REPORT ADDRESSING
AUDITOR'S 2023 SUGGESTED RECOMMENDATIONS

07/30/2024

CYBERSECURITY

Recent headlines have seen no shortages of cyber-attacks across the governmental landscape, including many here in Florida. These attacks have varied from using ransomware to take control of a government's enterprise resource planning (ERP) system, targeted attempts through email to change vendor information, and attacks on water supply systems whereby an attacker gained access to the water control system and altered chemical additives to the purification process.

While all attacks are difficult to eliminate, we want to recommend the Town continue to develop and maintain a functioning Cybersecurity Risk Management Program to assist with comprehensively identifying cybersecurity weaknesses, potential threats and risks, and controls used to safeguard information and systems. We also recommend that you continue to investigate, develop and consider implementation of a Cybersecurity Risk Management Program covering Cybersecurity risk assessment, identification of sensitive data, use of strong passwords, software updates/patching cadence, audit security measures, and monitoring and testing of controls in place. A complete Cybersecurity Risk Management Program also encompasses incident response, disaster recovery, and business continuity policies and procedures, as well as regular testing of the organization's back-ups. Our Firm has experts in place to help you with these efforts. Please feel free to reach out to us if we may ever be of service to you in these areas.

STAFF RESPONSE:

Town Manager Dyess has an IT background with experience in dealing with a ransomware attack and understands the concerns over proper IT solutions and procedures (the city did not have to pay the ransom). In the IT industry it is no longer a discussion of "IF" an attack occurs, but rather "WHEN". In the past it was all about blocking intrusions/firewalls/virus software, which are still important, but the internal human element is now more important than ever. A staff member clicking on what looks like a legitimate link in an email can lead to a big vulnerability that is harder to prevent than other forms of intrusion. This is why backup and recovery have become the most focused on system component in the organization's IT infrastructure.

A few years back state law changed making information about governments IT systems exempt from public record so that it was not readily available as to what types of systems and software are being used in hopes to cloud the knowledge from lawbreakers. The state then created a law to prevent any government from paying ransomware extortion in hopes to further prevent lawbreakers from attacking governments. This year's law change had to do with liability and if your organization adopted certain guidelines and reporting steps you would be exempt from liability.

In April, Town Manager Dyess adjusted the Town's technology policy to adhere to the latest law changes regarding guidelines and reporting procedures. He also removed any detail about specifics to the Town's software and systems brands. The Town does have a very good backup and recovery system and uses a 3-2-1 methodology (3 Copies of Data – Maintain three copies of data. 2 Different Media – Use two different media types for storage. 1 Copy Offsite – Keep one copy offsite to prevent the possibility of data loss due to a site-specific failure.). The Town, also, utilizes a staff training service that keeps staff updated and trained on potential attacks. This service also conducts random testing to see if anyone is falling victim to scams and then schedules them for additional training. The Town has all the standard prevention as well such as firewalls, virus protection, anomaly detection, etc. Most importantly, after evaluating our operations, Town Manager Dyess noticed that there is very little internal exposure. The Town's on-premises systems are minimal, and he would be happy to explain that to each individual Council member.

DISASTER PREPAREDNESS

Disaster preparedness has become an increasingly important issue for local jurisdictions. Entrusted with mitigating the effects of disasters, local jurisdictions regard a quick response and effective recovery a paramount goal of disaster planning. For local jurisdictions, the concept of resiliency should be an integral part of disaster preparedness. Resiliency emphasizes the capacity of infrastructure, operations, and even social systems to respond to and recover from extreme events. Resilient systems reduce the probabilities of failure, the consequences of failure (such as deaths and injuries, physical damage, and negative economic and social effects), and the time for recovery. A resiliency-based approach is not reactionary to the effects of a disaster but establishes parameters to contain the effects and because of this, a jurisdiction can measure its resiliency by how quickly it can rebound.

Traditional disaster preparedness emphasizes reacting to a disaster to effectively minimize losses rather than establishing a capital program to invest in assets that can better withstand and recover from extreme events. A growing sentiment within local jurisdictions recognizes that reactive policies may not be enough. Instituting a resiliency-based approach to capital planning can help sustain local services and assure that local jurisdictions remain functional or recover more rapidly following a disaster.

Building resiliency into the capital planning process includes setting appropriate parameters for new construction and the continued maintenance of key assets and infrastructure in order to strengthen a community's ability to withstand and respond to a disaster. Establishing a resilient capital program can aid the Town by identifying costs associated with building, rebuilding or retrofitting infrastructure prior to disasters, and emphasizes the constant need for continued maintenance and improvement. A resiliency-based capital program can help the Town identify critical assets, prioritize infrastructure risk, build in the appropriate and necessary costs, and establish a system that reduces the impact of disasters and the time required for a community to recover and get critical services back up and running.

We recommend the Town incorporate resiliency into the capital planning process to produce a sustainable community and mitigate the effects of disasters. Ways of incorporating resiliency in the capital planning process include:

a) Raising the visibility of resiliency by including in capital plans. Resiliency-based capital planning recognizes the likelihood of disasters and operates proactively to reduce effects on the community. In planning for new capital projects, resiliency should be among the factors considered in prioritizing the construction, maintenance, or replacement of infrastructure and assets.

b) Establishing roles and engaging the general public. It is essential for the Town to promote financial literacy to its citizens and its governing board so they understand the trade-offs associated with resiliency investments. For that reason, a program seeking to build a resilient community must include at a minimum the following participants: finance officers, Town manager, public safety officers, emergency management and business continuity officers, engineers and construction project managers, public works officials, building regulations staff and planning and risk management staff as well as the public.
c) Developing a resiliency plan. Identifying the types of extreme events likely to befall upon the Town and the type of infrastructure most likely to be affected provides the basis for resiliency investment and initiates the process for establishing measures of success.
d) Planning begins by identifying resiliency needs. To properly establish a resiliency-based approach to capital projects, the Town should prepare a comprehensive inventory of its physical assets, create a system to determine critical assets and respective resiliency, and establish a scoring system that evaluates levels of resiliency. By doing so, the Town can assess the ability of **infrastructure** and operational systems to withstand disasters.
e) Funding decisions should be pursued after resiliency plans and project prioritization have been finalized. Funding and building resiliency into infrastructure assets and operational systems can proceed in two basic ways. First, the Town can use the rating system and prioritization to determine if resilient practices can be funded by capital budgets. This step should consider both resilient projects and non-resilient projects, and base funding decisions on the critical nature and need of the project. Second, if resiliency funding falls outside the scope of the capital budget, the Town can pursue alternative funding mechanisms such as federal or state grants.

STAFF RESPONSE:

> The town has applied for and received a $225,000 grant to complete a resiliency study. Once the study is complete, we will start focusing on the outcomes of the study to address areas of critical need first.

INCLUDING THE FINANCE DEPARTMENT AS PART OF DISASTER PREPAREDNESS

Planning for a disaster is no easy task. Calamity, man-made or natural, may strike at any time, threatening public safety or property, and recovery can be difficult and costly. The challenges the Town could face could be even greater if the Town's emergency operations plan does not specify the roles and responsibilities the Finance Department should play an emergency. Upon determining the potential financial impact of a disaster, the Town should consider incorporating the Finance Department into its emergency operations plan and spell out four (4) phases of its emergency management process: mitigation, preparedness, response, and recovery:

a) Mitigation. The finance team actively participates in the disaster mitigation process by allocating financial resources such as hazard mitigation grants to reduce the risk of identified hazards.
b) Preparedness. The team conducts annual disaster workshops for all city departments to review the Town's policies and guidelines.
c) Response. Preparing Town staff and the community at large before an emergency takes place makes it easier for the Town to coordinate response when a disaster occurs.
d) Recovery. Because recovery can be a lengthy and costly process, the city manages its resources efficiently and tracks costs for reimbursement that will help return it to pre-disaster conditions.

Through clearly defined and designated roles, the Town's Finance Department can play a key part in ensuring that the Town mitigates its risks, is prepared, can effectively respond and quickly recover when disaster strikes.

STAFF RESPONSE:

The Town of Juno Beach does have an Emergency Management Hurricane Plan that is updated annually, and each department is involved with preparations. In the NIMS incident command structure Finance is in charge of the logistics section, which is responsible for resources and needed services to support achievement of the incident objectives. NIMS is the National Incident Management System that is utilized by FEMA. We have recently begun the process of becoming F-ROC certified by the state. This is a system that the finance director has been working on that standardizes the FEMA process and if you are an F-ROC organization and meet the qualifications the state will give you more immediate reimbursement percentages instead of waiting years on FEMA.

OPERATIONAL STRATEGY

During our discussions with management and governance, we noted that the Town has had turnover at key management positions, including the Town manager and Finance Director, within the last 12 months. Anytime there is a change in key personnel, it provides an opportunity to evaluate the operations of the Town and determine if any best practices can be implemented to enhance operating efficiencies and effectiveness. Potential areas for enhancement relate to policies, procedures, internal controls business processes, organization and general operations.

STAFF RESPONSE:

The Town of Juno Beach has recently updated and/or created policies such as personnel manual, purchasing policy, etc. to enhance operating efficiencies and effectiveness. Staff has proposed in the 2024/2025 budget a new finance software package which will create opportunity to rewrite or revise operating procedures. This creates the mechanisms to incorporate best practices. These new control mechanisms could be evaluated by an outside audit firm. Again, with two new members of leadership coming into an organization that has done it a certain way for many years could benefit from having these control mechanisms evaluated and help ensure that best practices are being applied.