# RISKY BUSINESS

| MVRMA OFFICERS | |
| --- | --- |
| **PRESIDENT** | **BILL KUCERA, BEAVERCREEK** |
| **VICE PRESIDENT** | **EMILY CHRISTIAN, MIAMISBURG** |
| **TREASURER** | **KATIE SMIDDY, MONTGOMERY** |
| **SECRETARY** | **SANDY CAUDILL, MVRMA** |

| MVRMA STAFF | |
| --- | --- |
| **EXECUTIVE DIRECTOR** | **TOM JUDY** |
| **LOSS CONTROL MANAGER** | **STARR MARKWORTH** |
| **OFFICE MANAGER** | **SANDY CAUDILL** |

## COUNSELOR's COMMENTS

### Status of Vaccine Mandates in Ohio

*By Surdyk, Dowd and Turner*

On July 14, 2021 Gov. Mike DeWine signed into law HB 244, that prohibits public K-12 schools, colleges and universities from requiring individuals to get a vaccine if the vaccine does not have "full approval" from the U.S. Food and Drug Administration. This law applies the current Covid 19 vaccines (Pfizer, Moderna and Johnson& Johnson), which have all been approved by the FDA through Emergency Use Authorization.

The law provides that Ohio public schools cannot "discriminate" against an individual who has not received the vaccine, defining discrimination to include "requiring an individual to engage in or refrain from engaging in activities or precautions that differ from the activities or precautions of an individual who has received such a vaccine." For example, under the new law a public school could still mandate mask wearing for all students, but could not mandate that only non-vaccinated individuals be required to wear one. This prohibition does not however apply to private schools, and hospitals and health care facilities that are owned by, operated by, or affiliated with a university of college.

The provisions of the bill do not go into effect until October 13, 2021, and Governor DeWine has expressed his support for prompt full FDA approval of the vaccines. If full approval were to occur, the prohibitions contained in the law would not apply.

The Ohio House has also taken further action to try to prohibit both public and private employers from requiring employees to get the vaccinations. Currently there is nothing prohibiting an employer from requiring

*Counselor's Comments...continued*

the vaccine, subject to making accommodations for (1) individuals with a disability that would prevent them from getting the vaccine, or (2) individuals with a sincerely held religious belief that prevents them from being vaccinated.

House Bill 248 (Vaccine Choice and Anti-Discrimination Act), was introduced in April. Among its many provisions, it would prevent both public and private employers from requiring its employees to receive **any** vaccine, which would even include vaccines fully approved by the FDA. Governor DeWine has publicly opposed the bill. It has further met opposition from business groups, the Ohio Chamber of Commerce and multiple health care associations including the Ohio State medical Association.

The Ohio house has adjourned for the summer with HB 248 remaining in committee. We shall continue to monitor it progress once the proposed bill and provide updates as necessary.

# FYI –

# July 1, 2021 Property Insurance Renewal

*By Tom Judy*

The MVRMA Board recently approved the renewal of the pool's excess property insurance coverage for July 1, 2021 to July 1, 2022. MVRMA self-insures the first $250,000 of most property losses. Excess insurance coverage is purchased for claims exceeding that amount. This property insurance market has been difficult for the last several years. Our excess coverage will see a 40% rate increase for the 2021-22 policy year. This follows double-digit increases of 17% and 9% in the two previous years. The initial catalyst for this nation-wide prolonged hard market were extremely large weather-related losses in 2017-18. This trend continued and was exacerbated by the COVID-19 pandemic and the impact of the historically low interest rates on insurers' investment earnings. The trend of large insurance losses continued as 2020 was the fifth worst loss year ever for the property insurance market. The first quarter of 2021 will set a record for the most first quarter claims ever filed. As a result, many carriers pulled back from this market. During this renewal, our brokers approached several dozen carriers, but we received only two proposals, the best of which was with our current carrier, the Alliant Property Insurance Program. Although MVRMA's property losses continue to be low, it is impossible to escape this national tidal wave in the property insurance market. It is only because of MVRMA's good claims experience that the increases were not even larger.

*FYI – Continued*

The graph below illustrates the historical rates associated with MVRMA's excess insurance coverage. You will note a large spike in the post-9/11 period followed by a prolonged period of favorable rates. The rates in the current hard market now exceed the previous peak in 2003.

## MVRMA Property Rates
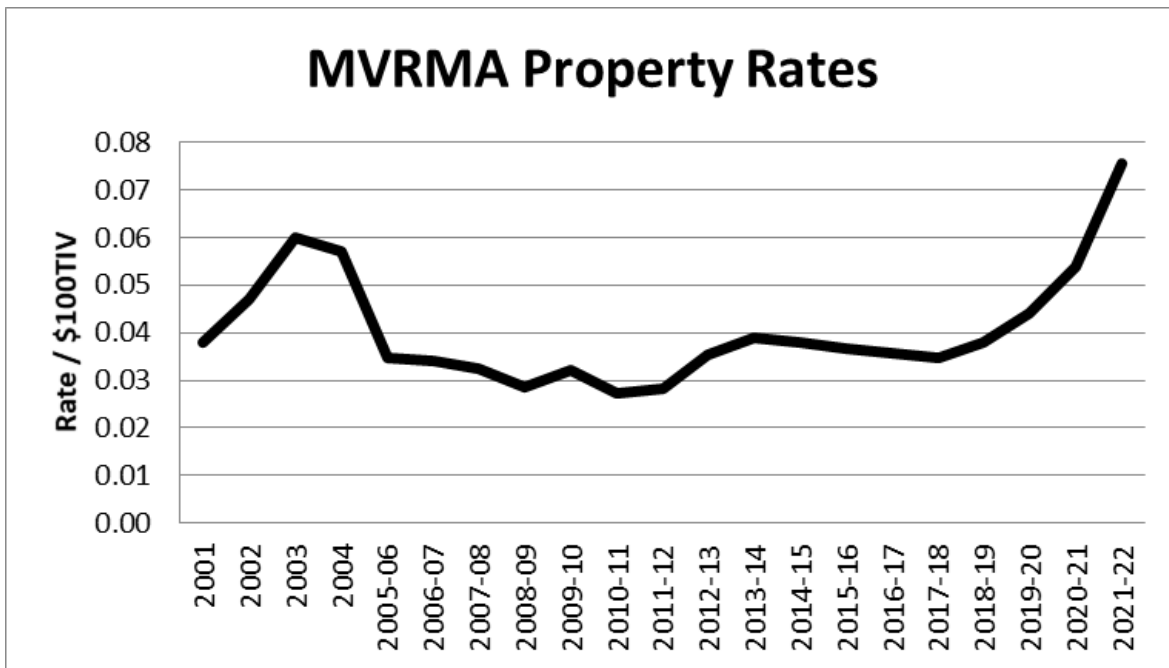


The concept of pooling came into being for times like these. Public entity risk pools were created at a time of crisis when commercial insurers abandoned the municipal market in the 1970s and then again in the 1980s. It became necessary for public entities to find a new way to finance insurance losses. MVRMA was formed in 1988 during such an insurance market. Spreading the risk over a larger base creates more pricing stability. Also, by pooling their resources, pool members can self-insure for most losses and purchase insurance for only the high-dollar claims. This enables pool members to distance themselves from the unforgiving volatility of the commercial insurance market. For instance, MVRMA members use their pooled resources to fund a large deductible - $250,000 for most property claims. Over 99% of MVRMA members' property claims are under that amount. On the other hand, it likely would be difficult for the average small municipality purchasing coverage on a stand-alone basis to assume that much risk and their premiums would skyrocket in a market such as this. There definitely is strength in numbers.

# RISKY BUSINESS

## Loss Control Lowdown…
### *MVRMA Launches a New Website*

*Starr Markworth*
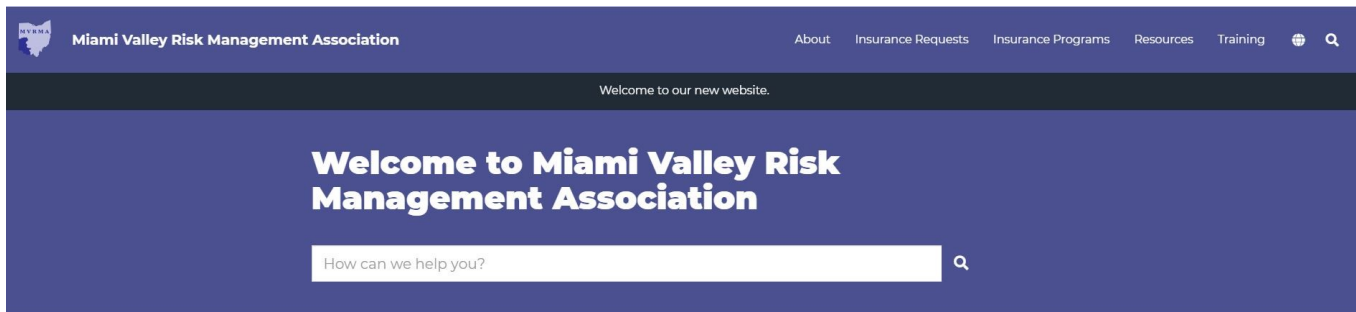


Miami Valley Risk Management Association (MVRMA) has launched its new website located at www.mvrma.com.

The new user-friendly design greatly simplifies the process of navigating MVRMA's website. The previous website had been in place since 2012 and content had been updated but design and structure had remained the same.

The new, service-focused website is mobile-friendly, secured for user privacy protection, and makes accessibility a priority. The new website has a sharp new look and feel and creates a better user experience for both desktop and mobile users.

The new website also better empowers MVRMA staff who manage ongoing updates and changes to content as website administration.

The website includes an *About* section with general information, *Insurance Requests*, *Insurance Programs*, and *Resources* sections for MVRMA members as well as a *Training* section for upcoming training and online registrations.

MVRMA is collaborating with government technology software-as-a-service company ProudCity (https://proudcity.com) for its digital city platform. MVRMA has contracted with ProudCity to manage all software, hosting, as well as staff training and support needs.

Please contact MVRMA staff if you have any questions.

# 2020 Risk Management Performance Awards

At the June 2020 board meeting members were recognized for their loss control successes.

The Standard of Excellence Award is earned by member cities who incur claims losses less than $100 per full-time employee for the year.  The 2020 Standard of Excellence Award winners were the cities of  Mason, Montgomery, Sidney and Springdale.  The city of Bellbrook and Madeira received special recognition as Overall Winner.

Members' departments with zero losses for the year receive recognition in the form of a breakfast or other celebration.  A total of 45 of our members' departments qualified for this award.

Special recognition is given to departments with three ore more consecutive years with zero losses. These departments are presented with a plaque commemorating this achievement.  Departments so recognized were:

| CITY/DEPARTMENT | CONSECUTIVE ZERO LOSS YEARS |
| --- | --- |
| Bellbrook  Streets / Refuse / Public Works | 3 |
| Blue Ash Police | 3 |
| Englewood  Water / Wastewater | 3 |
| Englewood  Parks / Recreation | 3 |
| Montgomery  Streets / Refuse / Public Works | 3 |
| Troy  Fire | 4 |
| Vandalia  Water / Wastewater | 4 |
| Bellbrook Fire | 5 |
| Madeira Parks / Recreation | 5 |
| Indian Hill  Police | 6 |
| Tipp City  Streets / Refuse / Public Works | 6 |
| Indian Hill  Parks / Recreation | 7 |
| Wilmington  Fire | 7 |
| Bellbrook  Water / Wastewater | 8 |
| Wyoming  Parks / Recreation | 12 |

# Broker's Beat

## Protecting your City Against Ransomware

A ransomware incident is one of the most disruptive and costly attacks a City can suffer. Ransomware is on the rise and is showing no signs of slowing down. Public entities are one of the most targeted industries and as a result, many carriers will no longer write public entities or pools.  This has resulted in meaningful premium increases and coverage restrictions.

MVRMA's primary cyber carrier, Beazley's claims and breach response services teams, in conjunction with their partners, have developed a ransomware best practices guide to help you prevent these incidents from occurring.

**Minimum protection**
- Deploy and maintain a well configured and centrally managed End-Point Protection (EPP) solution: A robust EPP/anti-virus solution is a basic component of any security program.
- Email tagging: Tag emails from external senders to alert employees of emails originating from outside the organization.
- Email content and delivery: Enforce strict Sender Policy Framework (SPF) checks for all inbound email messages, verifying the validity of sending organizations. Filter all inbound messages for malicious content including executables, macro-enabled documents and links to malicious sites.
- Office 365 add-ons and configuration: Enable two-factor authentication (2FA) on Office 365 and use Office 365 Advanced Threat Protection.
- Macros: Disable macros from automatically running. Ideally disable them from running at all if your business does not need them.
- Patching: Conduct regular vulnerability scans and rapidly patch critical vulnerabilities across endpoints and servers – especially externally facing systems.
- Remote Access: Do not expose Remote Desktop Protocol (RDP) directly to the Internet. Use Remote Desktop Gateway (RDG) or secure RDP behind a multi-factor authentication-enabled VPN.
- Media usage controls: Put in place controls on the insertion and/or use of media which does not carry appropriate authentication/media identifiers.
- Well-defined and rehearsed incident response process: Helps mitigate losses and rapidly restore business operations after a ransomware attack.
- Back-up key systems and databases: Ensure regular back-ups which are verified and stored safely offline.
- Educate your users: Most attacks rely on users making mistakes, train your users to identify phishing emails with malicious links or attachments. Regular phishing exercises are a great way to do this.
- Firewalls: Use network and host-based firewalls with well considered rule-sets, for example, disallow inbound connections by default.

**Broker's Beat…Continued**

### Stronger protection

- Establish a secure baseline configuration: Malware relies on finding gaps to exploit. A baseline configuration for serves, end-points and network devices that conforms to technical standards such as Center for Internet Security (CIS) benchmarks can help plug those gaps.
- Filter web browsing traffic: Web filtering solutions will help prevent users from accessing malicious websites.
- Use of protective DNS: Helps deny access to known malicious domains on the Internet.
- Manage access effectively: Ransomware doesn't have to go viral in your organization. Put in place appropriate measures for general user and system access across the organization: privileged access for critical assets (servers, end-points, applications, databases, etc.) and enforce multi-factor authentication (MFA) where appropriate (remote access/VPN, externally facing applications, etc.)
- Regular testing of back-ups: Reduces downtime and data loss in the case of restoring from back-ups after a ransomware attack.
- Disconnect back-ups from organization's network: Prevents back-ups from being accessed and encrypted by ransomware in case of a successful attack on an organization's main network.
- Separately stored, unique back-up credentials: Prevents bad actors from accessing and encrypting back-up data.

### Best protection

- End-point detection and response (EDR) tools: EDR solutions monitor servers, laptops, desktops and managed mobile devices for signs of malicious or unusual user behavior/activity. These tools also enable near immediate response by trained security experts. When effectively deployed and monitored, EDR tools are one of the best defenses against ransomware and other malware attacks.
- Intelligent email evaluation: Automatically detonate and evaluate inbound attachments in a sandbox environment to determine if malicious prior to user delivery.
- Centralized log monitoring: Centralized collection and monitoring of logs, ideally using a Security Information and Event Management (SIEM) system, identifies threats which breach your internal defenses.
- Subscription to external threat intelligence services: Provides access to external services that can provide details of developing attacker tactics, techniques and procedures. They also provide access to databases of known bad websites, mail attachments, etc.
- Encrypted back-ups: Prevents use of back-up data by bad actors.
- Network segregation: control access and/or traffic flow within the network environment. A well-configured firewall rule set will ensure that only the required traffic can flow from one segment to another. Furthermore, segregate end of life/support systems/software as a priority.
- Web isolation: Use of a web-isolation and containment technology to create a secure Internet browsing experience for your users.
- Application permissions: Only permit applications trusted by your organization to run on devices.

# Calendar of Events

**Upcoming Training Events**

Verbal De-escalation for Law Enforcement - August 24th-27th

Driver Trailer Training - August 3rd, 5th, 10th, 12th and 19th

Fall Heavy Equipment Driver Training

**Upcoming Board Events**

**Committee Meetings**

    Risk Management - September 2nd, 10:00 AM
    Finance - September 2nd,  1:30 PM

**Board Meeting**
September 20th, 9:30 AM at Home2Suites, Centerville

## *From The Board Room*
## *June 21, 2021*

- Approved property/cyber/pollution liability renewal

- Approved the 2021-2022 property coverage document

- Approved excess cyber renewal

- Approved deadly weapon renewal

- Approved the 2020 annual report

- Approved the 12/31/20 actuarial report

- Approved Target Solutions renewal

- Approved the 2020 awards

- Approved the revised contingency plan