Cyber Phishing Scam

Background

Tax time is a period of increased computer hacking and email phishing scams due to the amount of personal and financial information being handled. Cybercriminals have increasingly targeted municipalities because they are considered high value targets that hold a significant amount of personal identifiable information that can be stolen and sold, and because they are often soft targets. A cyber phishing scam at a CIRMA member resulted in a data breach of personal information and a significant liability loss.

Scenario

The incident occurred in February when an employee in the Finance Department received an email that appeared to be from a coworker. The email asked for the W2 forms of all employees throughout the municipality. Without verifying the identity of the coworker or the nature of the request, the employee forwarded over 1,900 W2 forms in a reply email. It was later discovered that the email request was not sent from a coworker, but by a cybercriminal posing as a coworker by "spoofing" the coworker's email address. Once the breach was discovered, the CIRMA member notified local authorities and CIRMA's claims department.

Damages. Once CIRMA was notified, CIRMA's cyber liability carrier was able to begin its forensic investigation. It was discovered that, out of the over 1,900 W2 forms that were released, 98 fraudulent tax returns were filed. Under Connecticut Public Act 15-142, the employer is responsible for providing credit monitoring to all employees who have been affected by a data breach for two years following the incident. CIRMA's cyber liability carrier was able to assist the Town in establishing this program almost immediately, which provided ease of mind to the Town and their employees. However, due to the number of fraudulent tax returns that were filed, there was a potential for $600,000 in exposure. The claim was ultimately closed for $72,000.

Key Recommendations. By implementing the programs outlined below, the municipality will have a better understanding on how to limit preventable accidents and minimize exposures.

Lessons Learned

- Verify the source of E-mail requests, especially those that ask for personal identifiable information.
- Encourage staff to report all suspicious cyber activity following with the department's internal reporting procedures.
- Contact local law enforcement and CIRMA if there is suspicion of a cyber-attack.
- Develop, implement, and provide frequent training to all staff on the municipality's Cyber Policy.
- Provide frequent training to all employees on current and emerging cyber trends.

Resources:

Understanding the Basics of Cyber Security Training Program

Cyber Security Threats to Public Entities - E-Learning Program

CIRMA's Cyber Tips & Alerts E-Publications

Cyber Security Whitepaper

For more information on this topic, please contact your CIRMA Risk Management Consultant. Please visit CIRMA.org/Training & Education page for a list of current training programs and E-Learning Center courses.

Questions? Ask your CIRMA Risk Management Consultant.