Members Partner with MMRMA to Achieve Shared Value

by Michael Bosanac, Board Chairman

**WHEN IT COMES TO BUSINESS**

relationships, a key focus is often the perceived value of the arrangement. Many factors go into the ultimate measurement of perceived value: services, expertise, responsiveness, outcomes, and cost. Depending on who is evaluating, other criteria might also be important. Stakeholders form many personal and professional beliefs over time, based upon their unique experiences.

**Mutual Benefits**

MMRMA values the relationships with its 400-plus members. Each is significant to the long-term success of both the member and MMRMA, which is always focused on how members benefit from their affiliation with MMRMA.

MMRMA exists to assist members in meeting their risk management, risk financing, and loss control needs. Each member best understands its internal capabilities and appetite for various levels of financial risk related to property and liability claims.

**When its annual claims and liability costs rose above $1 million, the county took decisive action.**

MMRMA’s Regional Risk Managers also help members understand what model and level of risk are most appropriate, given their past claims and loss experience.

Taking those considerations into account, MMRMA members have varied self-insured retention (SIR) levels. They range from a $50,000 shared SIR among State Pool members to Individual members who retain higher SIR options up to $1 million.

SIR works very much like the deductible on your home or auto insurance. The higher the deductible, the greater the risk you take on.

**One County’s Experience**

To illustrate the responsiveness of MMRMA, I’ll share Monroe County’s story.

We began our journey with MMRMA in 1985 as an Individual member with a $75,000 SIR.

Since those early days of municipal pooling, larger SIR amounts have become more commonplace, as public entities have developed quality risk management programs and understand more fully the value of self-insured risk. But 33 years ago, a large SIR would have posed a huge risk for Monroe County.

We used MMRMA’s expertise to help change our culture and took practical steps to reduce our risk. MMRMA hosted a series of meetings with Monroe County leadership to convey the importance of better risk management in every department.

We knew we had to change the equation and our culture to compel more employee accountability.

**Partners in Risk**

First, we opted to take on a higher SIR, putting more of our own money at stake to create bigger consequences from our own actions. While at first glance that might seem risky, we knew a concerted effort could ultimately pay off, justifying our move to a SIR of $300,000.

When its annual claims and liability costs rose above $1 million, the county took decisive action.

**One County’s Experience**

To illustrate the responsiveness of MMRMA, I’ll share Monroe County’s story. We began our journey with MMRMA in 1985 as an Individual member with a $75,000 SIR.

Since those early days of municipal pooling, larger SIR amounts have become more commonplace, as public entities have developed quality risk management programs and understand more fully the value of self-insured risk. But 33 years ago, a large SIR would have posed a huge risk for Monroe County.

We used MMRMA’s expertise to help change our culture and took practical steps to reduce our risk. MMRMA hosted a series of meetings with Monroe County leadership to convey the importance of better risk management in every department.

We knew we had to change the equation and our culture to compel more employee accountability.

**Partners in Risk**

First, we opted to take on a higher SIR, putting more of our own money at stake to create bigger consequences from our own actions. While at first glance that might seem risky, we knew a concerted effort could ultimately pay off, justifying our move to a SIR of $300,000.

We used MMRMA’s expertise to help change our culture and took practical steps to reduce our risk. MMRMA hosted a series of meetings with Monroe County leadership to convey the importance of better risk management in every department.

**Partners in Risk**

First, we opted to take on a higher SIR, putting more of our own money at stake to create bigger consequences from our own actions. While at first glance that might seem risky, we knew a concerted effort could ultimately pay off, justifying our move to a SIR of $300,000.

We used MMRMA’s expertise to help change our culture and took practical steps to reduce our risk. MMRMA hosted a series of meetings with Monroe County leadership to convey the importance of better risk management in every department.

We knew we had to change the equation and our culture to compel more employee accountability.
Managing Cyber Security Threats in Public Spaces

by Cindy C. King, Director of Membership Services & Human Resources

NOW MORE THAN EVER, MMRMA members feel the need to protect electronic data from potential threats. Many of you employ knowledgeable information services and technology personnel inside your organizations.

You use the latest firewalls and other programs designed to protect systems and data from hackers. Employees are trained to be cautious when opening email attachments and to choose sophisticated passwords. Meanwhile, policies exist to govern who has access to which data.

But what about the risks when we connect our devices to the networks of other organizations? What happens when an employee is working remotely, traveling, or accessing work systems via Wi-Fi at the local coffee shop?

Travel Trouble
A July 19, 2018 article on the Tech Republic website identified several U.S. airports as having Wi-Fi network risks that could expose travelers’ devices—cell phones, tablets, or laptops—to cyberattacks. Unfortunately for Michigan travelers, Detroit Metropolitan Airport was named one the ten most susceptible airports. Others on the “top 10” list include Newark, NJ, Charlotte, NC, and Fort Myers, FL.

As Alison DeNisco Rayome writes on Tech Republic: “It’s much easier for attackers to access and exploit data from devices connected to airport Wi-Fi. … Hackers can use the poor cyber hygiene and insecure Wi-Fi at many airports to inject advanced network vulnerabilities like captive portals, Evil Twins, ARP poisoning, VPN gaps, honeypots, and compromised routers.”

The article adds that any of these methods could allow an attacker to access credentials for Microsoft Office 365, Dropbox, or other software programs. Culprits could also gain access to cloud apps or deliver malware to devices. Hacking one employee’s laptop could give an attacker access to your entire organization’s electronic database.

Safety Suggestions
Tech Republic’s advice to travelers: avoid using public USB charging stations and connect only to trusted Virtual Private Networks (VPNs). Other tips include turning off Wi-Fi and Bluetooth connectivity, encrypting laptops and other devices, and using cloud-based products with strong security measures.

One employee’s hacked laptop could pose a threat to your entire organization’s electronic assets.

Tech Republic encourages employers to implement a policy governing remote access to their data and systems, limiting those who can access employer resources while offsite. For instance, a city could prohibit an employee whose position primarily involves face-to-face interaction—such as a cashier or building inspector—from accessing the city’s electronic files remotely or while on vacation.

A policy could also require all connectivity to the employer’s systems and data to occur through secure VPNs rather than public networks, and only through devices provided by the employer. Minimally, a policy should require strong, sophisticated passwords, prohibit sharing login credentials and passwords with others, and require all devices to be equipped with the latest anti-malware software.

Costs Go Beyond Dollars
Various cyber experts predict that the economic impact to public entities that become the victims of cyber breaches will exceed $20 billion over the next several years.

MMRMA offers comprehensive Data Breach Coverage with a limit of $5 million per occurrence, and the included coverage was updated this year (see page 3 for details).

Coverage is important, but even with it, breaches can disrupt operations, compromise an entity’s reputation, and drain time that could otherwise be spent serving constituents. A sound risk avoidance plan requires ongoing diligence to stay abreast of ever-evolving cyber threats.

Source: Alison DeNisco Rayome, “The 10 airports where your phone is most likely to get hacked” www.techrepublic.com
Updated Data Breach Coverage Reflects Evolving Risks

by Michael Rhyner
Executive Director

AS OUR MEMBERS RELY MORE on electronic technology to handle information, unauthorized access or unintended release of such information can pose the risk of a significant loss.

The primary exposures relate to unauthorized release or breach of confidential data, personal information, and protected health care information. In addition, organizations may be subject to regulatory fines and penalties for certain data breaches.

The Board of Directors initially revised the MMRMA Coverage Document to add Data Breach Coverage for all members effective July 1, 2013. Each member is currently provided coverage of up to $5 million per occurrence at no additional cost to Individual and State Pool Members.

Original Coverages Remain in Effect
MMRMA’s Data Breach Coverage continues to include:

**Data Breach and Privacy Liability.** Protects against third-party losses resulting from unauthorized or potential unauthorized access to their electronic communications systems.

**Network Security Loss.** Reimburses members for damages to their electronic communications systems as a result of unauthorized or potential unauthorized access to those systems. Coverage is also provided for business interruption while systems are being repaired and restored.

**Breach Mitigation Expense.** Provides for losses resulting from unintentional data compromise. Coverage reimburses members for the cost of:
1. Public relations professionals
2. Notifications to comply with security breach laws
3. Data security experts
4. Credit monitoring services.

Responding to Ever-Increasing Risks
Data breach is an ever-emerging exposure. Since we began offering this coverage, the insurance industry has updated risk assessments for data breach and cyber threats. The risks and potential damages are increasingly significant as methods used to compromise systems have become more sophisticated.

Earlier this year, we made numerous revisions to the Data Breach and Privacy Liability Coverage Documents, which include clarifying language as well as enhanced and expanded coverages based on evolving risk exposures.

The expanded coverage helps protect members that accept credit card payments and maintain credit card data.

**As the methods to compromise systems become increasingly sophisticated, the potential damages become more costly.**

**Media Injury Liability.** Protects from losses resulting from allegations of:
1. Libel, slander, defamation
2. Invasion of privacy
3. Infringement of copyright, trade name with respect to their electronic communication systems.

Claims are typically related to information disseminated on the member’s website.

**Network Security Loss.** Reimburses members for damages to their electronic communications systems as a result of unauthorized or potential unauthorized access to those systems. Coverage is also provided for business interruption while systems are being repaired and restored.

**Breach Mitigation Expense.** Provides for losses resulting from unintentional data compromise. Coverage reimburses members for the cost of:
1. Public relations professionals
2. Notifications to comply with security breach laws
3. Data security experts
4. Credit monitoring services.

**PCI Assessments.** Protects members that accept credit card payments and maintain associated credit card data. Members are reimbursed for:
1. Fraudulent charges
2. Replacement of credit/debit cards
3. Fines, fees, and penalties resulting from payment card data breach.

**Social Engineering Loss.** Reimburses members for:
1. Money, securities, bonds
2. Misdirection of funds in escrow or trust
3. Theft of funds from fraudulent or deceptive communications.

**Reward Coverage.** Reimburses members for rewards that lead to the arrest and conviction of cyber criminals.

continued on page 4
Partnering to Achieve Shared Value, continued from page 1

In addition, we recognized the need to work more closely with MMRMA loss control and claims staff. We put concentrated effort into problem areas in employment-related claims that were the source of the most significant litigation and losses.

Looking back, the payoffs are clear. The County has saved contribution dollars by taking on a larger SIR. We still have a SIR of $300,000, and this year’s total property/liability budget is $645,000 less than what we paid out in 2007 for all claims, legal, and contributions for that year’s activity.

The Benefit of Investing Net Asset Distributions
These positive results are also due, in part, to the benefit of MMRMA’s net asset distributions. Since the Net Asset Policy was implemented in 2006, Monroe County has deposited its entire distribution into its retention fund in each of the 11 years a distribution was declared.

As a result, the fund currently holds five full SIR limits as well as additional funds for paying legal and claims expenses.

Key Takeaways
Through our partnership with MMRMA, we have learned the value of:

> Communicating sound, consistent loss control practices across all departments.

> Informing all stakeholders of our organization’s stake in our selected SIR limits.

> Contacting MMRMA loss control staff whenever additional resources are needed.

> Understanding causes of claims and litigation, when they arise, to handle incidents properly and prevent future iterations.

> Debriefing with defense attorneys after the conclusion of litigated claims to recognize what went right and learn from any mistakes to avoid their recurrence.

Monroe County has increased investment in its retention fund and reduced its annual budget for property and liability expenses.

Despite members’ best efforts, adverse events over which we have limited control may occur. When they do, we must work to mitigate the exposure as best we can.

Fortunately, MMRMA has the expertise and financial strength to address situations swiftly and appropriately. If an unfortunate loss should happen, every MMRMA member can rest easy, knowing we are supported by the strongest public entity risk pool in Michigan.

Updated Data Breach Coverage, continued from page 3

Telecommunications and Fraud. Reimburses members for fraudulent charges resulting from unauthorized or fraudulent access to outgoing telephone service.

MMRMA’s coverage protects against network security breaches such as hackers posting offensive material on a member’s official website.

This article provides an overview for informational purposes. Each type of coverage summarized here has specific reporting requirements, limits, deductibles, definitions, and exclusions. Members should refer to the MMRMA Data Breach and Privacy Liability Coverage Document for detailed descriptions of coverage, terms, and conditions.