MEL CYBER TASK FORCE UPDATE

Case Study #5: The Exception (for now)

Background

It was a typical work day for a municipal employee, performing much of their work on the municipality's computer network. However, the computer screen went black for this municipal employee after clicking on a link in an enticing email, shortly followed by an ominous message demanding a ransom be paid to give them back their network.

Attack

An employee of the municipality received a phishing email containing a malicious link. Once the link is clicked, a ransomware program is downloaded. In this attack, the ransomware strain was able to spread a bit. And of course, ransom was demanded to decrypt the network. The unique part of this case is the total cost: **$0…ZERO…NADA**.

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

1. **Training**: As noted above, despite all the protections money can buy, humans are the last line of defense and greatest vulnerability. Utilize a great cyber hygiene training organization that updates their material and focuses on effective educational methods. Test your organization. And do all of this over and over again. Also, the entity's Cyber Policies should be used in the training.
2. **Bifurcation**: If possible, further bifurcate the network, separating the various categories of sensitive information.
3. **Logs**: Enable logging in your system, and test the logging for accuracy. Should an attacker get in, proper logs can tell you where they have and have not been in the network, which could be a significant difference in cost.

Closing Thoughts

So why did this case cost the municipality nothing? First, let's start with the process. The employee was well-trained; they noticed strange anomalies on the computer, and first decision made was to disconnect the data cable (NOT THE POWER). Disconnecting the data cable stops the spread of the ransomware. Next, the employee called IT Support, who then scanned the network. Finally, the municipality had proper data backups whereby they could essentially just wipe the device and reload the backup data. All in, the event took 3.5 hours from discovery to 100% again.

With the MEL Cyber Risk Management Plan, this case will no longer be the exception for the members of this program, but the norm.

Quick Tip: Do not disconnect the power unless IT has reviewed the situation and instructs you to do so. Disconnecting the power potentially causes loss of memory in the computer, which could result in loss of those valuable logs.

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

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL ·

MEL

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.