



Protect Your Municipality Against Ransomware Attacks

Across the country many state and local government partners have been targeted by ransomware attacks. If infected, ransomware can immediately shut down your business by blocking access to your networks and critical data. Statistics show that the average ransomware infection can cost over \$125,000.00. Through implementation of some basic cybersecurity measures, businesses can effectively minimize the risk of a ransomware attack. Cyber preparedness is critical to secure your networks and prevention is the most effective defense against ransomware.

The Cybersecurity and Infrastructure Security Agency (CISA), Multi-State Information Sharing and Analysis Center (MS-ISAC), National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO) have called for all levels of government to take the following three steps to resilience against ransomware.

- 1. Back-Up Your Systems Daily**
- 2. Reinforce Basic Cybersecurity Awareness and Education**
- 3. Revisit and Refine Cyber Incident Response Plans**

MIIA CyberNET Coverage is tailored to meet the specific need of municipalities. The Cyber Security Training area of our website, emiia.org, provides access to resources to assist you with steps 2 and 3 as you strengthen your cyber defense strategy. Please review our offerings and talk to your Account Representative if you have any questions about these training programs. Which are all free to our members.

Reinforce Basic Cybersecurity Awareness and Education Resources

Go to MIIA CyberNET area of the MIIA website to learn more about how to reduce your risk of a costly ransomware attack. Within our Best Practices section, you'll find:

- Ransomware Training Video
- Ransomware: The Basics and Prevention
- Beware of Ransomware! Poster

Within our Recorded Webinars section, leading experts discuss topics ranging from broad issues, such as social engineering, to more technical topics like encryption, tokenization or ransomware.

- Cyber Threat Update: Spotlight on Ransomware

Revisit and Refine Cyber Incident Response Plans

Incident response is a structured methodology for handling security incidents, breaches, and cyber threats. A well-defined incident response plan allows you to effectively identify, minimize the damage, and reduce the cost of a cyber attack, while finding and fixing the cause to prevent future attacks.

Also, within the CyberNET area of our website, you'll find Incident Response Plans. Which includes the following content to support you in every step of your planning.

- Getting the Board "on Board"
- Building an Incident Response Team
- Training Employees to Report Data Security Incidents
- Preparing an Incident Response Plan
- Testing the Plan
- Industry Specific Considerations: Healthcare/Financial/Retail
- Additional Guidance on Incident Preparedness and Response
- Archived Webinars on Incident Response from leading legal, regulatory and data security experts

MIIA CyberNET – Personalized Support and Risk Management

MIIA's CyberNET® Protection includes access to expert cyber risk advisors when you need them, plus 24/7 online training courses, sample cyber risk policies and procedures, as well as guidance with sample contract provisions that can be added to vendor agreements to reduce cyber risk exposure.

MIIA is focused on helping you and your organization mitigate the risk and impact of a cyber breach.

Cyber Security Training

Get 'cyber smart' with online courses, including:

- Data Security Basics
- Social Engineering and Phishing Schemes
- Ransomware Attacks

Compliance Material

Keeping your organization up to date:

- State and Federal, Industry Specific
- Data Protection Guidelines
- Links to Government Sites

Risk Management Guidance

Implement preventative measures:

- Best Practice Guidelines
- Risk Assessment & Fitness Checklist
- Incident Response Planning

Contact your MIIA Account Representative to learn more about all of the Cyber Liability Protection that is available to help protect your digital assets.