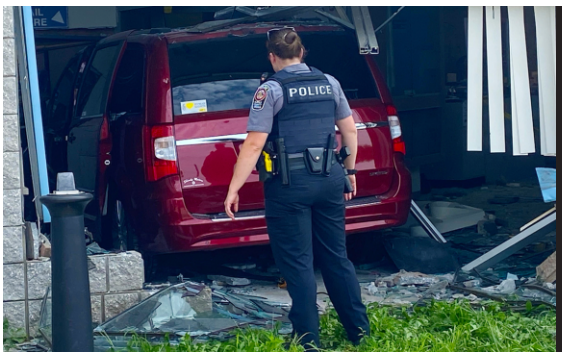
RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS AUGUST 2026

Bollards Are Not All the Same: Lessons from Vehicle Intrusions

by Phil Kamm, Senior Risk Control Consultant



Vehicle intrusions can cause substantial property damage, disrupt operations, and result in serious injuries or fatalities.

ON JANUARY 23, 2026, a Mercedes sedan breached the entrance of Detroit Metropolitan Airport, penetrating the terminal's glass façade and entering the building. Six individuals were treated for injuries. Photographs and witness accounts indicated that the vehicle overcame several bollards before reaching the structure.

Michigan incidents raise concerns

In its post-incident review, the Wayne County Airport Authority concluded that the bollards did NOT fail. Rather, they performed as designed—to separate pedestrian traffic from vehicle traffic. The Authority determined that the existing barrier system was not intended to stop an impact from an accelerating vehicle. Although defensive measures were present, they were inadequate to prevent the car's penetration into the terminal.

A second Michigan incident further illustrates the complexities associated with vehicle intrusion protection. On March 12, 2026, an armed assailant drove a truck into Temple Israel in the Township of West Bloomfield, breaching the building and entering an interior hallway before being stopped by security.

Effective protection requires evaluating both barrier performance ratings and overall site design.

Published reports indicate that the attacker's vehicle maneuvered around the bollards before reaching the building and crashing through the front entrance.

No children or staff members at the synagogue's early childhood center were injured, although a security officer was struck by the vehicle while responding to the attack. The FBI subsequently characterized the event as a targeted act of violence against the Jewish community.

Unlike the airport incident, where questions arose about whether the existing barriers were designed to stop a moving vehicle, the Temple Israel attack demonstrates another critical consideration: bollards can only provide protection when they are properly positioned and arranged to prevent vehicle bypass.

Vehicle incidents can be catastrophic

Together, these incidents highlight two distinct but equally important vehicle intrusion hazards. First, barriers may not offer sufficient crash resistance to stop the threat. Second, even highly capable barriers may provide limited protection if gaps or site configurations allow vehicles to circumvent the protective perimeter. Effective vehicle intrusion protection requires evaluating both barrier performance ratings and overall site design.

While vehicle intrusion incidents remain relatively infrequent, they do present a significant and often underestimated risk to public facilities. Whether caused by driver error, medical emergencies, impaired operation, mental health crises, or intentional acts, intrusions can cause substantial property damage, disrupt operations, and result in serious injuries or fatalities.

continued on page 3

CYBER RISK MANAGEMENT, PART 2

AI Governance: Managing Risks and Realizing Benefits

by Dan Bourdeau, Director of IT and Cybersecurity, and Tamara Christie, Communications Manager

The goal of sound risk management is not to prohibit AI use but to support its responsible implementation.

IT'S NEARLY IMPOSSIBLE to go a day without reading about the pros and cons of Artificial Intelligence (AI). Beyond the headlines, AI is quickly becoming part of daily work across all sectors, including public entities.

Generative AI can draft correspondence, summarize documents, analyze information, and create content, and AI capabilities are increasingly embedded in software organizations already use.

AI governance guidelines

For MMRMA members, the question is no longer simply whether employees will encounter AI but how the organization will govern its use.

Our resource, *Benefits of AI Governance for Government Entities,* gives an example of "a structured approach to managing the deployment, use, and oversight" of AI technologies. Effective governance can help public entities address risks such as bias, data privacy, and security while promoting accountability.

Governance is not intended to prohibit useful technology but rather to support its responsible application. The

AI governance is a leadership responsibility—not solely an IT function.

aim is to align AI usage with public service goals while allowing automation and data analysis to improve efficiency.

Start with policy guardrails

The challenge for members is to ensure appropriate guardrails around AI use. Our experts developed an *AI Governance Model Policy,* which provides a framework for doing just that while complying with the National Institute of Standards and Technology (NIST) AI Risk Management Framework, NIST Cybersecurity Framework 2.0, and Center for Internet Security (CIS) Critical Security Controls.

A key principle of the document is that "AI governance is a leadership and governance responsibility—not solely an IT function."

Depending on each member's needs, leadership, legal counsel, human resources, records management, department heads and others may have roles in determining how AI is authorized and managed.

The model policy classifies AI uses as Minimal, Limited, High, or Unacceptable. For example, using AI to draft communications is deemed a limited risk as long as an employee reviews and makes final content decisions. When AI is deployed in ways that could affect public safety, finances, access to services, and individual rights, it is imperative to apply greater scrutiny to its use and output.

Keep humans in the process

Generative AI poses the potential for inaccuracy. Because AI systems can produce "fabricated facts, citations, statistics, or legal references," the model policy requires independent verification of factual claims and human review of all AI-generated public-facing content.

Sensitive information requires similar caution. The model policy prohibits employees from entering personally identifiable information (PII), protected health or criminal justice information, privileged communications, and other confidential data into public or third-party generative AI tools unless appropriate authorization and protections are in place.

Risk management is ongoing

AI governance, like all areas of risk mitigation, is not a one-time exercise. It requires training, monitoring, risk assessment, and periodic policy review. We encourage members to regularly evaluate "organizational needs and address them through sound policies to govern AI and other technology-related tools and activities."

Our policy is not one-size-fits-all, so we urge each member to adapt it for their circumstances and have legal counsel review it before implementation.

Vehicle Intrusions, continued from page 1

Public entity facilities are often directly adjacent to vehicle traffic, creating exposures that extend beyond traditional property damage concerns to include occupant safety, operational continuity, and liability exposure. As a result, vehicle intrusion protection should be viewed as an important component of an organization's overall risk management and physical security strategy.

Bollards vary in intent

Bollards are designed for a variety of purposes, and their ability to withstand an impact varies considerably. As organizations evaluate physical security measures and public safety risks, it is important to know that not all barriers provide the same level of performance. Don't assume that any bollard installed adjacent to a building entrance can stop a moving vehicle.

Historically, bollards installed at courthouses, community mental health facilities, libraries, and other municipal buildings were intended to guide traffic, discourage unauthorized parking, or to protect pedestrians from low-speed vehicle movements. These decorative or traffic-control bollards may appear substantial, but they are often not engineered to resist high-energy impacts.

By contrast, crash-rated bollards are specifically designed, engineered, and tested to mitigate vehicle intrusion. These systems typically incorporate heavy-gauge steel, reinforced concrete foundations, and deep embedment below grade. Depending on the design, individual bollards may be interconnected beneath the surface to absorb impact forces throughout the system.

Most importantly, crash-rated bollards are subjected to formal performance testing under recognized standards such as ASTM F2656, Department of State (DOS) K-ratings, and the International Workshop Agreement (IWA) 14-1 standard. These tests evaluate a barrier's ability to stop vehicles of specified weights traveling at defined speeds. For example, an ASTM M30/P1-rating indicates that a barrier will stop a 15,000-pound truck traveling at 30 miles per hour while limiting penetration beyond the barrier to less than 3.3 feet.

Looking beneath the surface

One challenge for facility managers and risk professionals is that decorative and crash-rated bollards often appear nearly identical above ground. Manufacturers frequently incorporate aesthetically appealing architectural sleeves and finishes that conceal the underlying structural components. Visual inspection alone is insufficient to determine whether a bollard system can provide meaningful vehicle-impact protection. Accordingly, public entities should periodically evaluate vehicle intrusion exposures as part of their overall security, safety, and loss control programs, particularly at facilities with high public occupancy, vulnerable populations, or direct vehicle access near building entrances.

These steel bollards are placed close together to protect the building's lower-level glass entry doors from vehicle intrusion.

Facilities that serve children, older adults, people with disabilities, and/or those experiencing behavioral health crises may warrant additional consideration when evaluating vehicle intrusion risks. Understanding the purpose, design, and tested performance of existing barrier systems is critical to determining whether current protections align with site-specific risks.

When evaluating the best security methods, consider:

> Vehicle approach paths and available acceleration distances

> Adjacent roadway configurations and operating speeds

> Potential bypass routes around existing barriers

> Pedestrian traffic patterns and occupancy levels

> Vulnerable populations and special-use areas

> Building construction and setback distances

> Critical assets located near building entrances

> The design and performance characteristics of existing barrier systems

Effective risk management requires more than visible security measures; it requires verification that protective systems can perform as intended when needed most. The question is not whether bollards are present at a facility, but whether those bollards have been engineered, tested, and installed to stop the targeted threat that may ultimately occur.

Members are encouraged to contact MMRMA's Membership Services team with questions about this and other risk control topics.

RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

MMRMA Increases Property and Cybersecurity Coverage

Every August since 1995, the Woodward Dream Cruise has celebrated classic car culture. The world's largest one-day cruise attracts more than a million spectators to view over 40,000 vintage vehicles from across the globe. Owners caravan from far and wide to cruise the 15-mile stretch from Ferndale to Pontiac.

The *Risk Journal* is edited by Tamara Christie, Communications Manager (tchristie@mmrma.org), and published six times a year for members of Michigan Municipal Risk Management Authority.

Please note that the *Risk Journal* may include AI-assisted content. The authors and editor thoroughly reviewed and vetted all such material.

by Lorraine Zurenko, Underwriting Manager

MMRMA IS PLEASED TO announce increases in Property and Data Breach/Cybersecurity coverage limits.

MMRMA completed reinsurance renewals for Property and Data Breach/Cybersecurity coverage, which both went into effect on July 1, 2026. Executive Director Bryan Anderson and our underwriting team worked with reinsurance broker Guy Carpenter and our reinsurance partners on the renewal terms.

The following increased limits apply to both MMRMA and MCCRMA members.

Property/Crime Document

The All-Member Occurrence Limit increased to $500 million per occurrence, up from $350 million per occurrence in the previous coverage year.

Data Breach and Privacy Liability Document

The per member limit increased to $2.5 million per occurrence, with a $2.5 million per member annual aggregate, an increase from the prior year limits of $2 million per occurrence and $2 million annual aggregate.

The limit for F–Social Engineering coverage increased from $100,000 per occurrence/$100,000 annual aggregate to $250,000 per occurrence/$250,000 annual aggregate.

The increased coverages went into effect on July 1, 2026.

NOTE: These changes apply only to coverage written or renewed effective July 1, 2026 or thereafter. For example, members that renewed effective June 1, 2026, would retain the $2 million limit until their June 1, 2027 renewal.

MMRMA's team is working to update the Coverage Overview. Members who have already renewed coverage effective July 1, 2026 or later will not receive another Coverage Overview.

Ongoing review and update

MMRMA first began offering data breach and privacy liability coverage in 2013 at no added cost. The specific terms and limits have varied since inception, based on reinsurance market conditions and the rapid and often unpredictable nature of cyber risk activity and exposures.

An internal working group meets several times each year to review MMRMA's Coverage Documents and evaluate potential enhancements to benefit our membership.

Each year, the Executive Director and Underwriting team collaborate with MMRMA's actuarial business partners and reinsurance broker to coordinate reinsurance coverage for all areas. MMRMA's reinsurance structure is layered and includes members' self-insured retentions, MMRMA's own layer, and several reinsurance partners.

Reinsurance flexibility

MMRMA formed Greenstone Insurance Company, LLC, its wholly owned captive, in 2016 to offer additional services and coverage for members, including tax collection bonds.

Greenstone is also a participating reinsurer in MMRMA's casualty liability and data breach programs. This affords MMRMA more flexibility in its reinsurance structure, and any profits associated with Greenstone flow back to MMRMA as the sole captive owner.