MEL CYBER TASK FORCE UPDATE

Final Thoughts

At the end of the day, a sophisticated enough attacker will get in if they want to get in. But there are so many free or affordable security measures we can deploy to make it very difficult for attackers, as well as temper the impact of a successful attack.

The MEL Cyber Risk Management Program was specifically designed for New Jersey public entities with cost and effectiveness in mind. We strongly encourage reviewing the entirety of the program with your IT/Security Professional, and enact the program.

We also referenced a few other resources in the cases above. Such resources can be found below:

- ✓ **Contract Insurance Guidelines**: Utilize these guidelines in your IT Contractor's contract, but also start including Cyber in all of your contracts. Attached.

- ✓ **MEL Email Dos & Don'ts**: Provide to all employees, train them on it, and have them use it. Attached and here. MEL Email Dos & Don'ts

- ✓ **NJCCIC**: The NJCCIC is New Jersey's state agency on cyber security. It provides significant free resources and updates. Most importantly, register with them…..it's FREE! NJCCIC

- ✓ **MEL Cyber Risk Management Program**: The MEL Cyber RMP already highlights each of the prevention steps discussed in each case, plus many more. Based on the case studies, it is clear the MEL Cyber RMP *CAN PROTECT YOU*! Find it here. MEL Cyber RMP

Bonus Points!!!

In how many of the case studies did we see **"Human Error"** as a critical point of failure? If your answer is "4", "Four", "All", "Each one", "100%" or anything similar than you are correct! Cyber security reports are showing upwards of 90% of cyber security incidents are caused by human error.

Solution? Constant and continuous training, and utilize the MEL Email Dos & Don'ts infographic: MEL Email Dos & Don'ts.

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

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL ·

MEL