MEL CYBER TASK FORCE UPDATE

Case Study #2: Whoops!?!?

Background

We constantly identify mundane tasks during our workdays, wishing that computer program could just automatically do ___. One such task we all suffer from is sending recurring emails to the same groups of people, and luckily there is an easy solution of creating such automatic groups. What could possibly go wrong with such an innocent and helpful process?

Attack

Usually this section of the case study would describe an ominous hacker scheming to gain money from you and/or ruin and/or destroy some of your operations, but this case is far from such. A payroll manager was performing their normal annual task of sending Form W-2 Wage and Tax Statements of the municipality's employees to various senior managers. And what better way to execute this recurring task then by creating a mail merge and using email groups?

Unfortunately, the municipality did not have a comprehensive enough policy in place for employee departures, and so the sensitive (Personally Identifiable Information) documents were sent to non-employees, triggering state data breach laws. The New Jersey data breach laws prescribe special notifications be sent to the affected individuals, along with the need for a credit monitoring facility and call center for such affected individuals.

Total cost of this case was about $100,000 in legal, forensics and notification expenses.

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

1. **Policies & Procedures**: Robust policies should be created detailing things like employee departures, whereby various departments are notified to update their records following a departure. Also, employees must be continually trained on these policies, and the policies should be periodically reviewed and updated.

Closing Thoughts

Fortunately, this case stopped following the municipality's completion of its data breach notification requirements, but it could easily have become a lawsuit for breach of confidential data or potentially even worse if the attacker utilized such data for their own financial gain. Many people may say they do not need to write that down or create a process for it because it is so obvious.

The two questions that should be asked for everything we do are:

1) What happens if I forget to do that? and,

2) Will new employees/my replacement know to do this? ***Bonus Points: "Human error" again.***