MEL CYBER TASK FORCE UPDATE

Recent Government Cyber Events

Regardless of the news source, whether it be cybersecurity industry blogs, local papers or national broadcasts, governmental entity cyber events are the ***#story***. If you recall our conversations between December and February, NJ public entities, including many MEL members, saw many cyber events in just a three month period. Most of these events were promulgated via remote desktop compromise and successful phishing attempts, demanding ransoms in the $200k - $300k range. We want to highlight three recent highly publicized events, taking a dive into the key issues and provide lessons learned. You may also want to re-read the bulletin we released regarding the City of Atlanta's cyber event last year. Above all, review the MEL Cyber Risk Management Program!

City of Baltimore (MD)

Date	May 7, 2019
Strain	RobbinHood
Vector	Remote desktop connections or phishing
Ransom	3 bitcoin (~$35k) per affected system or 13 (~$152k) for entire network, with a 4-10 day window

Baltimore lost a significant amount of connectivity, most notably email and phones. While emergency services continued to operate, their ability to operate efficiently and safely was impacted. Certain revenue sources to the city were also impacted, such as water billing and parking/speeding tickets. Beyond the city's own operations, the attack affected many other operations and organizations dependent on the city, such as hospitals, vaccine manufacturers, airports, real estate transactions and ATMs.

Baltimore is still recovering from the event, but estimated losses are $8,000,000 from not being able to process payments and $10,000,000 in recovery expenses.

Similar to Atlanta, Baltimore demonstrated an overall lack of preparedness for a cybersecurity incident. This is initially confirmed by public records indicating the city's information security manager requested to purchase Cyber Insurance and invest in cybersecurity in previous year, which was denied. But there were a few key missteps we can see in how the event was handled. For instance, the city made a statement saying the Eternal Blue malware, leaked by the NSA, was the horse that the RobbinHood ransomware rode in on. To date, security researchers have not found evidence of Eternal Blue being used, along with a public denial by the NSA. Making this negative publicity all the worse, the City should have known a free security patch for the Eternal Blue malware has been available since early **2017**. Aside from the negative publicity, the city clearly did not have disaster recovery plans in place, partially as evidenced by its attempt to create Gmail accounts for its users, immediately followed by Google revoking those accounts because it violated its policies on business use of Gmail accounts. Finally, there were of course the lack of other cybersecurity practices and controls, such as proper backups, security patching and employee training.

Lessons Learned? Establish proper and full technology practices (including security patching), enact and sustain employee cybersecurity training, create and practice a disaster recovery plan, and work with proper legal counsel and public relations.

MEL CYBER TASK FORCE UPDATE

Lake City (FL)

42 Bitcoins (~$426,000)
16 TB of data

Date	June 10, 2019
Strain	Triple Threat (Emotet Trojan, TrickBot Trojan, Ryuk ransomware)
Vector	Phishing with weaponized Microsoft Office document
Ransom	42 bitcoin (~$480,000)

Lake City was able to respond within ten minutes of noticing the incident, disconnecting the network; however, the malware encrypted the phone, email and other electronic systems. In the end, many systems and information were not able to be recovered. The city, along with its professionals, decided to pay the ransom to reduce the overall cost of the event, although the success of this bet will not be known until the outcome.

Lessons Learned? It is early to tell very much, including total projected cost of the claim. In good news, the city seemed to be proactive in having a response plan in place, some cybersecurity measures, and the purchase of insurance. The cause of the attack is the key issue here, which was a fake email. Also, it seems as though they may have had some issues with or had limited backups. As such, we need to provide continual cybersecurity training to employees and ensure everything critical is backed-up and working.

Riviera Beach (FL)

~$600,000

Date	May 29, 2019
Strain	Undisclosed
Vector	Phishing (confirmed)
Ransom	65 bitcoin (~$600,000)

Riviera Beach suffered a ransomware attack due to a phishing email opened by a police department employee, which took down the city's email, vendor payment and 911 dispatch systems, amongst other issues.

Lessons Learned? As with Lake City, it is still early to identify all details here and how much this event could cost. From reports, this event seems to be more widespread than the Lake City event, affecting even the 911 dispatch system, which could result in bodily injury. Due to phishing being the vector, employee cybersecurity training is a must. In addition, it seems as the backups were insufficient or not working, so full and checked backups should be performed.