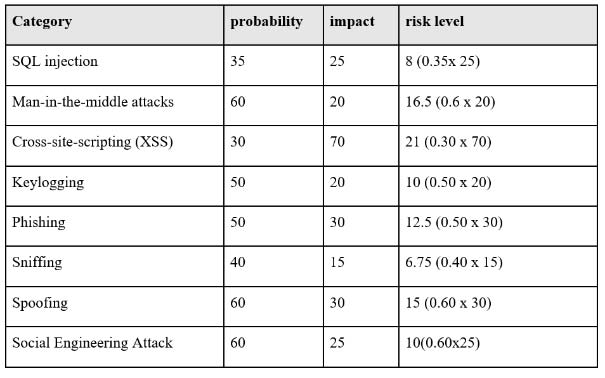
2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU)

Improvement Of The CIA Triad For Al-Rajhi Online

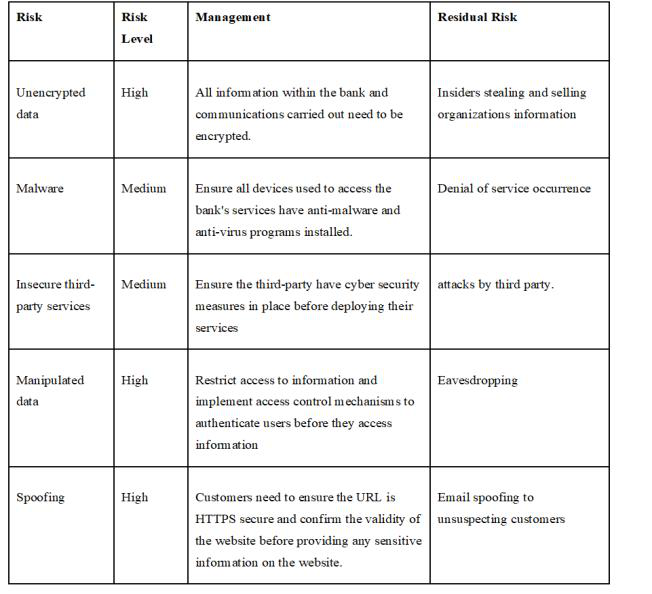
|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU) | 978-1-6654-0812-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/WIDS-PSU54548.2022.00025 | Banking System | | | | | | | | | |
| Sara Alshathri | | | | Eliana Alrashidi | | | | | Nouf Albawardi |
| *Information Systems Department* | | | | *Information Systems Department* | | | | | *Information Systems Department* |
| *Prince Sultan University* | | | | *Prince Sultan University* | | | | | *Prince Sultan University* |
| Riyadh, Saudi Arabia | | | | Riyadh, Saudi Arabia | | | | | Riyadh, Saudi Arabia |
| 218410159 @psu.edu.sa | | | | 218410290 @psu.edu.sa | | | | | 218410116 @psu.edu.sa |
| Haifa Almojel | | | | Nor Shahida Mohd Jamail | | | | | |
| *Information Systems Department* | | | | *Information Systems Department* | | | | | |
| *Prince Sultan University* | | | | *Prince Sultan University* | | | | | |
| Riyadh, Saudi Arabia | | | | Riyadh, Saudi Arabia | | | | | |
| 218410127 @psu.edu.sa | | | | njamail@psu.edu.sa | | | | | |
| ***Abstract*—** | **Online banking is** | | | **a financial institution** | | is sent to the registered phone number. After the user logs in | | | |
| **establishes an online presence and allows financial transactions to be conducted over the internet. It's the simplest way to make people's lives better because it eliminates the need for consumers** | | | | | | successfully all services are available.  Security Issues[3][4][5]: | | | |
| **and individuals to waste time and energy physically going to and visiting the bank every time, they need to complete a transaction. Because the main goal of online banking is for customers to be able to conduct their transactions online, a working internet connection is essential. Customers must also have an active account with their individual banks in order to access the online bank's website. The issue in online banking is** | | | | | | -OTP can be compromised by an attacker using many techniques.  -Passwords are not secure enough and are easy to acquire.-Biometrics are not used by the system.  -All actions are available without the need for further authentication once log in is successful. | | | |
| **unpredictable of risks that can impact the organization. This research discuss on the improvement of CIA triad to reduce the** | | | | | | II. RISK MANAGEMENT PLAN | | | |
| **risk on online banking system focusing Al-Rajhi Bank.** | | | | | | *A. Risk Register* | | | |
| **Keywords—Bank,** | | **CIA,** | **Risk** | **Assessment,** | **Incidents,** | | |  | |
| **Control, Security Planning.**  I. INTRODUCTION  When financial organizations develop an online presence and allow financial transactions to be completed via the internet, this is referred to as online banking. It's the easiest approach to improve people's lives since it eliminates the need for customers and individuals to waste time and energy going to and visiting the bank physically every time they need to execute a certain transaction. Because the major objective of online banking is to allow consumers to conduct their tasks online, a functioning internet connection is required. Furthermore, to use the web bank's website, customers must have an active account in their respective banks. Users should also locate and register for the bank's online service, as well as create an account on the bank's website or application [1][2]. Banks frequently provide online banking services through a separate website or application. Pure internet banks, which do not have a physical presence, have recently grown in popularity. They can offer particularly tempting incentives to users because they are not encumbered by the costs of a physical branch. They also frequently form partnerships with other financial institutions to provide their consumers with access to services that need physical interaction, such as an | | | | | | | |
| automated teller machine (ATM). In this study, we'll be | | | | | | | | | |
| looking into Online Banking Applications' net banking services. | | | | | | | Threats [6] [7]: SQL injection, Man-in-the-middle attacks, Cross-site-scripting (XSS), Keylogging, Phishing, Sniffing , | | |
| Al Rajhi bank offers an application and a website to access | | | | | | | Spoofing, Social Engineering Attacks | | |
| their services. To log in to an account, you need a password  that must be more than 8 characters with alphanumeric values.  If the information is correct the bank will request an OTP that  978-1-6654-0812-7/22/$31.00 ©2022 IEEE 67  DOI 10.1109/WiDS-PSU54548.2022.00025  Authorized licensed use limited to: Marathwada Mitra Mandal's College of Engg. Downloaded on August 07,2023 at 09:00:04 UTC from IEEE Xplore. Restrictions apply. | | | | | | | | | |

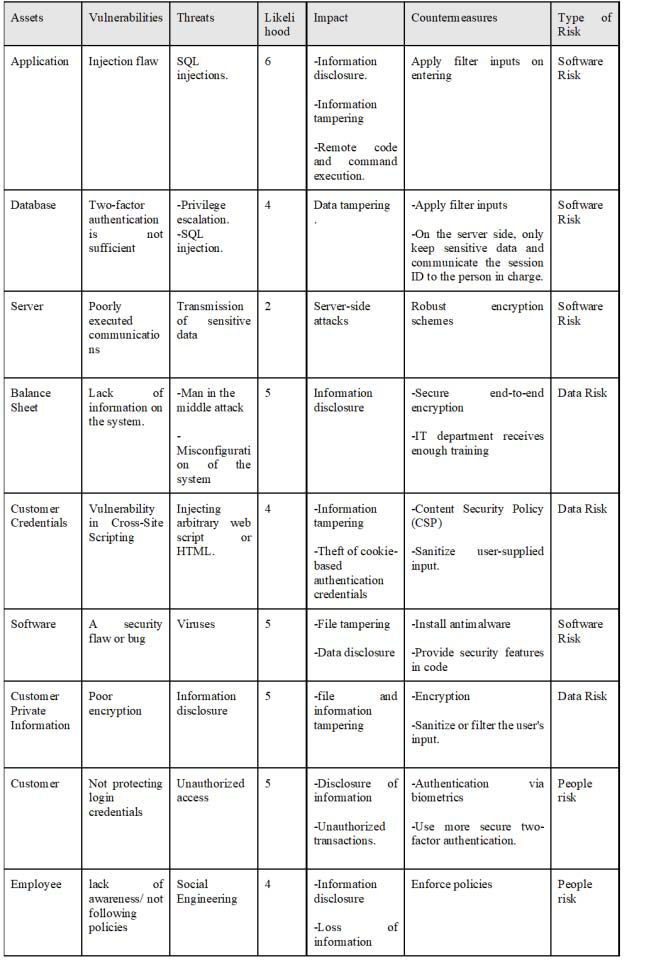
*B. Risk Assessment*  Risk Assessment





Risk Mitigation Strategy





*C. Policies And Guidelines*

Information security policy is the foundation for securing transactions within the banking environment. Organization information, customer information, processes, IT systems, and people involved in the operations of a bank are crucial to its success. Maintaining confidentiality, integrity, and availability of information is key in ensuring the smooth conduction of processes. The practices that need to be practiced in banking environment to guarantee security are [8][9]:

-Maintain an inventory of all information assets and be responsible for the controls that go with them.

-Rapid risk assessments are carried out to detect potential threats, weaknesses, and the threats' potential impact.

-Ensure that information's confidentiality, availability, and integrity are maintained.

-When it comes to the bank's IT resources, employees must be aware of their duties.

-Data should be segregated so that authenticated users can access information according to their permission levels.

-Use the least privileged option.

-To prevent unauthorized users from having access to the bank's information, the internet should only be utilized for commercial purposes.

-Users must use secure passwords with at least eight characters that should be updated every sixty days.

-Incident management should be developed to guarantee that security incidents are dealt with quickly and effectively.-To avoid eavesdropping and illegal access, sensitive information in the banking environment should be encrypted.

68   
Authorized licensed use limited to: Marathwada Mitra Mandal's College of Engg. Downloaded on August 07,2023 at 09:00:04 UTC from IEEE Xplore. Restrictions apply.

-According to the bank's policies, a periodic backup of all the bank's data is performed.

-Strengthening internal controls to counter insider threats, which are prevalent and deadly.

-Audit and review trails

Security guidelines relating to customers[9]:-Responsible for their assigned accounts' activity-Preserve the confidentiality of their passwords.

-Suspect actions must be reported; -Anti-virus software must be installed to avoid email phishing attempts  
-Customers will be educated on the security precautions they must take when using bank services.

-Transactions are monitored for suspicious activity at all hours of the day, seven days a week.

-Two-factor security solutions to verify customers' genuine identities -Customers are called by specific bank numbers that are publicly available -Customers are told not to open emails that include suspicious advertisements, messages, or purport to be from the bank to avoid email phishing attacks

III. IMPROVEMENT OF THE CIA TRIAD

By addressing the framework's weaknesses and shortcomings, the security of the Alrajhi online banking door could be improved. This will have a significant impact on overall system issues and vulnerabilities. As a result, the framework's overall secrecy, integrity, and availability will be greatly enhanced (CIA triad). The following are responses to security concerns about the AlRajhi online banking installment door :

Two-factor or multi-factor authentication (Confidentiality Improvement): One of the most common threats to the theft, security, and integrity of user financial and personal information is a breach of login credentials. All online banking logins, including mobile app and browser logins, should require two-factor or multi-factor authentication. The user must be asked for two-factor authentication while using mobile applications. The user should be asked to provide the authentication code given to their registered cellphone number or email address after entering their login ID and password. The code should be one-of-a-kind and valid for only one session. Protection against keyloggers and password attacks (Integrity Improvement): This includes ensuring that data is consistent, accurate, and reliable throughout its lifecycle. It must not be tampered with during in transit, and safeguards must be implemented to prevent unauthorized parties from altering data [.

1-Make sure your anti-virus software is up to date.

identifies a program attempting to transport data out, it will either ask for permission or display a warning. This barrier can prevent undesirable parties from gaining access to your computer or placing viruses on it when you are connected to the Internet.

DOS redundancy, failover, and RAID are all examples of preventive redundancy (Availability Improvement). This is best accomplished by meticulously maintaining all hardware, promptly performing hardware repairs as needed, and maintaining a stable operating system (OS) environment free of software conflicts. It's also crucial to keep up with any necessary system upgrades. Ensure proper communication capacity and avoid   
 bottlenecks are other important approaches. A network or server monitoring system can help you keep track of your network or server. Make sure you have a data recovery and business continuity (BC) plan in place in the case of data loss. Web application firewalls should be used by load balancers to protect web servers and application servers against DoS and DDoS attacks.

IV. CONCLUSION

Finally, security is the most important factor in banking systems. In bank security models, identification, authentication, digital signatures, and encryption must all be prioritized. Banking systems must protect all sensitive consumer data because there is so much at stake. Any data breach has the potential to be catastrophic. The banks' efforts, on the other hand, will be in vain if the consumer fails to protect his personal information.

ACKNOWLEDGMENT

The authors gratefully acknowledge the Information Systems Department, Prince Sultan University and Artificial Intelligence Data Analytics Lab (AIDA).

REFERENCES

[1] Kaspersky. (2021, March 11). Internet banking security to keep fraudsters away. Retrieved April 10, 2021, from https://www.kaspersky.com/resource-center/preemptive-  
 safety/internet-banking-security-keep-fraudsters-away

|  |  |
| --- | --- |
| [2] | Gez, D. (2021, February 02). Top 5 cyber threats FACING banks in 2020. Retrieved April 10, 2021, from https://hubsecurity.io/top-5- |

cyber-threats-facing-banks/

[3] Greek banks Replacing up to 15,000 credit cards due to security breach. (2020, January 16). Retrieved April 10, 2021, from https://news.gtp.gr/2020/01/15/greek-banks-replacing-up-to-15000- credit-cards-due-to-security-breach/

[4] Saudi central bank systems, government AGENCIES struck by Iran malware Shamoon. (n.d.). Retrieved April 10, 2021, from https://www.google.com/amp/s/amp.smh.com.au/world/saudi-central-

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Antivirus software protects your computer from dangerous | [5] | bank-systems-government-agencies-struck-by-iran-malware- | | | |
| shamoon-20161203-gt37l2.html | | | |
| software such as viruses, worms, trojans, and other malware. | The 5 biggest threats to a Bank's cyber security. (n.d.). Retrieved April | | | |
| To keep your computer safe from malware, make sure your | 10, 2021, from https://sqnbankingsystems.com/blog/the-5-biggest- | | | |
| antivirus software is up to date. This will allow you to detect | [6] | threats-to-a-banks-cyber-security/ | | | |
| and prevent new viruses from attacking your computer. Non- | Affendy, Khairul & Rosalim, Rayvieana & Yu Beng, Leau & Fun, Tan. | | | |
| virus threats like as spyware, keystroke loggers, and other | [7] | (2010). Security Issues on Banking Systems. International Journal of | | | |
| Computer Science and Information Technologies. 1. 268-272. | | | |
| harmful applications must also be detected by the program. |
| Google. (n.d.). Bank web apps are the "most vulnerable" to getting | | | |
| 2- On the internet, set up a firewall. | [8] | hacked, research says. Google. | | | |
| 10 ways to prevent or mitigate sql injection attacks. (n.d.). Retrieved | | | |
| A firewall is a piece of software or hardware that serves as a | [9] | March | 31, | 2021, | from |
| https://www.enterprisenetworkingplanet.com/netsecur/article.php/386 | | | |
| barrier between your computer and potentially harmful | 6756/10-Ways-to-Prevent-or-Mitigate-SQL-Injection-Attacks.htm | | | |
| Internet content. It is a great defense against keyloggers since | Benefits and Risks of Online Banking - Benefits & Risks of Online | | | |
| it closely monitors computer activities. If the firewall | Banking. (2021). Retrieved 31 March 2021. | | | |

69

Authorized licensed use limited to: Marathwada Mitra Mandal's College of Engg. Downloaded on August 07,2023 at 09:00:04 UTC from IEEE Xplore. Restrictions apply.