Financial Cybersecurity Results and Risk Management Based off Results

Risk Management: Identification of the Potential Risks and Vulnerabilities within our system

- Data Breaches- Unauthorized access to our company data that could lead to identity theft and data loss. The active directory stores all of the login data, and the secure encrypted database stores all data for the company. If the active directory is down, there are still measures in place like MFA and the firewall that must be passed through for someone to login. Since there are three solid measures in place to get into the system, there is not a critical level for a data breach. There is still a high level for it though if MFA is bypassed.
- Phishing- Emails or other fraudulent attempts to obtain information by an outside entity posing to be trustworthy. If MFA is bypassed identity theft and our company's financial data will be compromised. MFA in our system proves that a user is who they are, so without it users can more easily gain access to the system. Emails can also be sent from an outside source, as with any company system, because hackers want information. Systems admin, the internal security team, and the incident response team all need to be aware of the practice of phishing.
- Insider Threats- Employees with access to the system that can both unintentionally and intentionally cause harm. Employees within any system can cause harm, but it is more of a risk in our system, especially at first with the new implications. Employees can see the appointment times available in the database and take times from coworkers based on first come first served.
- DDoS Attacks- Overwhelming the system to disrupt services. The system could be overwhelmed by so many users trying to schedule appointments or do their tasks at the same time. The system could also be overwhelmed if a ton of users are trying to schedule their appointments at the exact same time, users would be back and forth between appointment scheduling screens. Our company could take a financial hit if the system becomes down for a short period.
- Zero-Day Exploits- Attacks on things that are unknown in the system so there are no fixes for those things. With the new implications of the new security system, there will be events that occur that training for will not cover.
- Cloud Vulnerability- Risks that are associated with storing and accessing data. Previously the system only used a windows defender and stored information in google drive. Transferring this data to the new database will make the data more

secure for employees to use and view. Misconfiguration of the data is what we have to watch out for while making this transfer.

Risk Assessment Matrix: Prioritizes Threats

Risk	**Impact**	**Likelihood**	**Risk Level**
Data Breach	High	High	Critical
Phishing	Low	High	Medium
Insider Threats	High	Low	Medium
DDoS Attacks	Medium	Medium	High
Zero-Day Exploits	Medium	High	Medium
Cloud Vulnerability	High	Low	Medium

Key:

- Risk Column = Risk Identified
- Impact Column = Impact on our system/company if these risks were to occur
- Likelihood Column = Likelihood of risk to occur on our system
- Risk Level Column = Overall severity of the risks

Incident Response Procedures: Detection, Response, Recovery

Phase	**Actions**	**Responsible Team**
Preparation	Conduct training, set up monitoring tools and a plan to communicate incidents	Internal Security Team
Detection	Monitor system, analyze alerts from the logging requests	Incident Response Team
Response	Isolate the part that needs to be fixed, implement updates	Incident Response Team
Recovery	Restore system, test functionality	Systems Admin

1. Preparation: Ensuring that employees in the company have proper training to recognize and report security incidents is important with this new system. The internal security team will implement a training program for employees to not only be able to recognize an incident but also show how to not do some of the recognized incidents. This lowers the possibility of the insider threat risk.
2. Detection: The incident response team will be responsible for monitoring our system to detect unusual or repeated activity. They will quickly assess the impact of the incident by analyzing the logging request information a user imputed into the system. They will document the incident.
3. Response: The incident response team will isolate the parts of the system that need to be fixed to prevent any further damage to the system. This could involve isolating the task or appointment section of the system. They will remove the cause of the incident and notify the two other security teams.
4. Recovery: The systems admin will restore the affected systems and their data. They will ensure that all the data is clean. The incident is resolved once the data is confirmed clean after the system is restored. The documentation of the incident will be reviewed.

Disaster Recovery Plan: Data Backup, System Restoration, Continuity of Operations

Data Backup- Data backup will be done as a full backup on a regular backup schedule through the encrypted database. This way a complete copy of all data will be stored instead of just the changes since the last backup being copied. Including a regular backup schedule of daily backups will be crucial for our system since it is in the financial sector. We have to keep track of appointments, tasks that need to be done, and money. The data can be used as a better tool to analyze incidents if it is all backed up, even though a full backup is comprehensive and needs storage space. Our data is backed up through the secure encrypted database as well as cloud storage. This hybrid combination of local and cloud storage offers enhanced security to our system. The encrypted backups ensure that our data remains secure and retrievable in case of an incident. Only systems admin and the incident response team have access to all backups, as employees can be trained on them but do not necessarily need access to all the behind the scenes with the institution. Employees can view appointment times and tasks, but not the financials for the whole company.

System Restoration- System restoration will be done through the processes of containment, eradication, and the update of security measures. This is done by all security teams involved. Depending on the level of incident, if it is task, appointment, or financially related, the system will undergo short-term or long-term containment. This is when the problem is isolated for a short period of time while minor fixes are implemented, or the problem is isolated for a long period of time to develop a permanent solution. The eradication process will remove the threat and eliminate its root cause. For example, unauthorized access could be a root cause for an incident in our system. Updating security measures through the system applies the necessary solutions and prevents recurrence. Documentation of these incidents and updated security measures will be documented for reference to future incidents.

Continuity of Operations- Continuity of operations will be done through the processes of validation and post-incident review. The systems admin will test the updates in the system to validate them to ensure they are functioning correctly. The post-incident review then happens after the system update is validated. All employees and security team members will be advised of the incident that happened and why. The security teams will report on the lessons they learned and their response actions through documentation. Employees will apply what they have read through the documentation to avoid repeatable incidents if applicable.