CALIBRE
CPA GROUP

7501 WISCONSIN AVENUE | SUITE 1200 WEST
BETHESDA, MD 20814
202.331.9880 PHONE | 202.331.9890 FAX

DATE: October 15, 2020

TO: Board of Trustees of the FELRA and UFCW Pension Fund

FROM: Calibre CPA Group PLLC

RE: Cybersecurity Risk Assessment Updated Memorandum

Pursuant to the request of the Board of Trustees of the FELRA and UFCW Pension Fund, we are providing an update to our enterprise-wide risk assessment memorandum provided on April 17, 2020. We have outlined below, pertinent information regarding the updated security measures within our network, to ensure the security of client data. As such, this Memorandum contains sensitive data which, if copied, proliferated, or shared publicly could compromise the security measures undertaken.

This Memorandum should not to be copied, forwarded, shared, or saved in any medium. As a result of our commitment to one of its long-time and highly valued clients, we are providing this document for review by your organization.

IT Risk Analysis and Assessment

In response to a data incident that occurred in 2019, and as part of our regular and continual assessment of its overall IT network systems, we commenced a system-wide review and analysis to identify any potential security risks across our environment and develop a plan to further enhance our security measures. This Memorandum serves to provide a summary of the potential risks identified, and the measures undertaken to strengthen our physical network and technological security.

The review was conducted by PKF O'Connor Davies (PKF) and entailed an enterprise-wide risk assessment to identify and eliminate potential risks in our environment. This third-party risk assessment was completed on November 25, 2019, and we have responded to the items identified since the completion of the review. Our efforts in bringing on a third-party to conduct such an analysis is illustrative of our commitment to protecting and securing the data it receives in the ordinary course of business.

Summary of Consultants Report and Measures Taken

We have hired a full-time dedicated Director of IT and Cybersecurity to spearhead the implementation of all recommendations identified in the Risk Assessment Report. The primary responsibility for this position is to ensure that all issues are addressed and identify any additional areas, where there could be risks. The scope of the consultant's report included the following areas:

1. IT Resources and personnel
2. Firewall configurations
3. Protection of personal information
4. Anti-virus
5. Cybersecurity Awareness program
6. Backup and patch management
7. Wireless security
8. IT standards operating procedures manual
9. Third-party IT vendor due diligence
10. Removable media
11. Business continuity and disaster recover
12. Incident response plan
13. Data loss prevention

A summary of the consultant's findings/recommendations are as follows:

1. Calibre should implement a formal system of IT governance and should better document IT plans and policies. Future policies need to be constantly updated with highly granular details. Business Continuity and Disaster Recovery plans should include updated, formal documentation and testing.
2. Calibre should increase IT staffing levels so current staff can be proactive with respect to strategic IT planning
3. Data storage and management needs to be better designed.
4. Calibre should increase the scope and availability of cybersecurity awareness training.
5. Certain aspects of the network infrastructure and security should to be reviewed and remediated. This includes firewall configuration, wireless access, password policy, network audit logging and remote access policies.

We have evaluated and accepted all of the consultant's recommendations. In the time since receiving the cybersecurity assessment from PKF, we have implemented the following initiatives and changes:

1. The development of a Cybersecurity Awareness Program for ongoing Cybersecurity education and training of all Calibre personnel to include ongoing Anti-Phishing campaigns;
2. Initiated the Calibre CPA Group IT Steering Committee to unify the Management Committee and all company stakeholders. This will align the overall IT objectives with the corporate direction and overall goals;

3. Implemented a comprehensive Problem Management System. This application allows for historical tracking of all IT and cybersecurity related IT incidents;
4. Developed of a comprehensive Information Security Plan to ensure that all employees and management have policy guidelines for IT and cybersecurity requirements;
5. Developed the Calibre CPA core Cybersecurity Principles, IAW NIST 800-53, rev. 5 and the NIST Risk Assessment Framework, 800-37 and;
6. Designed and implemented ongoing quarterly internal Risk Assessment Program followed with an Annual External Review;
7. Implemented Duo multi-factor authentication protocols for all forms of remote access, including Office 365, Remote Desktop, and VPN;
8. Implemented a new software deployment system which allows IT to quickly push third party software updates to workstations firmwide while providing granular insight on each workstation;
9. Implemented a proper helpdesk suite to be able to properly track and identify issues;
10. Forced password reset of all active directory accounts once illegitimate access was discovered;
11. Reviewed and disabled all dormant active directory user and service accounts;
12. Added an additional layer of email scanning via AppRiver, a software which scans for phishing, viruses, and malware;
13. Updated policies related to encryption of email correspondence, regardless of internal or external destination;
14. Migrated mail server to cloud-based Microsoft Office365 from on premises Exchange server;
15. Secured the local administrator account on all workstations with unique, complex passwords;
16. Enhanced the procedures and reporting concerning our local and offsite backups run by our third party managed service provider;
17. Increased the level of physical security in our branch offices;
18. Enabled Azure Active Directory to track all system logins and bolster auditing capabilities; and
19. Migrated from a self-hosted secure file transfer program (Biscom SFT) to Citrix ShareFile.

In addition, we are in the process of upgrading our overall Corporate network infrastructure and migrating to a more secure cloud-based tax application which offers multifactor authentication and granular security option.

Prior to the Data Incident

We have been committed to ensuring the data in our care includes maintaining the information in a secure environment, compliant with applicable laws, with continuous updates and adjustments geared towards bolstering security. Prior to the incident, some of the steps that we had implemented included the following:

1. Redesigning the way data has been retained by the organization and employ additional measures to safeguard all Tax Data, IAW IRS Publication 4557, “Safeguarding Taxpayer Data, A Guide for Your Business”.

2. Employing full disk encryption on all laptops to prevent data loss in the event of hardware loss;
3. Implementing an enhanced Password Policy requiring complex passwords (3/4-character classes) with 8+ characters required to change every 180 days;
4. Requiring employees in the field to connect to our systems via Remote Desktop or VPN to ensure secure communications;
5. Mandating that all employees complete HR compliance training annually, including a sixty-minute course on HIPAA privacy and a forty-five-minute course on HIPAA security;
6. Requiring all sensitive information emailed externally to be sent on secure platform;
7. Disabling our user accounts after 3 failed log-in attempts to prevent brute force attacks;
8. Disabled the ability for software on USB drives to run automatically;
9. Coaching new hires on data privacy policies during orientation and requiring completion of training programs within first five days of employment, including the execution of policy acknowledgement at new hire orientation;
10. Proliferating firm-wide email reminders to all users to be vigilant when clicking links or attachments, including advising employees to hover over links to verify URLs, and to contact sender when in doubt of authenticity;
11. Reminding all users via firmwide email regarding responsibility to protect client data, including details about not leaving any documents w/sensitive information on desks, shredding protected data instead of recycling, locking PCs to desks if leaving overnight, and locking physical files away rather than leaving on desks;
12. Upgrading Anti-Virus suite to search for suspicious behavior in addition to file signatures, the result of which is designed to prevents ransomware by stopping files from encrypting; and
13. Configuring network scanners to scan to a network share drive which is private to each user rather than scan to email.

Conclusion

Our IT and cybersecurity risk assessment and analysis are a continual effort and priority within the firm, of which one of the objectives is to ensure the safety and security of all client information in our care. Our IT and cybersecurity team will constantly be monitoring and assessing our overall network infrastructure and systems. This will allow IT and our Management to proactively identify, address, and remedy any potential vulnerabilities.