft	The lone firewall is a not a next-generation firewall, so there is no content filtering implemented. This makes the web App and API vulnerable to Identity theft, personal or financial information theft.
0010	Disgruntled Employees	Salary issue allows room for employee dissatisfaction, and also management is not properly monitoring to ensure that they act properly. Besides, employee relations are not a priority to the management. All these things may lead to the public disclosure of some dishonourable business practices conducted by the company which in turn might disrupt the reputation of the company.
0011	Weak Planning for Disaster Recovery.	Company doesn't have proper planning and facility of the backup, recovery and redundancy. Old school practice led to two occurrences of non-availability of the websites for few days.

Key Threats

The Key threats outlined in this section are what are believed to pose the greatest risk to the MBWM MPI project and infrastructure.

- Password Policy
- No dedicated firewall for the web application
- Phishing attack
- SQL injection
- DoS/DDoS attack on Web API
- Brute-force attack
- Server Misconfigurations
- Cross-site request forgery
- Information theft
- Disgruntled Employees
- Weak Planning for Disaster Recovery

Risk of Key Threats

The risks of key threats are calculated using the industry standard Risk Equation [1] below:

$$\text{Risk}_T = (\text{Probability}_T)(\text{Impact}_T)$$

Where:

Probability_T	= the likelihood the threat could occur with regards to the business
Impact_T	= how deleterious the threat is with regards to the business

Yielding:

Risk_T	= the risk of a threat currently facing a business

The equation will provide each risk with a numeric score and will allow comparisons between the other risks facing MBWM. The probability and impact will be given a total score out of 10. Once these numbers are multiplied, they yield a numeric score out of 100 that will demonstrate the severity of each risk. Below is an assessment of all the key threats listed above. Please see *TABLE 3: MBWM RISK RANKING (page 9)* for a risk evaluation using the Risk Equation.

Password Policy

While there is a password policy in place at MBWM, it does not meet the accepted industry standards for passwords. The password policy needs to ensure that users have strong passwords that will protect sensitive user-accessible information. Also, the password policy in place does not differentiate between administrative accounts or user accounts. Because of the non-compliant password policy MBWM website is vulnerable to password attacks which also include brute-force attacks. In a password attack, simply hacker tries to steal password. Because passwords can only contain only some letters and numbers it is easy to guess and steal. Hackers know that most of the time passwords are poorly designed, and sometimes companies do not follow password policy best practice. So password attacks will remain a threat as long as non-compliant passwords are being used.

No dedicated firewall for the web app server

Web Application and Web API are the two most important and valuable assets of the company which is directly connected with the company business with the client. Protecting these two items is of prime importance. Because there is no dedicated firewall to protect the web application located in DMZ, this can allow internal and external threats to access through the firewall. In case this firewall fails, the entire network could be exposed to multiple threats. Besides, this firewall is also not a NGFW (next-generation firewall), it doesn't do any content filtering making relatively easy access for the malicious attackers.

Phishing attack

In Phishing hacker normally motivate internal company user to download malware. Compromised accounts are used for this technique and usually occur via email. These emails come from trustworthy source for example known partner, customer or known co-worker. Hackers construct a thanks message to motivate users that designed to look genuine, and which usually require the receiver to take some form of action. If employees aren't sufficiently trained against phishing attacks or web application software isn't sufficiently updated against malware then it gives the hacker to establish C2C to the company's infrastructure.

SQL Injection Through the Web Application

SQL Injection is a type of attack by which attacker execute malicious SQL statements. They control a database server behind a web application and can bypass the application security measures. Criminal can use authentication and authorization of a web page or web application and recover the content of the entire SQL database for example customer information, personal data, trade secrets, intellectual property, and more. They can also add, modify, and delete records in the database. If there is no There is no web application firewall, Code inspection doesn't look for SQL injection, or new features are not properly inspected then it lead to compromise database server and leak sensitive information.

DOS or DDOS Attack

In Denial-of-service (DoS) attacks, the goal of the attacker is to make websites or applications unavailable to legitimate users by disrupting services by devastating them with fake network traffic. Attackers send so many repeating web requests to an app or API, overfilling systems and causing a disruption in service. In DDoS attacker does not target specific data, but instead make a website, app, or API unreachable. As a result, DDoS attacks hold data "hostage" by making it unavailable to end users. If API does not implement a load balancer or Traffic to API is not monitored and filtered it might be the weak point for the attacker to lunch DoS or DDOS.

Brute Force Attack

In a brute force attacks, an attacker attempt to gain access to an account or secured system by constantly entering credentials manually or in an automated way. The attacker lunches this kind of attack in order to uncover passwords to get into the accounts, and discover hidden URLs to find sensitive data, or decrypt passwords from a leaked data. Hackers might try to get into the backend of the website to compromising it or drop some malicious code.

Security Misconfiguration of Web Server

Security misconfiguration is a threat which takes place when an application component is vulnerable to attack because of insecure configuration option. For instance, web server software might have default user accounts that a cybercriminal could utilize to access the system. Or the software might have a known set of standard configuration files or directories, which a cybercriminal could exploit. In some software development there are some vulnerable services enabled, such as remote administration operations. So, the attacker can cause the application to be vulnerable to attacks and target any component of the application stack by this service.

Cross-site Request Forgery

In Cross-Site Request Forgery (CSRF) an attacker forces a user to execute unwanted actions on a web application in which the user currently authenticated. Attacker use little trick of social engineering (such as sending a link via email or chat), to the users of a web application to execute an action of the attacker's choosing. If the target is a normal user, a successful CSRF attack force the user to make state changing requests like transferring funds, changing their email address, and so on. If the target is an administrative user, CSRF can compromise the entire web application.

Personal Information Theft

In Identity theft, the attacker uses victim's personal or financial information without his permission. They might steal victim name and address, credit card, or bank account numbers, Social Security number, or medical insurance account numbers and use them. Hackers might obtain that information by breaching data or if a user enters that information on a public computer or an insecure website.

Backup & Redundancy

Business continuity and disaster recovery is of highest priority for any business organization today. Any negligence in this important issue leads to business loss, financial loss, and degradation of company reputation and public trust. It has been revealed that MBWM doesn't have proper planning and arrangement of the backup, recovery and redundancy. Old school practice led to two occurrences of non-availability of the websites for few days. This issue had been pointed out by some other company earlier, but the company failed to implement that.

Risk Ranking

TABLE 3: MBWM RISK RANKING

Ranking	Risk Name	Probability (1-10)	Impact (1-10)	Total (Out of 100)
1	Password Policy	8	8	64
2	Brute-force attack	8	7	56
3	No Firewall to protect Web App	8	7	56
4	DoS/DDoS attack on Web API	6	8	48
5	Phishing attack	6	8	48
6	Disaster Recovery	8	6	48
7	SQL injection	5	9	45
8	Disgruntled Employees	4	9	36
9	Information theft	3	9	27
10	Cross-site request forgery	3	8	24
11	Server Misconfigurations	4	4	16

Desired Outcomes

Skynet Security understands that the desired outcome of this Threat Risk Assessment is to have most or all high risks are mitigated. This includes but is not limited to a modification to administrative controls, technical controls, the purchase of hardware, etc. (depending on the mitigation proposals.)

Remediation Options

At Skynet Security, we believe providing multiple pathways an organization may take to secure their infrastructure. Different companies have different needs and methods of operation, and the best solution varies depending on these. With this in mind, we have prepared two different remediation options, one of which involves more money spent on external products as solutions and one of which involves more internal employee time spent working on the solutions. These options may be mix-and-matched; however, we recommend that one of the options is implemented for each listed category to ensure secure coverage of Money Bags Wealth Management's technological infrastructure.

Option A – External Product Focused

Cloud Migration

Migrating the entire technological infrastructure to the cloud could help reduce many of the risks that Money Bags Wealth Management is currently facing. Some of the main advantages that cloud solutions offer include redundancy of hardware for increased uptime, increased application security, and ease of user management. They also have load balancers implemented and can protect you against DDoS attacks. Cloud services include protective options against many of the threats with the highest risk ratings, like web application firewalls and user management policies.

We recommend migration to Microsoft's Azure cloud platform. Azure Active Directory allows ease of user management for company IT administrators. It also offers extreme flexibility over the services you choose to purchase, with a myriad of useful options to consider and it can also be scaled up with the growth of Money Bags Wealth Management's customer base.

Our recommendation is to begin with the Isolated Service plan for hosting the web application and API, using the I2 instance option. This will cost Money Bags Wealth Management approximately $555 each month, for a total of $6660 per year [1]. This amount may increase or decrease depending on the bandwidth needed for the web application but can easily be increased as the company's user base enlarges.

For migrating the company's database to Azure, it is recommended that Money Bags Wealth Management chooses the Gen 5 Standard Series vCore 4 database plan at $674 per month if a 3-year plan is selected. This comes out to a yearly expense of $8088 [2]. The resulting total yearly expense for both plans is $14,748.

This solution ends up being relatively inexpensive for such a large company and offers immense flexibility and security, therefore we consider it the best option for Money Bags Wealth Management. It is also generally a relatively simple switch for many technological professionals to make, as many are already familiar with Microsoft's software environment.

Web Application Firewall

Due to the high calculated risk of SQL injection, cross-site scripting, and data theft Skynet Security recommends that Money Bags Wealth Management purchases and installs a web application firewall to mitigate these risks. If the company decides to migrate to Microsoft Azure's cloud services, Azure has a web application firewall available as an optional feature. This would ease the installation and configuration of the firewall, and those familiar with Microsoft software will feel comfortable working with it instantaneously.

Skynet Security recommends the medium type of the Web Application Firewall Application Gateway option for your security needs, along with the medium sized option for data processing. The monthly cost of this option is estimated at $170 per month [3]. The price varies based on the number of users and amount of data to be processed. This option an also easily be scaled with the size of the user base as MBWM's user numbers continue to grow.

Password Policy

The current password policy at MBWM allows for weak passwords and contains vulnerabilities that an attacker may exploit. We recommend that the password policy is updated to comply with or exceed the PCI DSS compliance criteria. If the infrastructure is migrated to Microsoft Azure, password policies can be easily defined and enforced through Azure Active Directory's administration portal. The current password policy contains the following requirements:

1) Minimum length: 7 characters
2) Logged history: 12 months
3) Password cannot be reused if it is in the user's logged history
4) Maximum duration: 100 days
5) Complexity requirements:
   a) Password cannot contain the user's username
   b) Password must contain at least one uppercase letter
   c) Password must contain at least one lowercase letter
   d) Password must contain at least one number
6) Lockout threshold: 10 attempts
7) Lockout duration: 10 minutes

Our recommendation to increase the security of the password policy is to implement the following changes for standard accounts:

1) Minimum length: 10 characters
2) Logged history: 24 months
3) Password cannot be repeated if it is in the user's logged history
4) Maximum duration: 80 days
5) Complexity requirements:
   a) Password cannot contain the user's username
   b) Password must contain at least one uppercase letter
   c) Password must contain at least one lowercase letter
   d) Password must contain at least one number
   e) Password must contain at least one symbol
6) Lockout threshold: 5 attempts
7) Lockout duration: 30 minutes

For administrator or high-privilege accounts, we recommend the following requirements:

1) Minimum length: 12 characters
2) Logged history: 36 months
3) Password cannot be repeated if it is in the user's logged history
4) Maximum duration: 30 days
5) Complexity requirements:
   a) Password cannot contain the user's username
   b) Password must contain at least one uppercase letter
   c) Password must contain at least one lowercase letter
   d) Password must contain at least one number
   e) Password must contain at least one symbol
6) Lockout threshold: 3 attempts
7) Lockout duration: until reset by an administrator

Employee Satisfaction Measures

Disgruntled employees are a common source of data leakage and infrastructure attacks. They can do a lot of damage because they have more intimate knowledge of the technology in use and any potential vulnerabilities it may have, as well as ease of access compared to outsiders. The best way to mitigate against these is to ensure that employees are as satisfied with their work environment and tasks as possible. We recommend that MBWM executives get together and draft a plan for employee retention and satisfaction. This will also aid in attracting the best possible candidates to the organization, resulting in a more productive staff which will help the company to continue to flourish.

We recommend that a document be drafted that defines a policy for surveying employee satisfaction and gathering data on which areas workers are most and least satisfied with. This will help the company understand where it is doing well at fostering employee satisfaction and where it has room for improvement. We also recommend a separate policy document to define a process for auditing current salary and bonus numbers and comparing them to other, similar companies to ensure that MBWM remains competitive in the employee marketplace and its employees remain content with their employment situation.

Option B – Internal Work Focused

Complete Code Audit

SQL Injection, cross-site attacks, and data theft can all be mitigated through the writing of secure code. One option for reducing the security risks to Money Bags Wealth Management is to dedicate a team of developers with knowledge of secure code to audit the current web application. Any locations in the code where data is transferred between locations should be inspected for flaws that can be exploited.

We recommend that a team of 2-3 developers who have knowledge of security best practices be dedicated to auditing the current web application code, and that a policy is drafted that stipulates the frequency of auditing, as if this solution is chosen the code should be continuously inspected to ensure any new code added to the application is safe and secure. Having multiple developers on this project will help ensure that nothing will go overlooked because dedicating as many eyes and brains as possible to the task will observe more locations where the code can be improved.

Server Configuration Audit

The configuration of the on-premises servers can also leave hackers room for exploitation. In order to mitigate the risk contained in the server configurations, Skynet Security recommends that the servers also go through a complete configuration audit, done by IT professionals with knowledge of secure server configurations. This will involve inspecting the settings and configuration files of each server to ensure that all potential vulnerabilities and ensuring the software that is running on the servers is updated and patched to remove known attack vectors.

We recommend that a team of 2-3 IT professionals who are trained in secure server configuration to audit the servers, and that a policy is drafted that defines the frequency of server auditing and the process that the audits will follow. If this solution is chosen, similar to the code audit recommendations, the servers must be continually inspected to ensure that they contain as many mitigations as possible to deter potential attackers. Having a multi-person team on this task will ensure that at many vulnerabilities as possible are noticed and fixed.

Anti-DDoS Guardian

If the servers are kept on-premises, a solution to mitigate the potential for DDoS attacks should be implemented. Anti DDoS Guardian, an anti-DDoS software developed by BeeThink, helps prevent DDoS attacks from bringing Money Bags Wealth Management's servers down. It is effective against many DoS and DDoS attack methods, including SYN attacks, IP flood, TCP flood, UDP flood, ICMP flood, slow HTTP DDoS attacks, and Layer 7 attacks.

Skynet Security recommends that 2 licenses are purchased, one for the web application server and one for the database server. Each license costs $134, which comes to a total price of $268 [4], a small price to pay for protection against attacks that can bring the entire application infrastructure offline.

Password Policy

The current password policy at MBWM allows for weak passwords and contains vulnerabilities that an attacker may exploit. We recommend that the password policy is updated to comply with or exceed the PCI DSS compliance criteria. If the infrastructure is migrated to Microsoft Azure, password policies can be easily defined and enforced through Azure Active Directory's administration portal. The current password policy contains the following requirements:

1) Minimum length: 7 characters
2) Logged history: 12 months
3) Password cannot be reused if it is in the user's logged history
4) Maximum duration: 100 days
5) Complexity requirements:
    a) Password cannot contain the user's username
    b) Password must contain at least one uppercase letter
    c) Password must contain at least one lowercase letter
    d) Password must contain at least one number
6) Lockout threshold: 10 attempts
7) Lockout duration: 10 minutes

Our recommendation to increase the security of the password policy is to implement the following changes for standard accounts:

1) Minimum length: 10 characters
2) Logged history: 24 months
3) Password cannot be repeated if it is in the user's logged history
4) Maximum duration: 80 days
5) Complexity requirements:
    a) Password cannot contain the user's username
    b) Password must contain at least one uppercase letter
    c) Password must contain at least one lowercase letter
    d) Password must contain at least one number
    e) Password must contain at least one symbol
6) Lockout threshold: 5 attempts
7) Lockout duration: 30 minutes

For administrator or high-privilege accounts, we recommend the following requirements:

1) Minimum length: 12 characters
2) Logged history: 36 months
3) Password cannot be repeated if it is in the user's logged history
4) Maximum duration: 30 days
5) Complexity requirements:
    a) Password cannot contain the user's username
    b) Password must contain at least one uppercase letter
    c) Password must contain at least one lowercase letter
    d) Password must contain at least one number
    e) Password must contain at least one symbol
6) Lockout threshold: 3 attempts
7) Lockout duration: until reset by an administrator

Employee Satisfaction Measures

Disgruntled employees are a common source of data leakage and infrastructure attacks. They can do a lot of damage because they have more intimate knowledge of the technology in use and any potential vulnerabilities it may have, as well as ease of access compared to outsiders. The best way to mitigate against these is to ensure that employees are as satisfied with their work environment and tasks as possible. We recommend that MBWM executives get together and draft a plan for employee retention and satisfaction. This will also aid in attracting the best possible candidates to the organization, resulting in a more productive staff which will help the company to continue to flourish.

We recommend that a document be drafted that defines a policy for surveying employee satisfaction and gathering data on which areas workers are most and least satisfied with. This will help the company understand where it is doing well at fostering employee satisfaction and where it has room for improvement. We also recommend a separate policy document to define a process for auditing current salary and bonus numbers and comparing them to other, similar companies to ensure that MBWM remains competitive in the employee marketplace and its employees remain content with their employment situation.

Security Training

Since option B is so dependent on employees applying their security knowledge to the technological infrastructure of Money Bags Wealth Management, we recommend that employees are trained in security best practices. This is a good idea to ensure the security of your business in any case; however, if option B is chosen it is essential to have employees who have an in-depth knowledge of security practices.

Global Knowledge offers many cyber security courses for reasonable prices, including their Polaris Accelerate option. This comes at a cost of $480 per employee per year. With MBWM's current technology staff of 12 employees, the resulting cost is $5760 per year [5]. Some employee time must also be set aside for them to work toward completing these courses, we recommend either weekly or bi-weekly time slots be set aside for employees to study for and complete these classes. Although this represents a large amount of employee time, the benefits will propagate through the entire organization and benefits will be obtained as long as the trained employees continue to work for Money Bags Wealth Management.

Risk Reduction Strategies

We at Skynet Security believe that the most effective risk mitigation strategy is to migrate as much of your infrastructure as possible to a cloud service and use their integrated features. This option has the most flexibility and involves the least employee hours. Although there will be a transition period, the time and effort involved in migrating to the cloud will be less than the amount used to dedicate the necessary resources to auditing the on-premises infrastructure.

If you would like to maintain the current infrastructure, then the web application and server configurations should be inspected to ensure they are as up to date as possible, and any insecure code or configuration is changed to ensure security best practices. Employees should also be informed on how to create and maintain secure web applications.

The minimum mitigation necessary to improve MBWM's security posture is to update the software running on all servers and workstations, implement the recommended password policy, and add a web application firewall to deter many of the most common cyber-attacks.

Methods for Monitoring Risk

Outlined here are several guidelines to continue tracking the main risks for Money Bags Wealth Management. Monitoring the potential attack vectors is essential to maintain the continued secure functioning of MBWM. Using the information contained in the following guidelines will allow the organization to follow the current threats to the company and tailor their relevant plans in the future.

Event Logs in Azure Active Directory

If migrated to the cloud, Azure Active Directory (AAD) can be configured to log many different types of security events. It has many security options in its configuration, gathering data on login attempts, locations, IPs, and many more. Using the data contained in AAD's logs can allow you to determine when and where threats may be coming, which accounts may be breached, and any anomalous activity from the users.

Web Application Firewall Logs and Alerts

The Azure Web Application Firewall watches and logs traffic to the web application. This data can show what types of attack malicious actors are using against your web application. Preventative measures can then be applied to ensure the continues security of the web application.

Data from Employee Surveys

The surveys given to determine employee satisfaction can help steer the company and its culture in direction mutually beneficial for all involved parties. Data gathered can aid in decisions on what employees need to continue working effectively and keep them satisfied enough not to be a liability.

SIEM Logs for Unauthorized Events

The SIEM used by Money Bags Wealth Management should be tuned to track suspicious events. It will monitor activity across the network, ensuring that anything anomalous activities will be noticed and alerted. This information can be used to make decisions about how to track vulnerabilities going forward.

Anti DDoS Guardian Logs

If BeeThink's Anti DDoS Guardian is installed, it logs all network traffic and can be tuned to track more detail when it detects suspicious activity. Any interesting packets will be logged, and it breaks traffic down by port, allowing a detailed look into what is happening on your servers.

Projected Risk Scores after Mitigation

Table 4: MBWM Projected risk after mitigation

Ranking	Risk Name	Probability (1-10)	Impact (1-10)	Total (Out of 100)
1	Password Policy	2	8	16
2	Brute-force attack	2	7	14
3	No Firewall to protect Web App	2	7	14
4	DoS/DDoS attack on Web API	2	7	14
5	Phishing attack	2	7	14
6	**Disgruntled Employee**	2	5	10
7	SQL injection	2	7	14
8	Disaster Recovery	1	9	9
9	Information theft	2	7	14
10	Cross-site request forgery	1	8	8
11	Server Misconfigurations	1	4	4

Threat Metrics

Threat Metrics tables provide a summarized overview to help evaluate the applicable threat level of the given threats, and an overall image of how critical it is to address various threats based on how they are categorized to impact the organisation. The main threat metrics that fall in the scope of this evaluation is: the likelihood of a threat being realized; the impact of the downtime of an asset; the theft or breach of an asset; and the risk associated with potential threat actors.

The following legend will be used for tables and matrixes below:

Severity Rating	Very low	Low	Moderate	High	Critical
Numeric Value	1-2	3-4	5-6	7-8	9-10

Likelihood of a Threat

Table 5: Standard Likelihood of a Threat Matrix

Frequency of Unauthorized Access/Attack/sabotage	Frequency Descriptor
Rare	Will likely not occur in the evaluated time frame
Unlikely	Should not be expected to occur, but is a possibility
Possible	May occur, and should be accounted for
Very likely	Will likely occur, and re-occur on a regular basis
Near Certain	Will definitely occur or is occurring

Threat Impact by Asset Type

Table 5: MBWM Threat Impact by Asset Type Matrix.

Asset Type	Loss of service impact	Theft/Data Breach	Adjusted Impact
Server	🟧	🟥	🟥
Network	🟥	🟥	🟥
BYOD	🟦	🟧	🟨
E-Business Website	🟩	🟥	🟧
SaaS	🟩	🟨	🟨
Service	🟨	🟧	🟨
Workstations	🟨	🟧	🟨

Threat Actor Severity Matrix

TABLE 6: STANDARD THREAT ACTOR SEVERITY MATRIX.

Access to Company Assets **Skill and ability**	External, not part of the company	Very little, corporate staff	Moderate, Administrative staff	Extensive, Management and technical staff
Extensive/ Expert level knowledge.	🟧	🟧	🟥	🟥
Moderate/ Adept level knowledge	🟨	🟨	🟧	🟥
Amateur/ Little Knowledge	🟩	🟩	🟨	🟧
None, No knowledge	🟦	🟩	🟩	🟨

Risk Register

The risk register has been included as **Annex D** to this report. The risk register indicates the following: current threats and vulnerabilities, current mitigating controls, and the initial risk scores, risk owner, mitigation strategies, timelines, residual probability, residual risk and projected residual risk once remediation plans are implemented by MBWM. The initial risk scores were calculated using the Risk Equation found in the Risk of Key Threats section.

The projected residual risk scores were calculated using the standard Risk Equation while assuming that the mitigation strategies suggested by Sky-net Security were put in place within suggested timelines:

$$Risk_R = (Probability_R)(Impact_R)$$

Where:

$Probability_R$ = the likelihood the threat could occur with regards to the business

$Impact_R$ = how deleterious the threat is with regards to the business

Yielding:

$Risk_R$ = the risk of a threat currently facing a business

Appendices

Appendix A: Assumptions

- It has been assumed that Money Bags wealth management is willing to migrate their on-premises resources to a cloud service. Our recommendation is Microsoft Azure; however, Google Cloud and Amazon Web Services are all worthy options.
- For the calculated risk after mitigations, it is assumed that MBWM will follow our recommended remediation options. If these are not implemented, the values will not be an accurate assessment.

Appendix B: External Sources

[1] https://azure.microsoft.com/en-ca/pricing/details/app-service/windows/

[2] https://azure.microsoft.com/en-us/pricing/details/azure-sql-database/single/

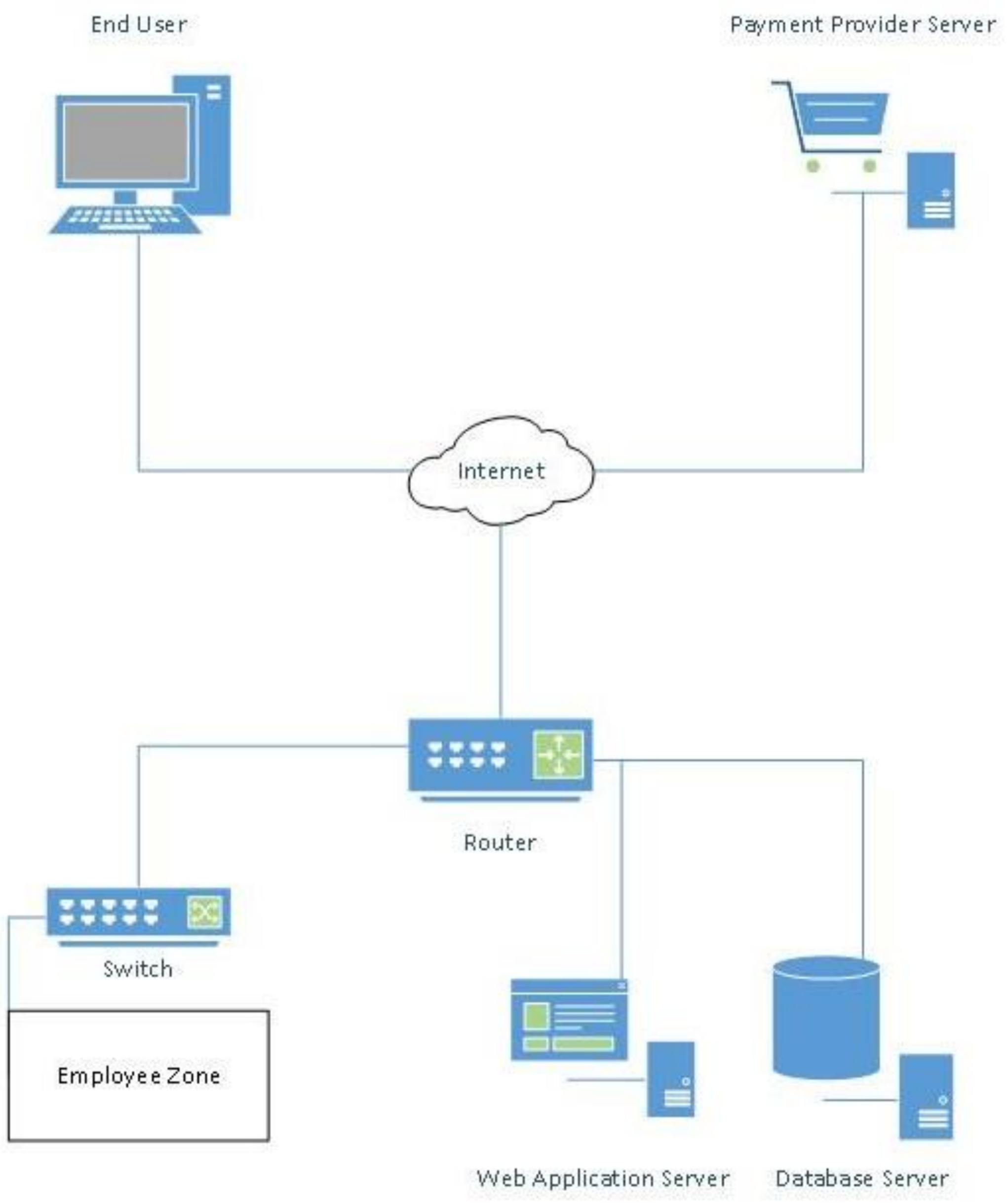
[3] https://azure.microsoft.com/en-ca/pricing/details/web-application-firewall/#purchase-options

[4] https://sites.fastspring.com/beethink/product/antiddosguardianiplicense

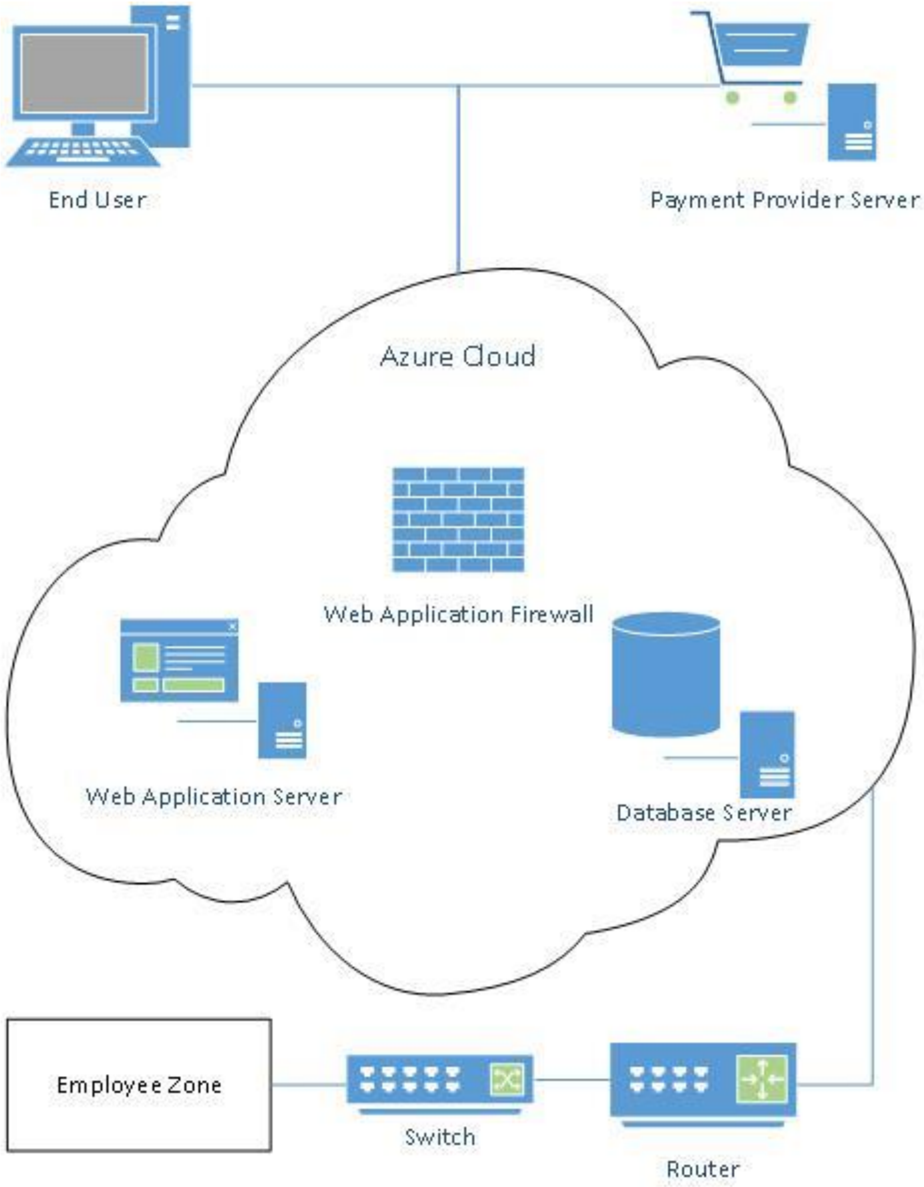
[5] https://www.globalknowledge.com/ca-en/content/gk-polaris/gk-polaris/

Appendix C: Network Diagrams

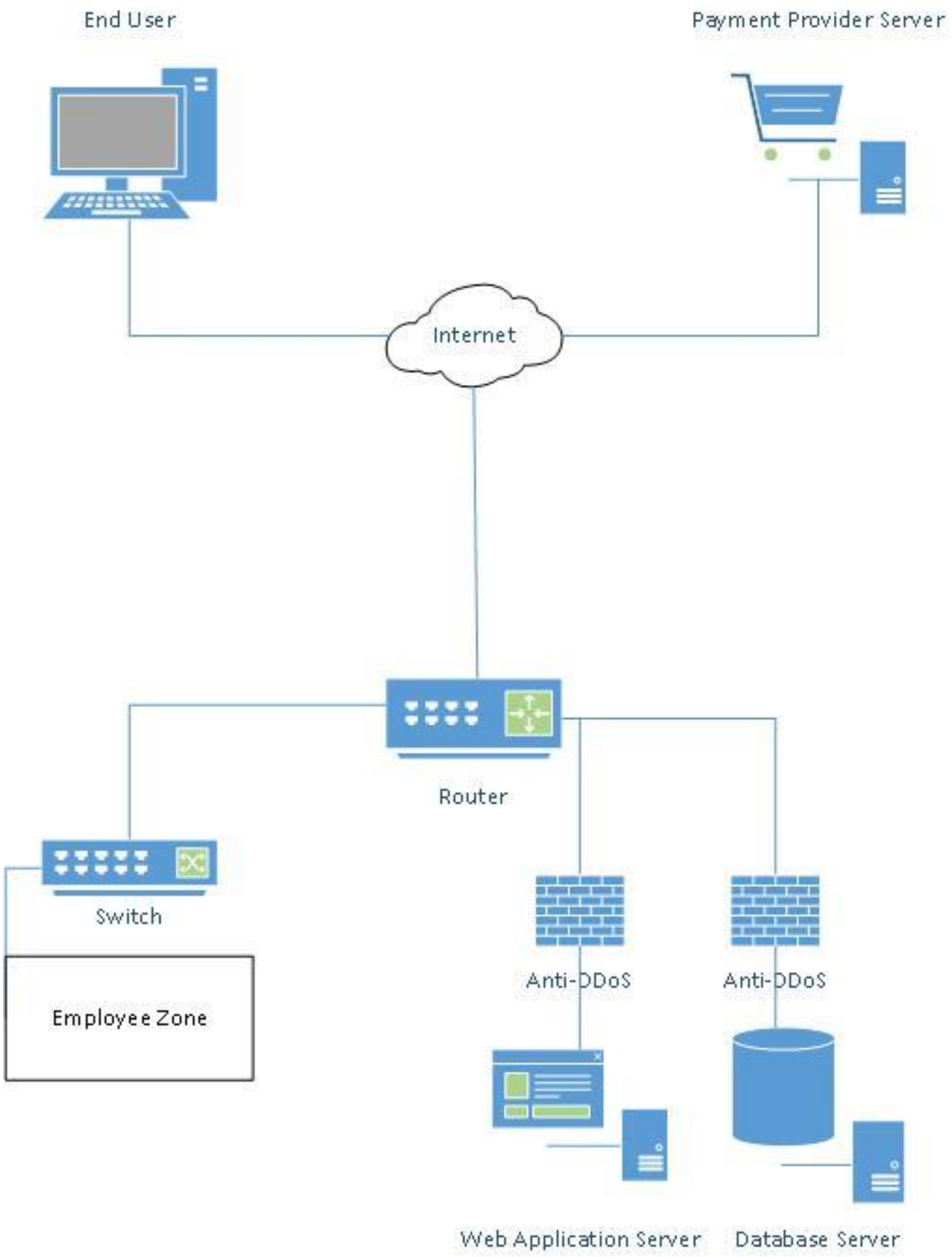
Current High-Level Design



Remediation Option A High-Level Design



Remediation Option B High-Level Design



Annexes

Annex A: Acceptable Use Policy

See attached document: 8801_Annex_A-AcceptableUsePolicy.doc

Annex B: Password Policy

See attached document: 8801_Annex_B-PasswordPolicy.doc

Annex C: Threat Evaluation by STRIDE

See attached document: 8801_Annex_C-ThreatEvalBySTRIDE.htm

Annex D: Risk Register for Key Threats to MBWM

See attached document: 8801_Annex_D-RiskRegister.xlsx