TO: IT Manager, Stakeholders

FROM: Naiya Whitley

DATE: January 19, 2024

SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please find below an overview of the recent internal IT audit conducted at XYZ Financial Services:

Scope:

Assessment of the cybersecurity program will evaluate the following:

* User permissions and access controls throughout databases, financial applications, and processing systems.
* Effectiveness of the current implementation of security measures.
* In-depth evaluation of financial compliance regulations with GLBA and PCI DSS specifications.
* Hardware and software for financial transactions.
* Current cybersecurity policies and procedures.

Our internal IT audit assessed the organization's information technology systems, assets, controls, and compliance with relevant regulations and standards.

Goals:

Internal cybersecurity audit goals are centered around business continuity, compliance with regulations, data protection, employee training, improved security solutions, and risk mitigation.

A brief overview includes:

* Vulnerabilities in financial operations and the development of a business continuity strategy.
* Compliance with all financial regulations for increased customer protection and trust.
* Added data protection features to ensure the security of customer financial records.
* Employee training programs specifically designed to encourage the best cybersecurity practices.
* Enhancement of security measures.

The primary objectives of this audit were to evaluate controls, assess compliance, identify vulnerabilities, and provide recommendations for enhancing security and risk management.

Critical Findings (Must Be Addressed Immediately):

1. Unsolicited access to customer financial data, employee devices, and internal networks due to limited access controls within the organization’s systems structure such as two-factor authentication, systems-generated unique identifiers, and or exclusive access requests to certain customer files.

2. Customer data is not thoroughly protected while in the possession of the organization. Lack of firewalls and encryption software. In the event of potential incidents and threats involving customer and organization data, there is no system in place to quickly detect intrusion and stop further threats.

Findings (Should Be Addressed, but No Immediate Need):

1. Data backups are not performed regularly leading to the prevention of data recovery of customer financials causing complex issues as it relates to business continuity.

2. Potential financial losses and legal consequences can arise from delays and lack of security during transaction processing within the organization or through online channels.

Summary/Recommendations:

In summary, the audit revealed critical findings requiring immediate action and additional findings for long-term improvements. We recommend addressing these findings promptly to enhance security and compliance. To maintain a reputable status within the finance industry and in customer relations employees must be made aware of the importance of data and systems security and the organization must develop and implement asset controls quickly and efficiently. The protection of intellectual data, customer financial records, and information systems networks is the focus of a business in this industry.

Sincerely,

Naiya Whitley

Information Security Analyst

XYZ Financial Services