Texas Council Risk Management Fund

Cyber Risk Control Services

Why Cyber Risk Control?
Risk management is a fundamental component of any successful public entity and has been for quite some time. The primary function of risk management is to allow public entity leadership to determine the best course of action based on the probability of a given outcome. As entities have embraced more technology, risk management has had to evolve to oversee not just traditional forms of potential risk such as operational, strategic, and financial; but also, the risks associated with technology. As entities have digitized, cyber risk control has become a pillar of an effective risk management strategy.

Background
Pre-breach services are a critical factor in both preventing cyber-attacks and minimizing damage after an attack occurs. Preparedness is critical, and we are poised to assist with implementing controls to reduce your cyber liability moving forward.

The Fund's IT consulting staff has 20+ years of experience with public entities and currently provides consulting services for a pool of over 1000 cities, townships, boroughs, and villages. In working with members ranging in size from a few staff to members with their own IT staff, the cyber risk control services have been designed to support members of any size.

Available Service Options
An initial phone consultation will be provided in order to determine a prioritized service plan based on the needs and risks specific to each member's operations.

Cyber Risk Services Available
- Risk assessment.
- Vulnerability audit.
- Identification and definition of staff that produces, accesses, uses, and serves as custodians of the agency's information.
- Identification of measures taken to protect the information from unauthorized access, disclosure, modification, or destruction.
- Password policy evaluation, refinement, and implementation.
- Acceptable use policy evaluation, refinement, and implementation.
- Records management plan evaluation, refinement, and implementation.
- Wi-Fi security plan evaluation, refinement, and implementation.

Identification and Prioritization of Information Assets
Information assets (hardware, software, including applications, versions and patch levels, data, etc.) would be identified to determine what is most critical to operations in order to prioritize a plan for protection of these assets.

Business Continuity Plan Development/Support
A loss can go well beyond the immediate cost of data loss or theft, so it is important to have plans in place to be able to resume operations with minimal business interruption. As part of the cyber risk control program, we would assist members with the development and implementation of appropriate business continuity plans.

Incident Response Plan Development/Support
A well thought out response plan that can be immediately implemented is another key factor in minimizing loss. We can assist members with their development of an incident response plan.

Resource Development/Coordination
Most Fund members obtain cyber coverage through Beazley. As a Beazley insured, members have access to comprehensive training materials and templates. In addition, the Texas Department of Information Resources has copious amounts of materials to address cyber exposures. Once a service plan is determined, we will identify the appropriate resources to deploy to support the plan, whether it's training programs, policy templates, or regular informational updates.

Simulated Phishing Solutions
As part of the cyber risk control program, simulated phishing solutions to mitigate the risks of inadvertent cyberattacks will be available to members. The solution includes key features like scheduling and automating phishing attacks, spoofing domains, targeting and reporting by organizational groups, and using and customizing phishing templates from a large selection of timely and relevant templates. It also includes a "Phish Alert" add-in button to email clients that allows end users to report suspicious emails.

HB 3834 Training
Members can use a learning management system to deliver a certified training course that was developed by the state https://www.youtube.com/watch?v=ofRl5VSSgNk and verify the training was completed, or we can coordinate with a state-certified training vendor to ensure training is completed. Many Fund members are currently contracting with KnowBe4 for cyber learning management services. We will work with members to ensure they are aware of and fully utilizing these available services.

Special Consultation
Special requests for information and training in the following areas can be accommodated.

- Training and Presentations
- Website and Hosting
- Network and Wireless
- Policies and Terminations
- Accounts and Passwords
- Asset Management and Disposal
- Surveillance and Monitoring
- Software and Applications
- Records Management
- Payment Card Security

- Disaster and Breach Planning
- Telework and Communications
- Endpoint and Firewall
- Encryption and Hacking
- IT Purchasing and Projects
- Imaging and Printers

Funding

These services would be available to members at no cost as a component part of the Fund's Loss Control Program. Initially, we would seek two or three volunteer members as pilot projects before making the service available to all members. Anticipated demand would be determined by demand during the pilot projects and based on feedback from the pilot project members.