Community-Based Nonprofit Proactively Addresses Cybersecurity Challenges

Featured Organization Profile

This organization provides a residential medical facility for homeless persons, serving patients requiring medical care, but not hospitalization. In addition to medical services, the organization provides transportation to medical appointments, meals, a variety of activities, and emotional and spiritual support.

Client: Residential Medical Facility

Entity Type: 501(c)(3)

Location: Washington, DC

Annual Budget: $4.5M

CPAs & ADVISORS

Challenge

Leveraging New Technologies Creates Additional Security Concerns

The stakes were high for a DC-based community organization. With a newly-hybrid work environment, increased government scrutiny on IT security, and rising cyberattacks, the CFO realized the organization's current IT vendor was not up to the challenge.

As a residential medical facility, the organization needed to maintain limited on-site operations throughout the shutdowns caused by the COVID-19 pandemic but moved many functions off-site. This shift to a hybrid work environment raised concerns for management and the board of directors about the security and reliability of its information technology systems.

In addition to a requirement to protect sensitive personal data, the facility's extensive use of technology in its medical care meant a cyberattack could have devastating consequences for its patients. The organization also relies on government funding, which is contingent on passing new, more stringent audit requirements related to IT security. SAS 145 requires auditors to gain a more comprehensive understanding of the IT environment and how it could materially affect the financial statements.

The organization had been using the same third-party IT vendor for decades. Despite strong personal relationships, the vendor was not able to keep pace with evolving needs. It was clear to the management team that the current services were insufficient, but they did not have the expertise to identify the nature of gaps, vulnerabilities, or priorities for upgrades and new investments.

Solution

After a rigorous selection process, the board of directors' finance committee chose GRF because of the team's technical expertise, including their proficiency in distilling complex technology issues down to the essentials necessary to help the board and management make informed decisions.

GRF deployed its proprietary Cybersecurity Risk Assessment and Scorecard – an evaluation of 20 different risk areas – to assess the organization's systems. The assessment provided a "hackers' perspective" of the system to identify gaps and vulnerabilities not currently addressed by their third-party vendor. The resulting report's color-coding and "A to F" grading system allowed the board to clearly understand the organization's IT environment without becoming bogged down in technical jargon.

The organization received a good initial score, with only minor issues flagged. This score improved over time after they completed the corrective actions. The IT audit gave much-needed reassurance to the board that the organization could keep up with the rapid changes associated with operating during a crisis like a pandemic. The CFO noted that they think very carefully about any expenses not directly related to their patients and do a lot of due diligence. The scan provided them with a low-cost option for gaining a solid understanding of their cyber posture.

The organization also engaged GRF to help identify a more suitable IT vendor since their directors lacked the technical expertise to evaluate the proposals they received. GRF's input helped the management team select a provider that was better able to meet their needs as the organization grows and expands.

Results

With the help of GRF's Risk and Advisory Services team, the facility strengthened its systems and implemented critical policies and procedures. The new IT service provider trains staff, management, and the board to improve their understanding of their risks and industry best practices, as well as their roles as cybersecurity stewards.

With this newfound understanding of cybersecurity risks and solutions, IT is now a standing agenda item for monthly finance committee meetings and annual board discussions with the service provider. This open communication allows board members to ask questions and receive answers at the appropriate level of detail. Staying on top of IT developments is a critical responsibility for boards, so having ongoing conversation about the status of cybersecurity from IT experts helps them manage risks and make informed decisions.

Contact Us

Cybersecurity is not a one-size-fits-all proposition. GRF CPAs & Advisors' cybersecurity scorecard is a valuable tool for organizations of all sizes and complexities, complementing existing cybersecurity measures while providing a comprehensive solution for cybersecurity. Contact us for more information about GRF's cybersecurity solutions.

Melissa Musser, CPA, CITP, CISA
Partner and Director, Risk & Advisory Services
mmusser@grfcpa.com

Darren Hulem, CISA, CEH, Security +
Supervisor, IT and Risk Advisory Services
dhulem@grfcpa.com

About GRF CPAs & Advisors

Our risk experts work with organizations to provide support for complex decision-making over a wide range of business and financial issues.

Services include Enterprise Risk Management (ERM), third-party risk assessment, internal audit, cybersecurity, privacy, fraud support, compliance consulting, and financial systems optimization. For more information on how our experts can support your organization, visit our website at **https://www.grfcpa.com/accounting-services/advisory-services/.**

Headquartered in the Washington, DC metropolitan region serving clients locally, nationally and around the world. GRF CPAs & Advisors is a full-service professional services firm providing clients with audit, accounting, tax and advisory solutions.