MEL CYBER TASK FORCE UPDATE

THERE IS NO SUMMER VACATION FOR CYBERSECURITY

Recent attacks should serve as a warning about how important it is to review your cyber risk management programs and find ways to better protect your networks. A simple breach in cyber security can cause a massive disruption to service, financial loss and can impact lives.

I. COLONIAL PIPELINE

A major U.S. oil pipeline was forced to shutdown due to a ransomware incident. The incident shows the typical administrative shutdown due to the malicious network encryption, but also the shutdown of its oil operations, which hits upon many risk management areas, including property damage, product damage, interruption and public relations.

The event boils down to two basic cybersecurity issues:

1) A compromised password; and
2) An unused remote connection.

Since a single password was compromised with no other evidence of breach, it was most likely due to such employee using the same password and/or email on more than one network (i.e. home and work email).

Takeaways:

1) Require strong passwords/passphrases/secrets, which are unique to the work account -- and consider changing them on a regular basis.
2) Inventory all remote connections/accounts with remote access -- and have a policy for regularly reviewing and closing unused remote connections.
3) There is also a chance the password was compromised in another breach, so consider utilizing deep web scans for previously breached accounts and passwords.

- more-

MEL CYBER TASK FORCE UPDATE

II. MASSACHUSETTS STEAMSHIP AUTHORITY

"We don't have cyber exposures like banks or pipelines." This is a phrase we thought we would not be hearing much of anymore, but new headlines reinforce the fact organizations of all types have cyber exposures and can be greatly affected.

The Massachusetts Steamship Authority, which operates a simple ferry service, is still recovering from a ransomware incident. Aside from the inability to access administrative systems, patrons are forced to pay with cash and bring paper trails of their tickets. The event luckily has not affected the actual ferry electronics and network, but the Authority may not have thought of such a scenario in the past. Imagine engine or navigation systems being affected.

Takeaways:

The cause and extent of the incident is still unknown, but the standard ransomware prevention tactics should be utilized:

1) Strong passwords policies
2) Remote connection security
3) Multi-factor authentication
4) Proper back-ups
5) Segregation of operational units

III. MULTIPLE HOSPITAL RELATED EVENTS

Numerous hospitals and emergency dispatch networks have been affected and even crippled by cyber incidents over past few years. One emergency department was shutdown due to a ransomware incident, forcing a cardiac arrest patient to be sent to another hospital about an hour away. The delay was a key factor in the patient's passing.

-more-

MEL CYBER TASK FORCE UPDATE

III. MULTIPLE HOSPITAL RELATED EVENTS *(continued)*

First response organizations must not only properly protect themselves from incidents, but also have contingency plans in place to continue their critical operations.

Takeaways:

In addition to all of the typical cyber event prevention steps, detailed incident response and disaster recovery plans must be in place (and continually practiced and reviewed) to continue operations. Your Continuity of Government (CoG) plans also need to address all of these cyber concerns.

SOLUTIONS

"What are we supposed to do?"

Every computer user MUST have a copy of the MEL's Email Dos & Don'ts infographic (click to download). We would have less than half of the incidents experienced so far if these guidelines were followed.

"I wish there was a cybersecurity guide telling me what I should do to help prevent these types of attacks."

There is! The MEL Cyber Risk Management Program - - AND we will reimburse you up to $25,000 for being in compliance at the time of a claim. Click here to download the latest Cyber Risk Management Program.

"Now I have to spend all of this time and money creating special policies and procedures."

NOPE! It's already done for you. MEL has put a template technology policy and incident response plan in the Cyber Program and our insurer (AXA XL) offers many more free templates.

- MEL Cyber Risk Control web page for more resources and information.
- AXA CyberRiskConnect - Use code 10448 to register.