Q&A

1. How do I select an employee training vendor?
    - See the Cyber Hygiene Training Vendor guide on our website.

2. Where can I find policies to comply with the MEL Cyber Risk Management Program?
    - Template versions of all of the policies needed for compliance can be found in the plan. Additional template policies can be found on our insurer's (AXA XL) Cyber website: https://www.cyberriskconnect.com, use 10448 as the Access Code when registering for the first time.

3. What do I do when I have (potentially have) a cyber incident?
    - Report the incident to your JIF Claims Administrator and call the AXA XL Breach Hotline at 855-566-4724. Also enact your Incident Response Plan, which should include getting in touch with your risk manager (if applicable). You can also review the Cyber Incident Roadmap to see all steps you will be taken through: https://njmel.org/wp-content/uploads/2017/11/cyber-incident-roadmap.png

4. Are there any incentives for compliance with the Cyber Risk Management Program?
    - Yes. Compliance with Tier 1 provides a $5,000 reimbursement on your Cyber deductible. Compliance with Tier 2 provides an additional $2,500 reimbursement ($7,500 total) on your Cyber deductible.

5. When resolving the claim for a cyber incident, can I be reimbursed for the time my employees allocated to recovering from the incident?
    - Via the Business Interruption and Extra Expense coverage of the Cyber policy, only the payroll and expenses above and beyond the normal hours can be recovered, such as overtime. In addition, most additional costs for an outside IT provider (should you not have one on staff) cannot be recovered.

6. I don't process credit cards or store confidential data, so why should I bother with the risk management plan?
    - Over 90% of the MELs' members' cyber claims have not had to do with credit cards or sensitive data. Rather they are mostly dealing with business interruption and loss of data from ransomware, and loss of funds from social engineering. Also, despite not storing confidential data, you may still be responsible for protection of the data; please consult your counsel.

7. Some of the questions on the Cyber Risk Management Plan are not applicable to my network setup, so how can I comply?
    - Please contact the MEL Underwriting Manager to discuss those items. The plan is written in a general nature to allow for variations, and not applicable questions have been approved in the past.