# CYBERSECURITY TOOLKIT

## FOR FMIT CYBER LIABILITY MEMBERS

FMIT
FLORIDA MUNICIPAL INSURANCE TRUST

FMIT
FLORIDA MUNICIPAL INSURANCE TRUST

## How to Report a Cyber Claim to the Florida Municipal Insurance Trust (FMIT):

You may email the cyber claim details and/or the completed Data Breach Claim Report Form to *newloss@flcities.com*.

You may also call 407.425.9142 or 800.445.6248 and select option 5, which will ring our Property & Liability Claims Supervisors. If it is before business hours (before 8:30 a.m.) or after business hours (after 5:00 p.m.), please contact **Chris Smith**, Property & Liability Claims Manager, on his mobile phone at 772.215.4031.

As soon as FMIT is in receipt of the cyber claim, we will immediately contact our cyber reinsurance partner Beazley to begin the investigation and notification process.

## What to Expect Once an FMIT Cyber Claim Has Been Filed:

1. Once a cyber claim is received, an adjuster from the FMIT will contact the member and send a Data Breach Claim report, which must be filled out as soon as possible and returned to the FMIT claims team.
2. The FMIT claims adjuster will send the Claim Report to Beazley (FMIT cyber reinsurance partner), who will respond within one business day with several different contacts, a breach response adjuster (if applicable), the indemnity adjuster, and the coverage adjuster.
3. Beazley will forward a list of pre-approved vendors for the member to engage with breach response and other services to quickly assess the cyber claim and create a path forward to resolution. These vendors will often require execution of a statement of work or contract by the member for their services to be provided.
4. Once the vendor response is initiated, Beazley will request that the member forward all invoices to their attention for review.
5. After Beazley reviews and approves the invoices, Beazley will forward them to the member to pay until they exhaust their retention (deductible).
6. Once the member's retention is exhausted, Beazley will forward the invoices to FMIT for payment. If the member does not have a retention, FMIT will pay all approved invoices incurred.

The Beazley and FMIT claims staff will work diligently to assist the member in the resolution of the claim. Once all invoices have been paid and no further action is required, FMIT and Beazley will close their files.

FMIT
FLORIDA MUNICIPAL INSURANCE TRUST

## Be Prepared to Answer These Questions After a Breach:

- Are you reporting an actual or suspected breach incident?
- Please describe the nature of the breach incident.
- When did the breach incident occur?
- In what city and state did the breach incident occur?
- When did you or your organization first discover that the breach incident occurred?
- What type of personal or confidential information is potentially implicated by the breach incident?
- How many individuals do you suspect are affected by the breach incident?
- If any electronic devices were involved in the breach incident, were they encrypted?

## Be Prepared to Provide the Following Information:

- Claim Number (Company internal reference)
- Policy Number
- Insured
- Insured Main Contact
- Insured Contact Phone Number
- Insured Address
- Insured Email Address
- Date Claim Received by Company

## Cybersecurity Best Practices for First Response to a Known Breach:

- When containing the attack as a first response, disconnecting infected devices from the network does **NOT** mean unplugging computers and servers.
- Always leave power on for all devices.
- Have a system in place that acts as an internet kill switch.
- Disconnecting from the internet from all points of access is the best way to limit the damage and preserve the data that forensic teams will need to determine the best path forward.
- Never unplug or turn off power, only disconnect from the internet.

**Resource:** *Incident Response in Action: What to Do When a Cyber Attack Hits - Visual Edge IT*

# Cybersecurity First Response Roadmap

01

## Detect and Identify the Threat

- Computer(s) running slowly
- User(s) locked out of accounts
- User(s) cannot access their documents
- Messages on screen demanding payment
- People indicating they received strange emails from your domain

02

## Contain the Attack

(Do NOT power off! Only disconnect from the internet network provider)

03



## Communicate Internally and Externally

- See FMIT's Cybersecurity Toolkit for contact information

04

## Assess the Damage

05

## Activate Incident Response Plan (IRP), Contact Insurance Provider and Law Enforcement

06

## Rebuild Systems as Needed

(AFTER clearance from cyber insurance provider)

07



## Work with Forensics Team

- Determine root cause

08

## Conduct After-Action Review

- Document lessons learned and areas for improvement

FMIT

FLORIDA MUNICIPAL INSURANCE TRUST