MEL CYBER TASK FORCE UPDATE

In the movie "The Rock," Sean Connery and team made their way into the drainage tunnels of Alcatraz to breach the prison. Despite its high walls and rocky cliffs, the drainage tunnels were a necessary weakness of operating the prison. In so many more movies about breaches of castles or prisons, it is common to see tunnels (or even a wooden horse gift from "your friends") as the chink in the protective chain. We have these same ***necessary weaknesses*** in cybersecurity.

Third Party Vulnerabilities

Do you employ an outside Information Technology (IT) consultant? Or maybe your payroll is managed by another company? How about health insurance management for your employees? Purchasing software from other companies? The following are events experienced by MEL members surrounding third party vulnerabilities. Each event resulted in **weeks of lost or diminished productivity**, **hundreds of thousands of dollars in extra expenses** and even more in **ransom payments**.

1. IT Company: You may recall a MEL story from a few years back regarding an outsourced IT company. As is customary, the IT company had access (password protected) to their customers' networks; however, the password of an employee of the company was compromised by an attacker. Multiple MEL members were hit at once.

2. Payroll Manager: Maybe you were one of the 8 million affected by Kronos in 2021. Kronos is a very popular payroll manager, including the likes of NYC Public Employees and Tesla, as well as many NJ public entities. In December, Kronos was crippled by ransomware resulting in people not receiving paychecks; and the delays continue today.

3. Software: Have you have heard of a company called Microsoft? Their software is on over 1 billion computers. In March, a Zero Day vulnerability was discovered in its Exchange software, allowing attackers access to users' systems. The result was countless organizations finding themselves crippled by ransomware.

4. Software of Software: Does the term "Log4j" sound familiar? Log4j is software in other software. In fact, it is in a TON of other software that can be found in everything from routers to servers to video games. Log4j had a critical vulnerability, attackers were able to exploit to gain access to users' systems and millions were affected by different attacks.

MEL Cyber Program

Here are items in the MEL's Cyber Program that directly help address these third party vulnerabilities, while other controls can address tertiary damage from these events:

- ✓ Patch Management (Tier 1) – *Stories 3 & 4*
- ✓ Defensive Software (Tier 1) – *Story 1*
- ✓ 3rd Party Risk Management (Tier 1) – *Stories 1 & 2*
- ✓ Remote Access (Tiers 2 and 3) – *Story 1*
- ✓ Business Continuity (Tier 2) – *Stories 2,3 & 4*
- ✓ Network Segmentation (Tier 3) – *Story 1*

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

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL · MEL