MEL CYBER TASK FORCE UPDATE

Case Study #3: We Trust The Pros

Background

With the sudden burst of ransomware claims throughout the world, notably in the public administration sector, many municipalities have moved quickly to protect themselves. In the top tiers of cyber protection are municipalities that have contracted with outside Information Technology and Security Professionals. So when multiple municipalities throughout New Jersey contracted with the same IT/Security firm to help setup computer network security and create data backups off-network what else would they have to worry about? *Spoiler Alert: IT Contractors utilize remote desktop connections into their clients' networks to perform much of their work.*

Attack

A two-pronged attack happened here accompanied by oodles of learning opportunities. WHERE the attack initiated makes this case particularly interesting and dangerous: on the IT Contractor's network. The IT Contractor was breached by an attacker; it is unknown what vector was used, but believe to be a compromised password. Time to recall that *Spoiler*: Once in the Contractor's network, the attacker was able to walk right into their clients' networks. Once in, the attacker chose to release ransomware across the clients' entire networks. Each client had ransom demands between $200,000 and $300,000, all requested in Bitcoin. Those that chose not to pay spent nearly $100,000 recovering from the incident, if not more. Did we mention the Contractor had nearly twenty (20) public sector clients that were affected? Quick math: +$4MM.

Prevention ***Included in MEL Cyber Risk Management Program:*** MEL Cyber RMP

1. **Limit RDP Access**: Even with your trusted IT Contractor, limit remote desktop (RDP) access to your network. And when access is required, monitor it and limit the time it can be accessed.
2. **IT Contractor Vetting**: Properly vet IT Contractors by requiring credentials and experience. Also, look into the contractor's own security practices, such as complex and unique passwords, use of Virtual Private Networks (VPNs) and encryption, and unique passwords when remoting into clients' systems. And of course ensure proper insurance is evidenced by the contractor to pay for losses you incur due to their errors, omissions and negligence.
3. **Backups**: At least one municipality almost escaped unscathed because they contracted for backups of all of their data. *Quick Tip: Proper backups are your "get-out-of-jail free card" following a ransomware attack*. Unfortunately, the contractor failed to ensure proper backups were in place. For reasons like this you should spot-check your backups frequently.

Closing Thoughts

It is difficult to imagine such failures by an IT Professional firm, as well as such a large single point of failure for multiple entities. But guess what? Municipalities have multiple aggregated points of failure, such as hundreds of them using the same accounting software provider, etc. While we have to balance the costs and benefits of every risk management recommendation, the steps outlined are easy additions that could have prevented the incident from ever occurring. *Bonus* ***Points: "Human error" caused by the IT Contractor.***

For details, contact the MEL Underwriting
Manager or your local JIF Executive Director

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL ·
MEL