1991 - 2026

IPARKS
Illinois Parks Association Risk Services

IPARKS QUARTERLY

SUMMER 2026

MEMBER RESOURCES & RISK READINESS

Park districts across Illinois face a wide range of operational, technology, and risk management challenges. This issue of IPARKS Quarterly highlights practical resources, emerging trends, and member benefits designed to help organizations strengthen operations, address evolving risks, and support informed decision-making.

Inside, you'll find information on a new youth employment resource available through the Resource eLibrary, the evolving cyber threat landscape, AI readiness resources, claim reporting tools, grant opportunities, and safety guidance for outdoor operations. Each article is intended to provide practical information and helpful resources that members can use to support effective operations and proactive risk management efforts.

IN THIS ISSUE:

SHARE YOUR STORY WITH IPARKS

Help us tell the story of Illinois parks, recreation programs, facilities, and the communities you serve. Selected photos may be featured in future IPARKS newsletters, calendars, websites, and other member communications.

We're Looking For:

- Community events and recreation programs
- Parks, preserves, trails, and natural areas
- Playgrounds, athletic facilities, pools, and amenities
- Staff in action and behind-the-scenes operations
- New projects, improvements, partnerships, and accomplishments
- Seasonal photos from throughout the year

Submission Tips

Include your agency name, location or event name, and a brief description. High-resolution, well-lit photos are preferred, especially horizontal images suitable for newsletters and website banners. All photos should be approved for external/public use before submission.

REMINDER

Submit by October 9, 2026

Email: iparks@iparks.org

Text: (518) 258-3686

After submission, an IPARKS representative will provide any required photo release information.

RESOURCE SPOTLIGHT: YOUTH EMPLOYMENT AND EQUIPMENT USE

By Chanelle Fagbemi, Del Galdo Law Group, LLC

Park districts often rely on young employees to support recreation programs, facilities, concessions, and seasonal operations throughout the year. Understanding child labor laws remains important for park districts that employ workers under the age of sixteen.

The Illinois Child Labor Law (820 ILCS 206/) regulates the employment of minors under the age of sixteen by limiting work hours and prohibiting work in hazardous occupations. Under the statute, no employer can permit a minor to work more than eighteen hours during a school week or more than forty hours during a non-school week. Generally, minors may not work before 7:00 a.m. or after 7:00 p.m. when school is in session. However, from June 1 through Labor Day, children may work up until 9:00 p.m. This extended time can apply even during a school week if certain conditions are met. These conditions include ensuring that the minor does not work beyond three hours daily and no more than two school days each week. Otherwise, minors are strictly prohibited from working beyond eight hours in any single twenty-four-hour period.

Children under sixteen are broadly able to work in nonhazardous industries. As relevant here, nonhazardous work may include working as an officiant or assistant instructor of youth sports activities for a park district if the minor is aged twelve or older. As for the types of work minors under sixteen may not perform, it should come as no surprise that no minor can serve alcohol or sell tobacco. Beyond this, the law generally prohibits children from working in hazardous occupations or environments. This limitation may include operating heavy machinery or power-driven equipment, using deep fryers or cooking equipment involving hot oil, meatpacking, performing construction work, and handling or applying harmful chemicals. Put simply, a child under sixteen may be responsible for leading recreational activities, and even refereeing a heated game of kickball, but not for operating machinery, like mowers and trimmers, used to maintain the park.

To ensure legal compliance, park districts and recreation programs should consider employing children for age-appropriate roles, such as camp counselors, front desk attendants, or concessions staff. Employers should also ensure that children under sixteen obtain work permits and are scheduled strictly within the hours permitted by law. Lastly, maintaining consistent and open communication with children and their guardians can help address concerns promptly and establish a safe and supportive work environment. By following these practices, park districts can meet their legal obligations while fostering valuable employment opportunities for young workers.

Looking for more detail? The complete Age-Based Guidelines for Equipment and Vehicle Use are available in the Resource eLibrary. Visit IPARKS.org > Member Benefits > Resource eLibrary for the full guide.

RESOURCE SPOTLIGHT: YOUTH EMPLOYMENT AND EQUIPMENT USE *(CONTINUED)*

AGE-BASED GUIDELINES FOR EQUIPMENT AND VEHICLE USE

AGE GROUP	ALLOWED	NOT ALLOWED / RESTRICTIONS
Ages 14-15	✅ Hand tools - manual tasks only	❌ Power equipment - mowers, trimmers, etc. ❌ Golf carts ❌ Utility vehicles - Gators, UTVs, side-by-sides ❌ Automobiles and trucks
Age 16	✅ Mowers - push and typically riding ✅ Trimmers, blowers, and edgers ⚠️ Limited use of golf carts, utility vehicles, ATVs, and on-site vehicles based on agency policy and training	❌ Skid steers, forklifts, and heavy equipment ❌ No driving automobiles or trucks on public roads for work purposes
Age 17	✅ Mowers - push and typically riding ✅ Trimmers, blowers, and edgers ✅ Golf carts on park property ✅ Utility vehicles - on property with training ✅ ATVs/off-road vehicles - with applicable supervision ✅ On-site vehicle use - with policy controls	❌ Skid steers, forklifts, and heavy equipment ⚠️ Public road vehicle use is limited. Certain 17-year-olds may drive automobiles or trucks under 6,000 lbs. Gross Vehicle Weight (GVW) for limited work purposes if specific legal requirements are met.
Ages 18+	✅ All equipment ✅ All park vehicles ✅ Automobiles and fleet vehicles - licensed drivers	None, subject to agency policies and required licensing/training

2026 CYBER THREAT LANDSCAPE

RANSOMWARE, SOCIAL ENGINEERING, & AI-ENABLED THREATS

By CRC Group

Ransomware and social engineering attacks have long been among the most disruptive and costly events that an organization can experience, but recent developments are accelerating their scale and effectiveness. The sophistication and accessibility of threat tactics have continuously increased in recent years, and artificial intelligence is now accelerating and reshaping these attacks, creating new challenges for organizations.

Why this matters for IPARKS members

Illinois park districts, conservancy agencies, and forest preserves often rely on a mix of public-facing services and vendor-supported systems (e.g., registrations and reservations, point-of-sale, finance/payroll, email and file sharing, and facility/security technology). That combination can make cyber incidents especially disruptive—impacting community services, staff operations, and public trust—while creating time-sensitive decisions around containment, continuity of operations, and notification obligations.

- Registrations/reservations, program management, or POS outages during peak periods
- Compromised email accounts used to redirect vendor payments (business email compromise)
- Exposure of HR, payroll, or patron data through stolen credentials or third-party access
- Disruption to facility systems (access control, cameras, or building management) where present

Ransomware Trends

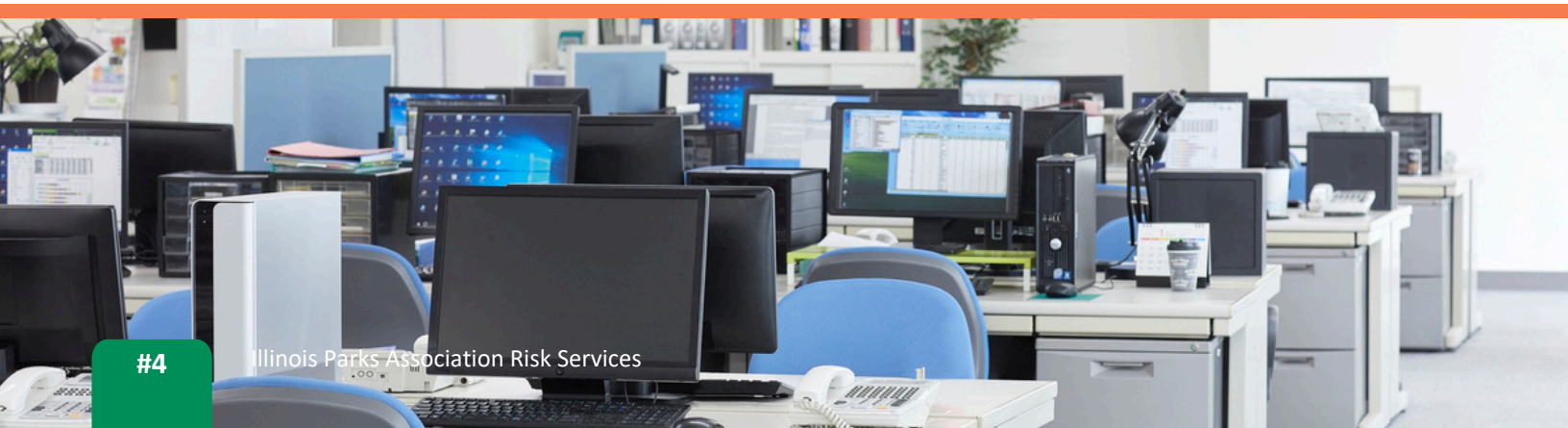
Ransomware attacks have evolved from broad, opportunistic campaigns into targeted, complex intrusions. Modern ransomware groups often conduct reconnaissance and exploit multiple entry points. The barrier to entry has also dropped due to ransomware-as-a-service (RaaS) models, where threat actors can purchase ready-made attack kits. As a result, the frequency of ransomware incidents continued to rise, with FBI Internet Crime Complaint Center (IC3) reporting an increase in ransomware complaints between 2023 and 2025.

Artificial intelligence is significantly contributing to these trends. Attackers are using AI to automate vulnerability discovery, generate malware that can evade detection, and optimize attack paths within networks. AI tools can also craft convincing phishing lures to gain initial access, as well as dynamically adjust ransomware behavior in response to defensive measures.

Social Engineering and Business Email Compromise

Social engineering and business email compromise (BEC) remain among the most common cyber threats. These attacks exploit human trust to trick employees into transferring funds or divulging sensitive information. BEC schemes, in particular, have proven resilient because they rely on relatively simple impersonation tactics rather than complex malware.

AI tools are significantly increasing the effectiveness of these attacks by enabling easily deployable, convincing emails targeting specific individuals and eliminating many of the red flags that users have been trained to spot. Attackers use AI to analyze publicly available data to craft personalized messages. In advanced cases, AI-generated voice cloning and deepfake technology are being used to impersonate individuals in real-time, adding a new layer of credibility to fraudulent requests



2026 CYBER THREAT LANDSCAPE *(CONTINUED)*

RANSOMWARE, SOCIAL ENGINEERING, & AI-ENABLED THREATS

How to Prepare Your Organization

Ransomware is becoming more adaptive and easier to deploy, while social engineering is becoming harder to detect. Organizations must respond by strengthening both technical defenses and human awareness.

While social engineering incidents inherently involve the deception of individuals, Verizon's Data Breach Investigations Report (DBIR) has consistently found that a human element is present in a majority of breaches. Employee training is a fundamental element of any effective cybersecurity program, and it is essential to execute ongoing training to ensure employees are aware of increasingly sophisticated and convincing tactics.

From a technical perspective, key controls continue to include multi-factor authentication (for remote network access, email, and privileged accounts), endpoint detection and response (EDR), secure backups, prompt patching, and incident response planning. Two other recommended controls that are often underemphasized are data asset inventorying/management and managed detection and response (MDR) as an enhancement to EDR. The former is fundamental to ensuring that all attack vectors are known and managed, and the latter adds prompt visibility and response to threats detected by EDR solutions.

PRACTICAL BASELINE CHECKLIST FOR IPARKS MEMBERS

- **Protect email and remote access**: multi-factor authentication for all users; extra protections for admins and finance; disable legacy authentication.
- **Harden backups:** maintain offline/immutable backups; test restores at least quarterly; document what "critical operations" must be restored first (payroll, registrations, POS, etc.).
- **Patch with priority:** focus on internet-facing systems (VPN, firewalls, remote management tools) and known-exploited vulnerabilities (e.g., CISA KEV Catalog).
- **Reduce BEC risk**: require call-back verification for payment changes/wires/ACH; implement dual approval for high-risk transactions; train staff on AI-enabled impersonation.
- **Know your vendors and data:** maintain an inventory of systems and where sensitive data lives; document vendor access paths and offboarding; ensure contracts include incident notification expectations.
- **Detection and response:** ensure EDR is deployed across endpoints/servers; consider MDR if internal monitoring is limited; keep an after-hours escalation process.

Lastly, incident response plans should include pre-identified points of contact for your IT leadership/managed service provider, cyber insurance carrier, outside counsel (if used), and an incident response/forensics firm. In the event of a suspected incident, engage those resources early to support containment, evidence preservation, communications, and recovery decisions. For Illinois entities, notification requirements and timelines can vary based on the type of data involved and the circumstances of the incident, so legal guidance is important to help determine applicable obligations and coordinate any required notifications (see, generally, 815 ILCS 530/10).

References

Federal Bureau of Investigation. (2026). Internet Crime Report (IC3). (Referenced for ransomware complaint trends.)
Verizon. (2025). Data Breach Investigations Report (DBIR). (Referenced for human element in breaches.)

NEED ADDITIONAL CYBER PROTECTION?

As cyber risks become more sophisticated, some organizations may benefit from increased cyber insurance limits. Members may increase their limits of cyber insurance. If interested, please reach out to your IPARKS Service Team at (800) 748-0554.

RESOURCE ELIBRARY UPDATE

A NEW COLLECTION OF AI READINESS TOOLS, GUIDANCE, AND SECURITY RESOURCES ARE NOW AVAILABLE WITHIN THE CYBER PORTAL!

https://apeepelibrary.com

support@apeepelibrary.com

We've expanded our Cyber Portal with a new suite of AI readiness tools designed to help organizations confidently and securely adopt artificial intelligence. These resources include practical guidance on AI governance and risk management, security assessment checklists, customizable policy templates, educational materials, and ongoing insights into emerging AI driven threats and trends.

These new AI resources were developed to help members strengthen their security posture while confidently leveraging the benefits of artificial intelligence.

We remain committed to equipping you with the tools and knowledge needed to stay ahead in an increasingly complex threat environment.

To access the new AI readiness resources:

1. Go to the Resource eLibrary website.
2. Sign in with your member credentials. Note: If you have not registered, please do so by selecting Login/Register at the top of the page. If you are having trouble logging in, please email support@apeepelibrary.com.
3. Navigate to the Cyber Portal.
4. Where you'll land on the AI Readiness Resources section.

Be sure to check out the Knowledge Center and Training and News sections!

DON'T FORGET YOUR IPARKS GRANT OPPORTUNITIES

APPLICATIONS DUE OCTOBER 31, 2026

The IPARKS Power Grant, Aquatics Grant, and Fall Prevention Repair Program is currently taking applications. If you haven't applied yet, there is still time to take advantage of these valuable member benefits.

IPARKS POWER GRANT
Flexible funding to support equipment upgrades, safety tools, and training resources.
Annual awards:
- $500
- $1,000
- $1,500

Based on member contribution levels.

AQUATICS GRANT
Up to $500 annually for approved aquatic training and auditing services through:
- Jeff Ellis & Associates
- Starfish Aquatics Institute
- American Red Cross

Ideal for lifeguard training, safety audits, and pool-management education.

FALL PREVENTION REPAIR PROGRAM
Receive up to $350 in reimbursement for repairs that address slip and trip hazards, helping keep facilities safe and accessible.

READY TO APPLY?

VISIT **IPARKS.ORG** TO REVIEW ELIGIBILITY REQUIREMENTS AND APPLICATION DETAILS.

KNOW BEFORE YOU NEED IT

CLAIM REPORTING RESOURCES

Claims can happen when you least expect them, and knowing who to contact can make all the difference in ensuring a prompt response and efficient handling. The information below outlines the reporting procedures and key contacts for property, liability, auto, employment practices, cyber, and active assailant incidents.

Property, Liability, Auto, and Employment Practices Claim Reporting

Gallagher Bassett serves as the claims administrator for IPARKS and provides experienced claims management services for property, liability, auto, and employment practices claims.

When an accident or incident occurs, the member should report the claim as soon as possible. The preferred method of reporting a claim is through the online claims portal on the IPARKS website. There is a link to file a claim on the home page, or you may navigate to it by selecting Contact Us – File a Claim.

Prompt reporting allows for timely investigation and helps ensure the most effective claim handling process. Remember, reporting a claim is not an admission of liability—it simply initiates the review and investigation process.

What Should Be Reported?

Claims and incidents that should be promptly reported include, but are not limited to:

- Slip, trip, and fall incidents
- Injuries to members of the public
- Vehicle accidents involving park district vehicles
- Property damage involving third-party property
- Allegations of discrimination, harassment, or wrongful employment practices
- Incidents involving playgrounds, athletic facilities, aquatic facilities, or special events
- Damage to member-owned buildings, equipment, or other property
- Any incident that may reasonably result in a claim, even if no one has requested compensation and no legal action has been threatened

When in doubt, report the incident. Early reporting allows claims professionals to investigate while information is fresh, preserve evidence, and help protect the member's interests.

Cyber Incident Reporting

A fast response is critical when dealing with a cyber incident. Early notification allows legal and cybersecurity professionals to assess the situation, help contain potential damage, and guide members through the response process.

Examples of cyber incidents that should be reported for review include:

- Suspected or confirmed ransomware events or cyber extortion threats
- Business email compromise, phishing, or fraudulent payment requests
- Potential privacy breaches involving employee, patron, or other private information
- Unauthorized access to systems or networks
- System outages, interruptions, or degradation that may be related to a cyber event

If your organization experiences a cyber incident:

1. Contact IPARKS cyber legal specialist, McDonald Hopkins, immediately at **(855) 7-IPARKS** (855-747-2757).
2. After calling the Cyber Hotline, submit the claim through the IPARKS Cyber Claim Reporting Portal available on the IPARKS website.

Active Assailant Incident Reporting

In the event of a suspected active assailant incident, immediate reporting is essential to activate crisis management and emergency response resources.

Contact Markel's crisis management consultant, Security Exchange, immediately at: **(312) 500-5093**

Early notification provides access to crisis response professionals who can assist with emergency coordination, communication support, and claim management during a critical event.

Additional Contact Information

While your primary point of contact during the claims process will be the assigned adjuster, members may also contact the following Gallagher Bassett team members:

- Kari Gipson, Client Service Manager
  (414) 203-4069, kari_gipson@gbtpa.com
- Kanelle Estrada, Auto/General Liability Supervisor
  (717) 610-3937, kanelle_estrada@gbtpa.com
- Laura Cozzi-Deany, Auto/General Liability Supervisor
  (630) 285-3844, laura_cozzideany@gbtpa.com
- Melissa Nederhoff, Property Supervisor
  (248) 452-6040, melissa_nederhoff@gbtpa.com

IPARKS
Illinois Parks Association Risk Services

IPARKS Service Center
315 S. Kalamazoo Mall
Kalamazoo, MI 49007

If our mailing records need to be updated, please contact the IPARKS Service Center at (800) 748-0554.
IPARKS newsletters are available for viewing and printing at www.iparks.org.

NEW! EASY ONLINE CLAIM REPORTING

Need to report a claim? We've made it easier to access the IPARKS claim reporting portal. Simply scan the QR code below to quickly connect to the appropriate reporting resources and submit your claim online. Whether you're reporting a property, liability, auto, employment practices, or cyber-related incident, prompt reporting helps ensure timely investigation and effective claim handling.

Scan the QR Code Below to Get Started

IPARKS
Illinois Parks Association Risk Services

IAPD
Illinois Association of Park Districts

IPARKS is the risk management affinity partner of Illinois Association of Park Districts (IAPD), working to provide affordable, specialized coverage programs and valuable loss control resources for park districts, recreation and conservation districts, river conservancy districts, forest preserves and special recreation agencies.