MEL CYBER TASK FORCE UPDATE

Prevent Cyber Events: Learn from Each Other

The MEL's Risk Management programs are shaped based on the events we have experienced, as well as those of our peers. This simple principle also applies to our Cyber framework. We are, and need to be, constantly learning from each other. In this update, we present two claims experienced by our members and the claims process they experienced.

RANSOMWARE Cost a local Municipal police Department nearly 3 months and $600K.

A municipal police department clicked on a malicious file in a phishing email, allowing the attacker access to the network and eventually deploying the ransomware. The department remained encrypted for about 10 days, with no access to anything on network; just think, no employee data, payroll, investigation records, CJIS, etc. The event was noticed on a Saturday and the insurance company, cyber breach counsel, and forensic vendors were engaged by Monday. Two response tracts were running at the same time: *1) Identify where the attackers are/were in the network*; and *2) Secure the network and get operational*.

Forensics worked with the police's outsourced IT vendor in identifying nearly **1.1M data files**, while discovering backup copies of body cam footage were deleted. This turned out to be a double-extortion event, which means that not only is the system encrypted, but the attacker gains access to the system and exfiltrates data, demanding a second ransom to not release such data onto the deep web. They demanded a nearly **$1,000,000 ransom** and the attacker gave sample proof of data exfiltration. Data seen and exfiltrated included **payroll, thousands of police reports, victim/witness statements, Megan's Law PII (personally Identifying information), employee PII, employee psychological reports, internal affairs reports, disciplinary records, employee PHI (protected health information), youth academy PII, police candidate removal evidence, mugshots**, and more. It is expected the attacker was in the system for much time. During this time, forensics also recommended security measures to the police and implemented defensive software to protect the network.

END RESULT: Attacker negotiations initiated due to exfiltrated data, and such went on for nearly **six weeks**. The township was faced with deciding whether it should pay the ransom in a best effort to protect all this data or to rely on just notifying all impacted individuals. Although not frequent, there is the chance regardless of decision made of a lawsuit against the township for failing to protect the data. Ransom paid, nearly three months of interruption and credit monitoring established

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

RANSOMWARE: Cost a local Municipality nearly 3 months $300K

A municipality was breached via an unprotected remote connection, which allowed the attacker to physically enter the network. The attacker was able to exfiltrate sensitive data and encrypt the network via ransomware, which allowed them to make this a double-extortion, whereby ransom was demanded to decrypt the network and a second ransom to prevent the exfiltrated data from being released. About **$100,000 in ransom** was demanded.

The insurer, breach counsel and forensics were brought in within two days. The municipality setup dual off-network back-ups, but *both were found to be corrupted*. This emphasizes the need to not only have back-ups but set them up correctly and check them. In review of the files accessed and exfiltrated, there was **sensitive employee and third-party data**. This left the municipality with the decision of whether to pay the ransom or not or to just setup credit monitoring for affected individuals.

END RESULT: The municipality was eventually able to recover much of their data within a few weeks. Ransom was not paid and credit monitoring was setup for those affected. It took many weeks to review all potentially affected files and send proper notices to those compromised.

WHAT CAN WE LEARN?

First, if you think this cannot happen to you – think again. It is estimated that nearly **three quarters of organizations saw a cyber event last year** (5%+ of MEL members are hit each year) and the national ransomware claim average is over $4.5M. Most of our claims are in the $300K - $500K range, which is bad enough, but we have luckily not had to pay a large ransom over $1 Million, nor have we seen follow-on lawsuits.

Second, various security control failures in both of these events are glaring:

1) Not reviewing back-ups;
2) Credential integrity and password policies;
3) Encrypting and managing sensitive data; and
4) Securing remote connections.

These stories present an opportunity to think about the many decisions you will have to make when a cyber event occurs. One of the biggest -- weighing the option to pay a ransom to a criminal or terrorist organization in order to protect your data, especially when the Federal government says not to pay ransoms. So, learn from each other, and find ways to prevent and prepare for cyber-attacks, which are becoming more prevalent and severe every year.

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

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL · MEL