blumshapiro
accounting • tax • advisory

29 South Main Street
P.O. Box 272000
West Hartford, CT 06127-2000
Tel 860.561.4000

blumshapiro.com

To the Honorable Mayor and Members of the
Court of Common Council
City of Hartford, Connecticut

In planning and performing our audit of the financial statements of the City of Hartford, Connecticut, as of and for the year ended June 30, 2020, in accordance with auditing standards generally accepted in the United States of America, we considered the City of Hartford, Connecticut's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the City of Hartford, Connecticut's internal control. Accordingly, we do not express an opinion on the effectiveness of the City of Hartford, Connecticut's internal control.

We noted the following matters involving the internal control over financial reporting and its operation that we offer as constructive suggestions for your consideration as part of the ongoing process of modifying and improving accounting controls and administrative practices.

Cybersecurity Threats

Cybersecurity has reached a new crossroads. Companies can no longer have a "wait and see" attitude toward securing operations and data. Proactively assessing and managing operations and IT environment(s) in anticipation of cyber threats is critical. Managing your organization's risk to cyber threats starts with a consideration of the following:

- Cybersecurity is now considered a key business risk by most Boards.
- Global spending on cybersecurity is projected to increase each of the next 10 years.
- Nearly 70% of funds expended due to a cyber event are unrecoverable.
- Ransomware attacks force the majority of impacted businesses to pay to get their data back.
- The scale of data breaches and lost funds due to phishing and business email compromise is exponentially trending upward.
- Most companies do not know all locations where personal/confidential information is stored and/or how it is protected.
- With the most frequent cybersecurity attack vector migrating from the network perimeter, directly to the individual user, everyone who touches technology can be a point of exposure.

As such, cybersecurity strategies require a new approach to identify where critical information exists that needs to be protected, a new way of foreseeing and deterring the threats that could result in the theft of information or the loss of funds, and a new way to understand the overarching corporate risk associated with cyber-attacks.

Recommendations

Understanding your baseline exposure to cyber threats is a critical best practice. An annual security and vulnerability risk assessment should be performed that identifies and evaluates exposures, hazards and/or potential for breach that could negatively impact an organization's ability to conduct business. These assessments help to identify the inherent cyber risks and provide measures, processes and controls to reduce the impact of these risks to business operations. From this assessment you should identify and locate personal/confidential information and understand how this information is secured and gain a clear understanding of potential for exposure. Risk mitigation plans should be designed to tighten areas of exposure and establish stronger security protocols. Limited resources will be applied to the areas most in need of protection.

As a key component to building and maintaining a resilient culture of cybersecurity, strengthening employee cybersecurity awareness through focused training will be a critical component of an organization wide cybersecurity initiative. Progressive ways of assessing how employees respond to targeted threats through phishing simulation attacks can proactively identify areas of exposure, reinforce learning objectives, identify training opportunities, and help identify missing security protocols.

This letter should be read in conjunction with our report on Internal Control over Financial Reporting and on Compliance Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards* dated December 27, 2020.

This communication is intended solely for the information and use of management, Members of the Court of Common Council, others within the organization, and federal and state awarding agencies, and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

Blum, Shapiro & Company, P.C.

West Hartford, Connecticut
December 27, 2020