Kamini Patel, MBA, CIC, CPCU, AIDA ®
Deputy Executive Director

Cyber Risk Initiatives

- MEL Cyber Risk Management Plan
- Cyber JIF
- Employee Cyber Hygiene Training
- Phishing Campaign
- External Network Vulnerability Scanning
- External Network Penetration Testing
- Technology Risk Services Director

MEL Cyber Risk Management Plan

- **Version 1.0 - Released in December 2017 - Two Compliance Tiers**
  - Tiers Security standards based upon current loss trends
  - Compliance with Tier 1 - $5,000 Reimbursement of deductible
  - Compliance with Tier 2 - $7,500 Reimbursement of deductible
- **Version 2.0 - Released in September 2020 - Three Compliance Tiers**
  - Tiers Security standards updated based upon current loss trends
  - Deductible Reimbursement
    - Tier 1- $10,000
    - Tiers 1 & 2- $20,000
    - Tiers 1, 2 & 3 – $25,000

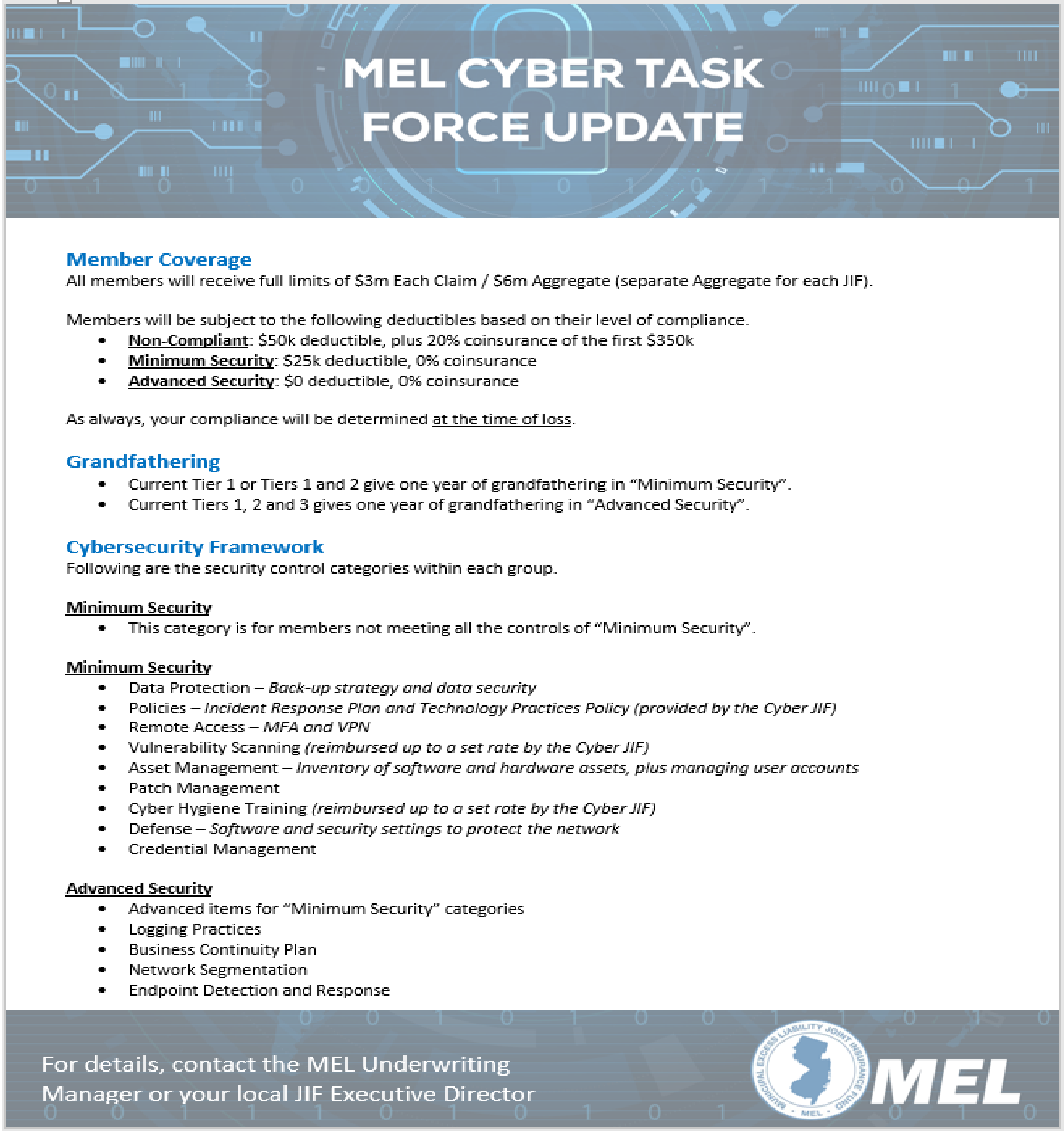
The MEL Cyber Risk Management Plan has matured as the cyber risks have become more sophisticated

MEL Cyber Risk Management Plan

- Compliance Status as of December 31, 2022 for TRICO JIF Members
  - Tier 1- 74%
  - Tier 2- 68%
  - Tier 3 - 63%

Cyber Risk Management JIF

- Cyber is very unique peril
- The program is more about managing the risk of the use of technology by the members than coverage for a loss
- Easier to secure coverage for the entire membership
- Greater flexibility in changing programs & coverage
- The MEL's positive experience with the E-JIF



MEL CYBER TASK FORCE UPDATE

Member Coverage

All members will receive full limits of $3m Each Claim / $6m Aggregate (separate Aggregate for each JIF).

Members will be subject to the following deductibles based on their level of compliance.

- **Non-Compliant**: $50k deductible, plus 20% coinsurance of the first $350k
- **Minimum Security**: $25k deductible, 0% coinsurance
- **Advanced Security**: $0 deductible, 0% coinsurance

As always, your compliance will be determined at the time of loss.

Grandfathering

- Current Tier 1 or Tiers 1 and 2 give one year of grandfathering in "Minimum Security".
- Current Tiers 1, 2 and 3 gives one year of grandfathering in "Advanced Security".

Cybersecurity Framework

Following are the security control categories within each group.

Minimum Security

- This category is for members not meeting all the controls of "Minimum Security".

Minimum Security

- Data Protection – *Back-up strategy and data security*
- Policies – *Incident Response Plan and Technology Practices Policy (provided by the Cyber JIF)*
- Remote Access – *MFA and VPN*
- Vulnerability Scanning *(reimbursed up to a set rate by the Cyber JIF)*
- Asset Management – *Inventory of software and hardware assets, plus managing user accounts*
- Patch Management
- Cyber Hygiene Training *(reimbursed up to a set rate by the Cyber JIF)*
- Defense – *Software and security settings to protect the network*
- Credential Management

Advanced Security

- Advanced items for "Minimum Security" categories
- Logging Practices
- Business Continuity Plan
- Network Segmentation
- Endpoint Detection and Response

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

How Does This Impact Me?

Your municipality experiences a cyber incident which results in a $500,000 loss. How much will it cost your municipality?

MEL Program	
Not in compliance	$25,000 Deductible
Tier 1	$25,000 Deductible - $10,000 reimbursement $15,000 Member's responsibility
Tier 2	$25,000 Deductible $20,000 reimbursement $5,000 Member's responsibility
Tier 3	$25,000 Deductible $25,000 reimbursement $0 Member's responsibility

Cyber JIF	
Not in compliance	Member pays $50,000 deductible plus $60,000 (20% of next $300,000) in co-insurance Total: $110,000
Basic	Member pays $25,000
Advanced	$0

Cyber Security Initiatives – TRICO JIF

- RFP for Cyber Security Services – 2022 - Present
- Awarded contracts to Wizer & D2
- Employee Cyber Hygiene Training, Phishing, External Network Scanning, Annual Network Penetration Testing

The Goal – Make the services needed to comply with the Cyber JIF Program requirement available to all Members in a consistent and cost effective manner

Wizer

D2 CYBERSECURITY

Employee Cyber Hygiene Training
as of June 29, 2023

- Two 30 minute training sessions each year
- First training released in February 2023
  - 1,747 employees registered
  - 83% of employees completed the training
- Second training released on July 10, 2023

Phishing Campaign

- Whitelisting must be completed
- 22 members are actively participating
- 1 members waiting confirmation of test email
- 14 member is not participating
- Randomly tests your employee’s knowledge
- **Current Statistics as of June 30, 2023:**
  - 6,609 Phishing emails sent
  - 1,993 Phishing emails were opened
  - 233 links were clicked
  - 3.53% Click rate

External Network Scanning & Penetration Testing

- Verification of IP addresses and points of contacts started in January 2023 and is currently ongoing.
- As of July 17, 2023:
  - 35 out of 37 members are participating in **monthly** external network vulnerability scanning.
  - 35 out of 37 members are participating in **annual** external network penetration testing.

Technology Risk Services Director

- Contract awarded to Wintsec Consulting effective February 01, 2023.

Goal:

Assist Members and/or their IT vendors in understanding & complying with cyber security initiatives

Help Us Help You

- Share the new Cyber Security Program with your IT vendor
- Make a plan for compliance with the new standards that meets the Cyber JIF requirements prior to **01/01/2024**
- Utilize your EPL/Technology Risk Management Budget to help offset compliance costs
- Reach out to the Technology Risk Services Director for assistance

Special Mentions:

Thank You

To all the Members that have embraced the cyber security initiatives and have shown continuous commitment and improvement to your cyber security profile!

Kamini Patel, MBA, CIC, CPCU, AIDA ®
Deputy Executive Director

Gloucester, Salem,
Cumberland Counties
Municipal Joint
Insurance
Fund
JIF
Established in 1991
South Jersey Communities Securing Their Future

Technical Risk Services Director

aka “JIF Geek”

Three P's of Cyber Protection

People

- Represents 80% of the exposure to Cyber intrusion

Places

- Represents 10% of the exposure to Cyber intrusion

Procedures

- Represents 10% of the exposure to Cyber intrusion

- The form has a lot of statements but little substance, I am looking for policies I can implement.
- Must adhere to any additional Cybersecurity practices required by “law.” Where do I find that?
- Adopt a password policy to meet the NIST Password Standards 800-63B. This document is about 100 pages of techspeak that is 6 years old, updated once in 2020. Can’t you just tell me what the policy is?
- Disable unused ports on PC’s is not practical; the Police trade secure sticks with the Prosecutor’s office with evidence. I can’t have my IT person called in every time this occurs, could be at night.
- Segment your network key units such as finance, HR etc. We have one switch, one copier, one internet, one server…how can we do this?
- We replace PC’s on a needed basis; don’t have a standard image…the hardware changes so much. How does a standard image protect us anyway?
- 24/7 support…What is it? Who does it?
- Organization leadership has access to expertise that supports technology decision making. This is a statement not a policy.
- Risk rank third party providers based on accesses. What is a good/bad rank?
- When we ask for clarification, we are told to Google it.

Gloucester, Salem,
Cumberland Counties
Municipal Joint
Insurance
Fund

JIF

Established in 1991

South Jersey Communities Securing Their Future

?