MARCUM TECHNOLOGY

THE Climate + Clean Energy EQUITY FUND

CASE STUDY

Strategic IT Management for Nonprofits: Enhancing Cybersecurity and Efficiency with a Managed Services Provider

COMPANY OVERVIEW

The Climate and Clean Energy Equity Fund (CCEEF) is a leader in climate philanthropy with expertise in advancing structural policy change. They have a proven model for building power, supporting community-driven priorities for climate action, and focusing on the clean energy transition. The Equity Fund invests in the leadership of community-organizing groups in diverse communities (Black, Indigenous, Latinx, APPI and other communities) with catalytic and sustained funding, capacity building and technical assistance to lead organizing, civic engagement, advocacy, voter participation and communications strategies that advance equitable climate action and clean energy solutions.

CHALLENGE OVERVIEW

CCEEF recognized that it needed a partner to create a resilient and adaptable plan to address ongoing IT concerns and develop an appropriate cybersecurity strategy that would protect the organization from potential threats. With limited internal resources, CCEEF was seeking an MSP partner that had the technical abilities to execute cutting-edge technology solutions. Additionally, this partner would take charge of the majority of IT initiatives to make the organization more efficient and agile to adapt to the shifts in the rapidly evolving digital landscape. CCEEF had three strategic IT goals:

- Identify critical IT gaps and secure the organization from any potential vulnerabilities
- Ensure that new employees have the necessary support, access and tools while departing employees are securely offboarded to prevent any potential security breaches
- Maintain compliance and stay up-to-date with software licenses

HOW WE HELPED!

To effectively tackle the challenges at hand, The Equity Fund engaged in a strategic collaboration with Marcum Technology. This alliance was aimed at carrying out a comprehensive evaluation of The Equity Fund's IT infrastructure, with a view to executing a series of enhancements that included:

1. ESTABLISHED A ROBUST AND SECURE INFRASTRUCTURE

Challenge: Building a comprehensive security posture from the ground up involves assessing potential vulnerabilities and implementing suitable security measures. It also requires establishing robust protocols and well-defined policies and procedures. The challenge lies in identifying and addressing potential threats effectively and ensuring that the security infrastructure is resilient and adaptable to evolving cyber threats. Just as important was training employees on security awareness without overwhelming them.

Approach: Marcum Technology started the engagement by performing an IT assessment. The assessment reviewed not only systems and security but also policies and procedures. This allowed Marcum to get a better understanding of the business and the technology that is currently in place. It also helped identify any potential gaps between the current state, industry best practices, and the desired end state.

Results: After a thorough review of their IT environment, security posture and technology challenges that The Climate and Clean Energy Equity Fund shared with Marcum, a robust security plan was implemented to address their challenges and concerns . This included reviewing and updating permissions with the principle of least privilege in mind. Every workstation also went through a thorough review and a plan was formulated to address missing patches, removal of unnecessary software, removal of unnecessary

user rights and more. Marcum then installed standardized and centrally managed security tools including a remote monitoring and management tool, anti-virus, a web content filter, and an MDM (Mobile Device Management) solution. These tools combined help enforce strict passwords, drive encryption, and remote wipe in the event the laptop is lost or stolen. Lastly, Marcum implemented security awareness training to educate end users and help minimize the chance of bad actors gaining access to systems through end users' actions.

By taking a "defense in depth" approach to securing their environment, CCEEF now:

- Has a greatly improved security posture
- Is less vulnerable to known vulnerabilities and bad actors
- Has better trained end users
- Has improved compliance with cyber security insurance requirements.

2. LICENSED MANAGEMENT AND COMPLIANCE

Challenge: Managing software licenses and ensuring compliance with regulatory requirements can be a complex task. The organization needed to assess its software inventory and track licenses. The challenge here was to establish efficient license management processes, preventing any misuse or non-compliance issues that may lead to legal consequences or operational disruptions.

Approach: The first step was to get a complete understanding of what accounts and licenses The Climate and Clean Energy Equity Fund had, then review each with the appropriate CCEEF team member to fully assess organizational licensing needs. After the review process Marcum determined that all the accounts were being administered by internal non-IT staff.

Results: Marcum created new administrative accounts for all systems and in most cases removed the existing administrators as they no longer required that level of access. Marcum and the Climate and Clean Energy Equity Fund also deactivated or deleted accounts for previous employees and reduced permissions for active users where applicable. This placed control over users and permissions to the appropriate parties. Lastly, Marcum reduced license counts to reduce The Climate and Clean Energy Equity Fund monthly license expenditures.

3. STREAMLINED ONBOARDING/ OFFBOARDING PROCESS

Challenge: Developing seamless onboarding and offboarding processes involves integrating IT measures with HR procedures. This includes provisioning user accounts, managing access rights, and ensuring a smooth transition for employees entering or leaving the organization. The challenge was to create standardized and efficient processes that minimize the risk of security gaps during these transitions, ensuring that new employees have the necessary access and tools while departing employees are securely offboarded to prevent any potential security breaches.

Approach: Review existing onboarding and offboarding procedures and make recommendations as necessary.

Results: Once the review of the existing procedures was completed, Marcum worked with The Climate and Clean Energy Equity Fund to update the roles and responsibilities for the onboarding and offboarding procedures. Going forward, Marcum will be administering the account creation and permissions for new accounts as well as the termination of accounts allowing The Climate and Clean Energy Equity Fund staff to focus on their core roles and responsibilities of driving their mission forward.

MARCUM TECHNOLOGY

THE Climate + Clean Energy EQUITY FUND

CASE STUDY

Strategic IT Management for Nonprofits: Enhancing Cybersecurity and Efficiency with a Managed Services Provider

MARCUM LLP AND MARCUM TECHNOLOGY SERVICES

Are you truly positioned for success? Start the conversation about a more strategic approach to accomplishing your business goals.

Ask Marcum.
To learn more about Marcum LLP and Marcum Technology's services contact us today at:

800.331.6546
hello@marcumtechnology.com
www.marcumllp.com / www.marcumtechnology.com

MARCUM TECHNOLOGY PROJECT MANAGERS

MICHAEL COHEN
Senior Manager of Managed IT Services
301.337.3104
michael.cohen@marcumtechnology.com

GEORGE LOURIS
Vice President of Managed IT Services
631.414.4808
george.louris@marcumtechnology.com

QUOTE FROM EXECUTIVE SPONSOR

> “Marcum's MSP services have been exceptional and the cornerstone of our IT operations in more than 70 countries. From meticulous device enrollment to swift troubleshooting and strategic endpoint management, Marcum's dedicated team has ensured a harmonious partnership. We wanted the gold standard from our Managed Service Provider, and Marcum gave it to us through collaboration with our device provider, adept handling of IT projects and insightful cybersecurity recommendations.