JONAS
CLUB SOFTWARE

SECURITY & AI

Technology Governance **Plus**

A Board-Level Briefing for Private Clubs
Winter 2026 | Co-developed by
Jonas Club Software & Pulsar Security

Executive Abstract

Private clubs have entered into a new operating reality.

In 2026, clubs are no longer defined solely by facilities, amenities, or member services. They are **data-rich enterprises** responsible for safeguarding member identities, financial records, communications, operational systems, and increasingly, AI-enabled workflows. This shift has materially changed the club's risk profile — and with it, the responsibilities of executive leadership and boards.

Cybersecurity, data governance, and responsible use of artificial intelligence are no longer technical concerns delegated solely to IT staff or vendors. They are now **governance issues**, tied directly to fiduciary duty, insurance eligibility, regulatory exposure, and member trust.

Across industries such as healthcare, financial services, and hospitality, boards are responding by elevating technology oversight to the same level as financial controls and operational continuity. Private clubs are now expected to do the same.

This briefing is designed to help **General Managers, Boards, and Executive Committees** understand:

- **What has changed** in the technology and risk landscape affecting private clubs
- **Why these changes matter** to leadership, even without technical expertise
- **What a "reasonable standard of care" looks like in 2026**
- **What actions leaders should champion** to protect their clubs and their members

This document is not a product overview, not a fear-based assessment, and not a technical manual.

It is a **leadership guide** — intended to support informed decision-making, constructive boardroom dialogue, and practical next steps.

Clubs that proactively align technology, governance, and risk management will be better positioned to:

- Protect member trust and reputation
- Maintain insurability and financial stability
- Enable operational continuity and modernization
- Adopt new tools, including AI, responsibly and confidently

The goal is not perfection.
The goals are **clarity, accountability, and progress**.

Table of Contents

Executive Summary

The Evolving Security Landscape: Board Oversight in 2026

Board's Cybersecurity Oversight Checklist

Modernizing Infrastructure and Operational Continuity

AI Readiness and Ethical Use in Club Operations

Aligning Technology Solutions with Governance and Club Complexity

Calls to Action for Boards, GMs, and Committees

Final Thoughts

References

Executive Summary

Rising Cyber & Data Risks

In 2026, private clubs face a heightened cybersecurity threat landscape. Global cyberattacks jumped 44% year-over-year[1], and even exclusive clubs have been breached (e.g. a top San Francisco golf club had 10GB of member data stolen in 2025[2]). Boards have a fiduciary duty to ensure member data is protected, and critical systems are resilient. Independent security audits, compliance with proven frameworks, and proactive risk management are now baseline expectations at the board level.

AI Emerges as a Board Priority

The rapid adoption of Artificial Intelligence brings both opportunity and risk. Nearly half of Fortune 100 boards now explicitly oversee AI-related risks (up from 16% last year)[3]. Club boards should follow suit, establishing AI readiness and ethical use policies to govern how AI is deployed in club operations. This includes frameworks for responsible AI (transparency, privacy, bias mitigation) and clear guidelines so that tools like ChatGPT are used safely and in line with club values. As a recent report noted, *"trust in AI systems remains a significant challenge"* and many employees are using AI without proper controls[4][5]. Board oversight can ensure AI's benefits (efficiency, insights) are pursued while guarding against privacy or security pitfalls.

Modern Infrastructure & Continuity

Outdated, on-premises IT infrastructure is a liability in the modern era. Leading clubs are upgrading cloud-hosted systems and modern platforms to improve security, uptime, and scalability. For example, Jonas Club Software's guided cloud migrations typically finish in under two weeks with minimal downtime[6], allowing clubs to modernize with ease. Modern cloud hosting means automatic updates, regular data backups, and robust disaster recovery—critical for continuity during events like hurricanes or cyber incidents. This supplement contrasts the "traditional" vs "modern" technology posture (see Table 1) and urges clubs to meet new standards (e.g. secure Azure-based hosting, 24/7 system monitoring, mobile access) to support uninterrupted operations and member service.

Governance, Risk & Technology Alignment

Technology governance is now inseparable from overall club governance. Boards must ask management tough questions (see Board's Cybersecurity Oversight Checklist) about cybersecurity preparedness, data governance, vendor due diligence, and strategic IT roadmaps. This white paper provides functional checklists and conversation starters to guide board discussions with GMs, CIOs, and vendors. It also illustrates how Jonas Club Software's platform suite—Jonas Club Management (JCM), Jonas Encore, and Jonas Synergy—can each support governance and operational maturity appropriate to a club's complexity. Whether a club requires the comprehensive

capabilities of JCM/Encore or the simplified modern workflows of the new Synergy platform, technology choices should be aligned with the club's risk management and service goals.

Call to Action

Club boards and finance committees should audit their current technology posture and demand action plans for any gaps. In practical terms, this means commissioning independent cybersecurity assessments, adopting industry frameworks (for both data security and AI ethics), migrating off legacy systems that no longer meet security standards, and investing in staff training and policy development. Boards that champion technology oversight will reduce risk, protect member trust, and position their clubs for sustained success. As Pulsar Security's COO Katie Gusella emphasizes,

> *"Cybersecurity is a never-ending journey, and every organization is at its own unique place along the path… We remain focused on meeting clubs where they are on their journey and delivering targeted, world-class solutions at an affordable cost."[7] — Pulsar Security's COO, Katie Gusella*

The Evolving Security Landscape: Board Oversight in 2026

Cyber threats have escalated, and private clubs are no exception. High-profile breaches in hospitality and finance make headlines, but clubs house valuable data (member personal info, payment cards, staff records) that attract cybercriminals as well. In late 2025, the Qilin ransomware gang breached the California Golf Club of San Francisco, an elite members-only club, exfiltrating sensitive member lists, correspondence, and financial records[2][8]. This incident exposed wealthy members' personal details and even board meeting minutes, creating severe reputational and legal risks. It was a wake-up call: **if an exclusive century-old club can be hacked, any club can**.

Cybersecurity as a Top-Tier Governance Issue

Real-world data and cross-industry trends reinforce why boards must treat cybersecurity as a top-tier governance issue:

- **Soaring Attack Frequency & Costs:** Cyberattacks surged 44% globally year-over-year[1]. The average cost of a data breach in the U.S. hit an all-time high of $10.2 million in 2025[9]. Even smaller organizations suffer hefty damages from ransomware downtime, forensic investigations, member notifications, and lost trust. For example, casino operator MGM Resorts suffered a September 2023 attack that shut down operations (hotel door locks, slot machines, reservation systems) and is expected to cost ~$100 million in business losses[10][11]. While a local country club's scale is different, the relative impact of a cyber incident, like the days of canceled tee times, inaccessible member accounts, billing errors, etc., all contribute to a club's finances and reputation.
- **Regulatory and Insurance Pressures:** Clubs may not be directly regulated like banks, but the environment is tightening. Cyber insurers now demand rigorous security controls and audits before granting coverage[12]. In fact, many organizations struggle to even qualify for cyber insurance because they lack sufficient safeguards and documented practices[12]. Those that do get coverage face higher premiums unless they demonstrate ongoing risk reduction measures. Boards should view this as an impetus to improve by strengthening cybersecurity posture (policies, training, technology). Clubs not only reduce the chance of a breach but also maintain insurability[12]. Additionally, data privacy laws (from California's CPRA to Europe's GDPR) impose duties to protect personal information—clubs handling member data must be aware of and compliant with applicable standards to avoid legal liability.
- **Board Accountability:** In corporate America, board oversight of cyber risk has become the norm, and club boards are expected to follow suit. Nearly three-quarters (73%) of large companies now align their cybersecurity programs to frameworks like NIST or ISO 27001[13], up dramatically from just a few years ago. Furthermore, 58% of companies report conducting regular cyber incident simulations or tabletop drills for management and directors (up from a mere 3% in 2019)[13]. This trend toward structured governance is trickling all sectors. Simply put, a club's board should ensure that management isn't flying blind on cybersecurity. There should be a formal Cybersecurity Program in place, with metrics reported to the board, periodic independent reviews, and action plans for continuous improvement.

> *"Boards don't need to be cyber experts, but they absolutely need to ask the right questions." – Club IT Governance Consultant*

Independent Validation

One of the most effective steps a board can champion is independent third-party cybersecurity validation. This can take the form of vulnerability assessments, penetration testing, or full security audits performed by outside experts. A third party can "simulate real cyberattacks**"** on your club's network to find hidden weaknesses before criminals do[14]. These engagements yield candid reports on gaps and prioritized fixes. Consistently investing in penetration testing and external assessments allows clubs to quickly patch security holes and strengthen their defenses[15]. It also sends a powerful message that the club is serious about protecting its data. Boards should insist on seeing the results of such tests (in summary form) and hold management accountable for addressing the findings. In many industries, it's considered a best practice (and a board's expectation) to have at least annual independent security reviews – clubs

TECHNOLOGY GOVERNANCE **PLUS**

should be no different.

Security Maturity Tiers

Clubs vary in their cybersecurity maturity. Some smaller clubs may still be at a *"basic"* level; limited formal security practices, perhaps relying on a single IT generalist or an outside vendor for occasional support. Others have progressed to an *"intermediate"* level; they've implemented standard protections (firewalls, anti-malware, backups), staff security awareness training, and have some policies in place. The goal is to move toward an *"advanced"* or *"proactive"* posture characterized by regular third-party audits, continuous monitoring (e.g. managed detection and response), documented incident response plans, and alignment with recognized frameworks like NIST Cybersecurity Framework.

Table 1 later in this document contrasts elements of a traditional vs. modern IT posture, many of which correspond to higher security maturity. The board should ask management: *"Where do we fall on the security maturity spectrum, and what will it take to reach the next level?"* A key indicator of maturity is embracing external frameworks and expertise; for instance, 73% of leading companies map their security frameworks such as NIST CSF 2.0[13] – a practice that clubs can adapt at a scale appropriate to their size.

Finally, benchmark beyond our industry. Private clubs can learn from hospitality, fintech, and insurance peers: these sectors have pioneered risk management practices out of necessity. For example, major hotel chains perform regular network penetration tests and mandate PCI-DSS compliance scans for any system handling payments. Banks conduct phishing simulations to continually train employees to spot scams. Insurers apply enterprise risk management, quantifying cyber risks in financial terms, and treating them on par with other business risks. By seeking insights from these verticals, club boards can adopt proven strategies rather than reinventing the wheel. A club's culture might differ, but the fundamental challenges of securing data and systems safely are universal.

Board's Cybersecurity Oversight Checklist

Boards should incorporate cybersecurity into their regular agenda. Here are critical questions directors should be asking club management and IT providers:

1. **What are our top cyber risks, and how are we mitigating them?** – Expect management to identify the most sensitive data or systems (e.g. member credit card info, payroll systems, email accounts) and explain protections in place (encryption, multi-factor authentication, etc.). For each risk, there should be an associated control and a responsible owner.
2. **When was our last independent security assessment or penetration test?** What were the high-priority findings, and have they been remediated? Regular third-party tests[16] are crucial; if none have been done, insist on scheduling one. If one was done, the board should hear a summary of results and follow-up actions.
3. **Do we have an incident response plan and cyber insurance?** – Management should have a written plan for how to respond to a data breach or ransomware attack. Does it cover communication to members, isolating affected systems, legal steps, and recovery timelines? Has the team practiced this via tabletop exercise[17]? Also, confirm if the club carries cyber liability insurance, and if so, that policy requirements (like specific controls or breach of notifications) are being met.
4. **How are we protecting member data and privacy?** – Directors should understand how member and employee personal identifiable information (PII) is stored and secured. Is data encrypted at rest and in transit? Who has access to sensitive data, and is access limited by role (least privilege principle)? Are we purging data we no longer need (data retention policies)? If the club uses third-party software or cloud vendors, do contracts ensure those vendors follow strong security and privacy practices?
5. **What cybersecurity training do we provide for staff and management?** – Humans are often the weakest link. Phishing attacks can trick even seasoned employees. The board should hear that the club conducts regular security awareness training for all staff (including seasonal and part-time workers who handle systems). Training might cover how to spot phishing emails, use of strong passwords or passphrases, proper handling of confidential member info, and guidelines on using personal devices. A culture of security starts at the top: are senior executives modeling good practices? Consider also if the board itself might benefit from a briefing on cyber risks (perhaps via CMAA or NCA resources).
6. **Are our critical systems and backups resilient?** – Ask what the backup regimen is for key systems (e.g. Jonas Club Software databases, membership records, accounting). Are backups kept off-site or in the cloud to survive a physical disaster? Have we ever tested restoring from backup, and how long would it take? Also, what's our tolerance for downtime (hours, days?), and do we have arrangements to meet that (such as cloud failover or vendor support contracts)? In 2026, best practice is to have off-site, encrypted backups and a recovery time objective that aligns with the club's operational needs (for many, being down more than a day is unacceptable).
7. **How do we stay updated on emerging threats and update our defenses?** – Cyber threats evolve quickly (e.g. new ransomware strains, zero-day exploits, etc.). Management should be subscribing to threat intelligence (possibly via a security vendor or Pulsar Security's advisories) and have a patch management process to update software promptly. Boards can ask: *"Are all our servers and PCs getting security patches at least monthly? Do we promptly apply critical patches (e.g. zero-day fixes)?"* Delayed patching is a common cause of breaches.
8. **Have we identified an external cybersecurity partner?** – Even with skilled IT staff, clubs

TECHNOLOGY GOVERNANCE **PLUS**

may need outside help during a major incident or for specialized testing. Who would we call if we had a serious breach at 2 AM on a Sunday? It's wise to have a relationship (even retainer) with a cybersecurity firm (like Pulsar Security or similar) that understands our environment. Boards should encourage management to build this relationship *before* an incident occurs.

By asking these questions, directors set the expectation that technology risk is being managed deliberately. It also empowers GMs/IT leaders to take necessary actions and request budget support. Remember, cybersecurity is not just an "IT problem" – it's a governance priority. As Katie Gusella of Pulsar Security puts it, clubs must view security as an ongoing journey and meet each club "where they are" on that path[7]. The board's role is to guide the club further down that path toward stronger resilience and preparedness.

Modernizing Infrastructure and Operational Continuity

The foundation of a club's technology environment is its infrastructure – the software applications and the hardware or cloud systems they run on. If cybersecurity and AI are the new frontiers, infrastructure is the bedrock. Many clubs in 2025-2026 find themselves straddling two worlds: the *traditional* model of on-premises servers (often aging) and siloed systems, and the *modern* model of cloud-based platforms and integrated services. The board's oversight of technology should include ensuring that the club's IT infrastructure is reliable, secure, and can support the club's strategic goals (now and into the future).

Why Modernize?

Legacy systems and servers can pose hidden risks and costs: they may not receive regular security patches (opening vulnerabilities), could fail unexpectedly (with lengthy downtime), and often require expensive maintenance or lack of vendor support over time. Additionally, older infrastructure might limit a club's ability to implement new features or integrate with modern apps (e.g., a mobile booking app or advanced reporting tool might not work with a decades-old database). In contrast, modern infrastructure—especially cloud-hosted solutions—offers resilience, scalability, and managed security. For instance, a cloud-hosted club management system typically runs on secure, high-performance data center servers with continuous monitoring and backups by the provider[28]. This means the club benefits from enterprise-grade security (firewalls, intrusion detection, etc.) and regular updates/patches applied by experts[28], without burdening a small local IT team.

Consider the scenario of a local server at the club: if a tropical storm or fire hits the clubhouse, that server (and all data) could be destroyed. With a cloud solution, the data resides in professionally managed data centers (often with geographic redundancy), so a physical disaster at the club won't wipe out digital records – operations can continue from anywhere with internet. Operational continuity is a major benefit of modern hosting. In fact, many clubs experienced this during the COVID-19 pandemic: those with cloud-based systems could transition to remote work much faster (accessing club systems securely from home), whereas clubs on legacy systems struggled until VPNs or other workarounds were set up.

Hosting and Migration

A common concern among boards and GMs is the complexity or downtime involved in moving to new systems or cloud environments. The good news is that vendors like Jonas Club Software have refined the migration process significantly. Jonas Club Software reports that most cloud migrations are completed within two weeks and usually schedule any cut-over downtime during off-hours[6] so that member impact is minimal. A typical migration includes a thorough pre-assessment, secure data transfer, testing, and staff training – ensuring the switch is smooth[29][30].

For example, Jonas Hosting Solutions' onboarding involves an Initial Assessment (reviewing the club's configurations), Data Migration & Setup (transferring the database to the cloud and verifying integrations), Validation & Training, and then Go-Live with support on hand[29][31]. Knowing this, boards should not tolerate vendor or internal excuses that ***"it's too difficult to upgrade."*** In 2026, cloud migration is a well-trodden path, and staying on unsupported legacy infrastructure is a bigger risk than the temporary effort to modernize.

To illustrate the shift, below is *Table 1: Traditional vs. Modern Club Technology Posture,* comparing

key aspects:

Table 1. Traditional vs. Modern Technology in Private Clubs

Aspect & Category	Traditional Posture (Legacy Approach)	Modern Posture (Current Best Practice)
Infrastructure	On-premises servers on-site (in the "back office" or closet); often aging hardware with single points of failure. Capacity is fixed and must be manually upgraded.	Cloud-hosted environments (e.g. vendor-managed on Microsoft Azure or similar) with scalable resources on demand. Redundant, geographically distributed data centers protect against local disasters.
System Updates & Security	Infrequent, manual software updates (maybe once a year or when something breaks). Security patches may lag, leaving vulnerabilities. Reliance on basic antivirus and perimeter firewall.	Continuous updates and patch management by provider – software is always up to date. Systems are monitored 24/7 for threats. Advanced defenses (web application firewalls, DDoS protection) are built in. Compliance with standards like PCI, SOC, etc., is handled by the host[28].
Data Backup & Recovery	Nightly or weekly backups stored on-site or on tapes. Recovery untested or slow. High risk of data loss if backups fail or a disaster strikes the clubhouse.	Automated backups to off-site/cloud storage with versioning. Geo-redundant backup strategy (data is copied to multiple locations). Disaster Recovery Plan in place; regular drills conducted. Can restore systems in hours, not days.
Access & Mobility	Limited remote access; staff often must VPN into on-site systems or be physically present. Systems are not designed for mobile use. Members and staff face friction access services outside the club.	Access from anywhere, anytime: staff and managers securely log into club systems via web browser or app[32]. Modern platforms are mobile-responsive (or have dedicated apps), enabling on-course or off-site work. Example: A manager can approve invoices or check club KPIs from a tablet at home.
Integration & Data Silos	Different departments use separate software (e.g., accounting software, tee sheet program, F&B POS, etc. are disconnected). Data must be manually re-entered or batch exported/imported, causing errors and delays. "Spreadsheet glue" and manual workarounds prevalent[33][34].	Unified systems or tightly integrated suite of applications. A single source of truth for member and financial data. APIs and integration hubs connect club software (e.g., membership system syncs with email marketing; POS feeds the accounting module automatically). **Fewer workarounds** – processes flow seamlessly across departments[33][34].
Scalability & Upgrades	Adding a new module or significant upgrade can be a major IT project (new hardware, installations on each PC, etc.). Systems might struggle with peak loads (e.g., online tee time rush crashing server). Upgrades often cost extra and require downtime.	Scalability is largely instant – need more capacity or a new feature? The cloud service scales up, often without noticeable downtime. New modules can be turned on remotely. Vendors push regular enhancements (sometimes monthly or quarterly) as part of subscription, so the club continually benefits from innovation.

TECHNOLOGY GOVERNANCE **PLUS**

Security & Compliance	Security depends on in-house efforts: maybe a part-time IT person updating antivirus, no formal compliance checks. Possible weak points like default passwords or outdated OS remain. Compliance (PCI for payments, etc.) may be at risk if not diligently maintained.	Security is "baked in" via professional management: data centers meet strict standards, all data is encrypted, multi-factor authentication is enabled for users. The club benefits from enterprise-grade practices and can more easily pass compliance audits[28][35]. Regular security reports and certifications from vendors provides assurance.
Support & Maintenance	Reactive "break-fix" support – problems are addressed after they cause disruption. Dependence on a few knowledgeable individuals (if they're sick or leave, knowledge gap). Significant time spent by staff on IT issues rather than on member service.	Proactive support model – continuous monitoring often detects issues before they impact users. Vendor support teams available 24/7 for critical issues. Software maintenance, backups, and performance tuning are handled behind the scenes[31]. Club staff can focus on operations, not IT maintenance.
Cost Structure	Large upfront capital expenditures (buying servers, licenses) and periodic large upgrade costs. Unpredictable repair costs if something fails. Possibly paying for unused capacity.	Subscription-based model (operational expense) that bundles updates, support, security, and infrastructure. More predictable costs, scalable with club usage. Eliminates surprise hardware repair bills; overall TCO (total cost of ownership) is often lower when factoring reduced downtime and labor.

Table 1: Comparing traditional vs. modern tech postures. A modern posture greatly reduces risk and improves agility.

Boards should review such comparisons with their club's situation in mind. If you recognize many "Traditional" characteristics in your club, it's a sign that a modernization initiative is due. An important governance insight is that technology risk often stems from obsolescence – systems that were state-of-the-art 15 years ago could be insecure and inefficient today. Thus, part of the board's risk oversight is encouraging ongoing IT renewal. Just as facilities need renovation and upkeep, so do technology platforms. The good news is, clubs don't have to do it alone; vendors and partners can do the heavy lifting. For example, Jonas Club Software offers a Hosting Solutions service to transition clubs from on-premise hosting to cloud with minimal hassle. They handle everything from the secure data transfer to ensuring integrations still work, and they manage the environment afterward (patches, backups) so club management can breathe easy[28][35].

Operational Continuity Standards

Another angle of infrastructure governance is continuity planning. Boards should set expectations for acceptable downtime and data loss. For instance, a board might establish that "in the event of a disaster, critical systems must be recoverable within 24 hours and with no more than 1 day of data loss." Management can then architect solutions to meet those targets (via cloud, backups, etc.). If a club's current setup cannot meet those standards, that is a risk to be mitigated. Modern platforms make it easier: e.g., if using a cloud SaaS for club management, the vendor likely has a disaster recovery plan and may guarantee uptime SLA (Service Level Agreements). Ask about it. During vendor assessments or annual reviews, boards can inquire: *"What was our vendor's uptime last year? Did we experience any outages, and how were they handled? Have we tested restoring data from backup?"* These questions ensure that business continuity isn't assumed – *it's verified.*

One emerging best practice is to maintain a "run book" or continuity playbook for technology. It lists what to do if each major system goes down, who to call, and how to operate manually if needed. Boards can request that management develop this if not already in place and even take part in a brief review of the plan. It's much like fire drills – you hope to never use them, but being prepared is invaluable. Given that 58% of large organizations now do cyber or continuity simulations regularly[17], clubs should at least have a basic plan drawn up.

Modernization Summary

Modernizing infrastructure is one of the highest-impact ways to reduce technology risk. It addresses many issues at once – security, reliability, efficiency, and future proofing. The board's role is to ensure that management has a roadmap for modernization (with appropriate budgeting), and that the club is not left behind due to inertia. If needed, bring in outside experts to present options and ROI of cloud vs on-premises – seeing hard numbers (e.g., how cloud could save money long-term and prevent costly breaches) can build consensus. In the next

section, we'll discuss how this technology choices tie into the specific solutions a club might deploy, and how Jonas Club Software's platform offerings can be matched to a club's needs to achieve strong governance and operational outcomes.

AI Readiness and Ethical Use in Club Operations

Alongside cybersecurity, Artificial Intelligence has rapidly become a double-edged sword for organizations. On one edge, AI offers powerful new capabilities – from automating routine tasks to uncovering insights into member data – which can greatly enhance club operations and member experience. On the other edge, AI introduces novel risks and ethical dilemmas that boards cannot ignore. In 2025 and beyond, "AI governance" is emerging as a key part of overall technology governance.

Why AI Matters Clubs

Many clubs are beginning to dip their toes into AI, whether they realize it or not. Perhaps your club's marketing team uses an AI tool to draft event promos, or your IT vendor has introduced machine learning in fraud detection for payment processing. Even member-facing tools might have AI elements (for example, an online concierge chatbot answering member questions). Internally, AI could help analyze member spending or predict usage patterns for better staffing. According to a 2025 OnBoard survey, 69% of board professionals (across various industries) reported using AI to support board work in the past 6 months[18] – for instance, summarizing long reports or gathering industry trend data via AI assistants. This indicates that AI adoption is happening at all organizational levels, including governance. Ignoring AI is not an option; clubs should instead ask how to *leverage* AI for advantage while *controlling* its risks.

AI Risks and Concerns

With great power comes great responsibility. AI systems, especially "black box" models like generative AI (ChatGPT, etc.), come with a host of concerns:

- **Data Security:** Many AI tools are cloud-based and trained on broad data. If staff feed sensitive club data (e.g. member lists or financial info) into a public AI service, where does that data go? There's risk of inadvertent data leakage. In fact, a KPMG study found that most employees were using publicly available AI at work rather than employer-provided solutions, often in ways that contravene policies[5]. This underscores the need for clear rules on what data can be put into AI systems.
- **Accuracy and Reliability:** AI can sometimes produce incorrect or fabricated answers with great confidence. If a club relied on AI to generate policy answers or member communications, it could spread misinformation. There have been cases of AI chatbots making up policy details or mis-stating financial figures – a risk for club communications or decision-making if unchecked.
- **Bias and Fairness:** AI systems trained on large datasets may unintentionally carry biases. In a club context, imagine an AI scheduling tool that inadvertently favors certain member demographics for popular time slots due to biased training data – this could create perceptions of unfair treatment. Boards should be mindful that AI decisions (which member gets what, or which applicant to hire, etc.) remain fair and transparent.
- **Ethical and Reputational Issues:** Using AI in ways that affect people's livelihoods (e.g. AI-assisted hiring decisions for club staff) or member experience (like dynamic pricing of club services) can raise ethical questions. A misstep could harm the club's reputation. Additionally, AI-generated content needs to be reviewed; for example, an AI-written social media post might use language that doesn't align with the club's voice or values.
- **Regulatory Horizon:** While few AI-specific laws apply to clubs today, regulations are on the horizon globally. The EU is finalizing an AI Act that will impose strict rules on AI systems based on risk tiers. Many jurisdictions are pushing for AI transparency (informing users when content is AI-generated) and accountability. There is strong public support for AI oversight – 70% of people believe AI needs to be regulated[19]. Boards that proactively implement ethical AI guidelines will be ahead of any future regulatory mandates.

Board's Role in AI Governance

Much like cybersecurity, boards should approach AI with a mix of curiosity and caution. Here are concrete steps and considerations for club boards regarding AI:

- **Set an AI Usage Policy:** Work with management to draft a policy that covers if and how staff may use AI tools in their work. For example, the policy might state that no member of PII or confidential club financials are to be input into public AI services. It might allow using AI for brainstorming or initial drafts of documents but require human review before anything is published. Also consider rules around AI image generators (to avoid copyright issues or inappropriate imagery). If the club uses AI in operations (say an AI scheduling assistant), disclose it to users transparently. The policy should encourage innovation but set guardrails – think of it as an "acceptable use policy" for AI.
- **Educate and Train:** Ensure that management and staff have basic training on AI's benefits and pitfalls. Just as we train employees on phishing emails, we should train them on the dos and don'ts of AI at work. For instance, emphasize that free AI tools may save what you input (so they must not paste sensitive data). Encourage a healthy skepticism of AI outputs – trust but verify. If the board itself is using AI (some board members use ChatGPT to summarize reports), be open about it and share best practices among

directors.

- **Leverage AI Responsibly:** Encourage management to identify areas where AI could improve efficiency or member experience, and pilot solutions in a controlled manner. The board can ask, "How are we exploring AI to stay competitive or enhance service?" Perhaps AI-driven personalization in club mobile apps, or AI analytics to find cost savings. However, any AI project should include an ethical and risk review. Before deploying, ask: what's the worst that could happen with this AI? Are we comfortable with its decisions, and can a human override if needed?
- **Implement an AI Readiness Framework:** Several voluntary frameworks exist to guide organizations on trustworthy AI (OECD AI Principles, NIST AI Risk Management Framework, etc.[20][21]). While these can be dense, the core ideas can be adopted in plain language: fairness, accountability, transparency, privacy, security, and human oversight. For example, the board can mandate that any AI system the club implements must be *"explainable and with human oversight."* In practice, that means if an AI tool flags a member for unusual spending, a human manager reviews that before any action; or if AI suggests dynamic pricing for an event, management checks it for fairness. A Jonas Software insight recommends labeling each AI use-case by risk and keeping a human in the loop for high-impact actions (like anything involving money or changing member data)[22]. Build these principles into the club's approach.

To visualize how clubs might evaluate AI uses, *Table 2* below presents a sample AI Risk Matrix with examples:

Table 2. Sample AI Risk Matrix for Club Applications

AI Use Case in Club	Potential Risk Level & Impact	Key Governance Measures (Controls)
Automated member email drafting – AI suggests content for club newsletters or routine member communications (staff edits before sending).	**Low Risk** (Efficiency gain, minor direct impact on members without human review). Potential risks: tone inaccuracies.	**Control:** Require human review & approval of all AI-drafted text. Provide style guidelines the AI must follow. No sensitive data in prompts.
Member help chatbot on website – Answers member queries about club hours, events, account balance, etc.	**Medium Risk** (Member-facing but non-sensitive info; incorrect answers could confuse or frustrate members).	**Control:** Limit chatbot answers from an approved knowledge base. Clearly indicate it's automated. Have staff periodically audit chatbot responses for accuracy. Allow easy escalation to a human if the bot cannot help.
AI analytics on member spending – AI flags "high-risk" or "at-risk" members based on spending changes or attendance patterns for follow-up.	**Medium-High Risk** (Informs decisions that affect member outreach or dues management; could be biased or intrusive if wrong).	**Control:** Ensure the algorithm is reviewed for bias (e.g., not inadvertently singling out a demographic). Use AI insights as *suggestions*, not final judgments – a manager reviews flagged cases privately. Communicate to members transparently if such analytics are used to enhance their experience (maintain trust).
AI-driven decision support for finances – AI forecasts budget or recommends cost cuts (or AI auto-approves certain expense requests).	**High Risk** (A bad recommendation could harm financial health; if automated, could erroneously cut a critical service).	**Control:** Keep a **human-in-loop** for all financial decisions[22]. Treat AI output as one input among many. Set conservative bounds – e.g., AI can *suggest* a budget reallocation but cannot execute anything. Have finance committee review AI-generated forecasts versus traditional forecasts to validate reliability.

TECHNOLOGY GOVERNANCE **PLUS**

AI Use Case in Club	Potential Risk Level & Impact	Key Governance Measures (Controls)
Facial recognition for facility entry – AI system at the clubhouse door to recognize members for entry (in lieu of showing ID).	**High Risk** (Privacy implications, bias risk, security if spoofed).	**Control:** Conduct through legal/privacy review. Obtain explicit member consent. Ensure high accuracy and fallback (e.g. manual check if uncertain). Regularly test for bias (system should work equally well for all demographics). Possibly avoid altogether if not aligned with club culture.

In the matrix above, as risk increases, so do the required controls and oversight. The board's Technology or Risk Committee (if one exists) could maintain such a matrix for all AI-related initiatives. This ensures a structured evaluation of AI projects. As noted in one AI governance report, boards are formalizing oversight: 40% of companies now assign AI oversight to a board committee (often Audit or Technology committees) in 2025, up from just 11% the year prior[23]. A club might not have multiple committees, but it can assign AI risk to, say, the Finance Committee or a new Task Force. The key is explicit accountability – someone at the governance level watching this area.

Ethical Use Framework

Given the lack of clear AI laws for now, a "soft law" approach grounded in ethics is wise[24][25]. Many organizations adopt principles such as fairness, transparency, and accountability as North Stars for AI use. A practical step is to draft a short AI Ethics Charter for your club. It could state, for example: *"Our club will use AI in ways that respect member privacy, avoid discrimination, and improve member services. We will be transparent about when AI is used, ensure human oversight of critical decisions, and regularly review our AI systems for accuracy and bias."* Such a charter, approved by the board, sets the tone from the top. It can be shared with members to build trust ("your club is forward-thinking but careful with AI"). And it gives management a clear mandate when implementing AI solutions.

Upskilling and External Advice

If board members or management feel out of depth on AI topics, leverage external resources. Many industry associations (including CMAA and NCA) are beginning to offer AI-focused education. For instance, CMAA's 2025 Leadership/Legislative Conference included sessions on "offensive cyber operations in the private sector" and the "strategic use of AI for threat detection"[26] – signaling that even club industry events are tackling these issues. Engaging experts or consultants for a briefing to the board can be a good investment. Jonas Club Software, through its webinars and publications, also provides insight into how AI intersects with club management. Jonas Club Software's R&D offers perspective – their next-gen Synergy platform, for example, *"combines trusted operational knowledge with modern design, automation, and AI-driven insight."* [27] This indicates that AI is being built thoughtfully into club management tools (e.g., predictive analytics in dashboards) rather than as hype. Boards should ask vendors to explain how they use AI in their products and ensure it aligns with the club's policies.

AI Summary

In summary, boards should neither fear AI nor embrace it blindly. Treat it as another area of oversight: one that requires understanding the strategic upside (better service, efficiency) and the risks. By establishing clear frameworks and expectations now, private clubs can harness AI to enhance member experiences and operations *responsibly*. The board's voice is crucial in setting that balance – championing innovation with ethics. As we turn to the next section on infrastructure, remember that technology governance spans people, processes, and the very systems underpinning everything – which we address next.

Aligning Technology Solutions with Governance and Club Complexity

One size does *not* fit all in private club technology. A family country club with multiple golf courses, a marina, and hundreds of employees will have different needs than a smaller golf club with a single dining room and a lean staff. What's important is that the technology platform(s) a club uses supports its governance, risk management, and operational goals. Jonas Club Software provides three core club management platforms – Jonas Club Management (JCM), Jonas Encore, and Jonas Synergy – which together cover a spectrum from highly feature-rich to streamlined and modern. Boards and GMs should understand where their club fits and how the right platform can bolster risk management and efficiency. Here's an overview:

Jonas Club Management (JCM)

JCM is Jonas Club Software's long-standing, full-featured system used by many large or complex clubs. It's proven and comprehensive – covering everything from accounting, membership CRM, POS, tee times, retail, events, payroll, etc. – a true end-to-end ERP for clubs. For clubs with multiple lines of business (golf, tennis, spa, lodging, etc.) or high complexity, JCM offers the depth needed.

Governance Angle: JCM supports strong internal controls and audit trails in financial modules,

integrates data across departments (reducing silo risk), and is continually updated. Jonas Club Software has shown commitment to modernizing JCM's user interface and features in response to client feedback. (In fact, club managers in 2025 noted "a major shift in [Jonas Club Software's] commitment to modernization" in JCM, with new dashboards that bring key information into one intuitive view[36].) JCM can now be cloud-hosted via Jonas Club Software, meaning clubs get rich functionality without having to maintain on-prem servers. Jonas Club Software publicly states that JCM (and Encore) remain "trusted, fully supported platforms…continuing to receive active investment and modernization."[37] This "software for life" promise[38] is crucial for governance. Boards can be assured that if they are on JCM, the vendor is not sunsetting it but rather keeping it current. The board's role is to ensure the club takes advantage of those updates and is on a supported version, ideally hosted for security.

Jonas Encore

Jonas Encore is another robust platform in the Jonas Club Software suite, historically favored by certain clubs (sometimes due to regional preference or specific module strengths). It's similar in scope to JCM in covering all core areas of club operations but might have a different interface or workflow. Think of it as an alternate flavor of a full club management system, also capable of handling complex needs.

Governance Angle: Jonas Encore, like JCM, can be cloud-hosted and benefits from Jonas Club Software's investments. It's designed for clubs that require a high degree of configuration and functionality. Boards overseeing clubs on Encore should ensure they are engaging with Jonas Club Software on updates and training. The existence of both JCM and Encore shows Jonas's approach of not forcing all clubs onto one system, respecting that different clubs have different legacy preferences or feature requirements. But importantly, Jonas Club Software positions Synergy as complementary to JCM and Encore – not a replacement for all clubs[37]. So, a board should evaluate whether their needs are met by the current platform or if a shift makes sense. Jonas Cub Software will continue to support JCM/Encore, so there's no immediate risk in staying, as long as they are modernized (e.g., hosted, latest version).

Jonas Synergy

Launched as the next-generation platform, Synergy is a browser-based, cloud-native system built "from the ground up" for clubs that want to simplify operations[39][40]. Synergy embodies modern design principles: it's intuitive, works on any device, and consolidates functions seamlessly. Jonas Club Software explicitly states Synergy is *"for private clubs that value tradition but are ready to move beyond disconnected systems and manual workarounds."*[41] It brings membership, accounting, POS, reservations, etc., into one connected interface, leveraging automation and AI-driven insights to assist staff[42]. However, Jonas Club Software also clarifies what Synergy is and isn't – it is not aimed at clubs needing "enterprise-level complexity"[43][44]. Rather, it's for clubs with *streamlined needs that want simplicity without sacrificing quality*[45]. For example, a golf club with a single course and a modest F&B operation might find Synergy covers everything in a clean, user-friendly way – eliminating the need for multiple add-ons or third-party integrations.

Governance Angle: By reducing system complexity, Synergy inherently reduces certain risks (fewer integration points, less need for workarounds that can introduce errors[33]). Its cloud-native nature means updates roll out regularly, and security is handled by Jonas Club Software. A board overseeing a club that fits Synergy's target profile might consider the benefits of moving to this platform – especially if the current patchwork of systems is causing headaches or risks. Synergy's intentional design around club workflows[46] also means faster training for staff (lower risk of user error) and better data visibility for management (e.g. real-time dashboards across departments[47]).

Matching Platform to Club Profile

The decision on which platform is best should be based on an objective assessment of the club's operational complexity and strategic direction.

Large Clubs

If your club has extensive operations (multiple departments, very large membership, complex accounting needs like multi-entity or tax scenarios, etc.) – JCM or Encore will likely remain in the backbone, as they have the proven breadth. The governance focus should be on *modernizing how you use those platforms* (cloud, modules fully utilized, etc.) rather than replacement.

Medium-Sized Clubs

If your club is medium-sized or looking to streamline and you find your staff juggling many systems that don't talk to each other – Synergy could be attractive. It's an opportunity to "reset" with a fresh platform that may improve efficiency and reduce IT overhead. The board should, however, weigh the transition carefully: ensure that critical features your club relies on are available in Synergy, or have a roadmap to be delivered. Jonas Club Software is actively developing Synergy with input from clubs (it's already in use at pilot clubs[48]), and they are likely adding features rapidly. Engage Jonas Club Software for a demo and ask tough questions about any feature gaps relative to JCM/Encore. A move to Synergy would be a strategic investment, and boards must ensure it truly aligns with the club's needs. That said, Jonas Club Software's emphasizes that Synergy is built specifically for *private clubs' workflows* (not a generic hospitality system)[49] resonates well with governance: it means less customization and bending of the software to fit club reality, because it was purpose-designed for clubs.

Small Clubs

If your club is small or has very unique/simple needs, there are also scenarios where an all-in-one might be overkilled. But even small clubs benefit from integrated systems. The risk of

TECHNOLOGY GOVERNANCE **PLUS**

using ad-hoc tools (Excel for accounting, a standalone booking app, etc.) is the lack of control and efficiency. In those cases, a right-sized solution like Synergy can elevate governance by introducing proper record-keeping, approval of workflows, and so on – without a huge cost or complexity burden.

Integration, Risk Management & the Human Element

Integration

It's worth noting that beyond core management systems, Jonas Club Software offers a range of integrated applications (websites via ClubHouse Online/MembersFirst, mobile apps, data analytics via MetricsFirst, payments, etc.[50][51]). The value of governance is that using a cohesive ecosystem reduces the cybersecurity risk of juggling many vendors. For instance, Jonas Club Payments ensures PCI compliance for club transactions[52], the websites platform offers secure member portals, and so forth – all under one umbrella.

A board might ask management for an inventory: *"How many different software vendors are we using to run the club?"* If the list is long, there's potential risks in each integration and vendor relationship. Consolidating with a primary partner like Jonas Club Software can simplify oversight. That said, no single vendor does everything, so the key is that whatever systems exist, they are well-managed. Ensure that any third-party systems connected to Jonas Club Software (for example, a specialty golf simulator that hooks into member charges) are also secured, and that vendor contracts include data protection clauses.

Risk

To highlight how technology ties back to governance and risk: imagine a board report that the GM/CIO might present annually about the club's technology. In a mature scenario, it would cover: system uptime statistics, notable upgrades made (e.g., "we migrated to cloud hosting in April with zero downtime"[6]), user adoption of new features (like managers using a new mobile app for approvals), cybersecurity incidents or lack thereof ("we had 3 minor phishing incidents, all contained, and no data breaches"), and planned initiatives ("next year we plan to implement MFA for all member logins, and deploy a new data analytics dashboard for more transparency"). By adopting robust platforms and processes, management can give the board concrete, positive metrics in these reports. If a club is stuck on old tech, those reports might instead be full of excuses: "server was down for 2 days, we're working on patching, we think data is backed up but haven't tested," etc. That contrast directly impacts the board's comfort that they are meeting their fiduciary duties in oversight.

The Human Element

Finally, consider the human element: technological governance isn't just systems; it's also people and accountability. Many clubs have limited IT staff – perhaps an IT Director who wears many hats, or an external IT service provider. Boards should ensure that roles are clear for technology management. If using Jonas Club Software for many services, lean on their customer success and support teams to fill knowledge gaps. Encourage management to conduct annual strategic reviews with key vendors. Jonas, for example, offers Strategic Account Reviews (as seen on their site[53]) to help clubs plan utilization and improvements. The board can ask, "Have we done a strategic review with Jonas (or our tech partners) this year to see how we can better use the systems and improve security or efficiency?" This keeps the vendor relationship proactive, not just calling support when things break. It also sends a signal to the vendor that the club's leadership is engaged – often yielding better service and alignment.

Technology Alignment Summary

In conclusion to this section, aligning the right technology platform with your club's complexity and governance needs is crucial. Jonas Club Software's platforms each provide a pathway to operational maturity when used correctly. Whatever mix of systems a club chooses, the board's focus should be on: are these systems secure, modern, well-integrated, and supporting effective oversight? If not, it's time to strategize a change. With that, we wrap up the detailed analysis and move to a concluding call to action for club leaders.

Calls to Action for Boards, GMs, and Committees

Technology governance might sound abstract at times, but it boils down to concrete actions. To supplement the comprehensive discussion above, here is a clear list of next steps and initiatives that club boards, general managers, and finance/technology committees should consider in the immediate term:

1. **Commission a Cybersecurity Assessment:** If your club has not undergone an independent security assessment or penetration test in the last 12-18 months, schedule one now. An external review will highlight vulnerabilities to address and demonstrate due diligence[54]. Many clubs partner with firms like Pulsar Security for this. As part of this, review your cyber incident response plan (or create one if it doesn't exist. Bring the results and plan to the board for discussion and approval of needed investments.

2. **Adopt a Security Framework & Improve Policies:** Task management (perhaps with consultant help) to map the club's practices to a known cybersecurity framework (for example, the NIST CSF or the CIS Controls). It doesn't have to be onerous – even a simplified checklist can reveal gaps (e.g., "Do we have MFA? Do we have network segmentation? Are backups encrypted?"). Use this system to improve. Simultaneously, update IT policies: password policy, acceptable use (covering personal device use, etc.),

TECHNOLOGY GOVERNANCE **PLUS**

data handling procedures. Ensure a clear data governance policy is in place – classify data (public vs. confidential) and outline how each category is protected and who is responsible. The board should formally approve these policies to show support from the top.

3. **Establish AI Guidelines and Training:** Don't wait for an AI mishap to react. Formulate an AI ethics and usage guideline as discussed in the AI section. Educate your team on those guidelines and the general risks of AI (privacy, accuracy). Encourage innovation within guardrails. Perhaps run a workshop for managers on "Using AI efficiently and safely" – including demonstrations of tools that could help (like automating a report) and discussion of what not to do (like uploading membership lists to ChatGPT). The board can request management to report on any AI pilot projects and their outcomes periodically.

4. **Evaluate Infrastructure Upgrades (Cloud Migration):** If your club is still running core systems on-premises, board committees (e.g., Finance or Tech committees) should work with management to evaluate a move to cloud hosting or a newer platform. Get proposals from vendors (e.g., Jonas Hosting Solutions) to understand cost vs benefit. Consider not just the IT perspective, but the member experience: modern infrastructure can enable new member-facing services (like better online self-service, mobile engagement) that old systems cannot. That tie-in can justify the investment to stakeholders. Set a target – for example, *"By next season, we will migrate our club management system to a secure cloud environment."* Then track progress. Given that Jonas Club Software can migrate in two weeks with minimal downtime[6], once approved, this initiative can be executed relatively quickly in the off-season.

Engage in Vendor Strategic Planning: Proactively reach out to key technology vendors (club software provider, website provider, etc.) for a forward-looking review. Ask them: *"What new features or security enhancements have you released that we should be using? What's on your roadmap that can help our club?"* This dialog can uncover opportunities (perhaps a module you already pay for but haven't deployed fully). It also lets you influence the roadmap by expressing your club's needs. For example, if your board is keen on data analytics for better oversight, ask Jonas Club Software about tools like MetricsFirst or new dashboard capabilities. Jonas often touts "deep insights and analytics" as part of their suite[55] – ensure you're leveraging those to get board-level KPIs on your club's health.

5. **Audit Current Tools and Contracts:** Initiate a review (maybe by an internal task force or external consultant) of all technology tools in use. Evaluate each for redundancy, security, and effectiveness. Often clubs accumulate niche software over time that might now be replaced by capabilities in an integrated system. Also check software licenses and support contracts – are you on current versions? Do any contracts lapse soon? This audit can feed into budgeting – perhaps consolidating software could save money or redirect funds to more critical areas (like cybersecurity training or an AI solution that adds real value).

6. **Improve Board Technology Literacy:** Encourage board development in technology governance. This could mean adding a board member or advisor with IT/cyber expertise (if your board lacks that skill set, consider recruiting a technology executive as a member or an advisory role). In the meantime, utilize resources from CMAA, NCA, or NACD on tech oversight. For example, NACD (National Association of Corporate Directors) has published "10 Questions Boards Should Ask About Cybersecurity"[56] and is focusing increasingly on AI oversight as well[57]. Tailor those for your club context and discuss them in a board meeting. A well-informed board will make better decisions and support management in tech initiatives rather than view them as mere expenses.

7. **Champion a Culture of Continuous Improvement:** Perhaps the most important call to action is cultural. Boards and GMs should send the message that "good enough" is not sufficient in the realm of technology and security. Just as clubs strive for excellence in member service, they should strive for excellence in the systems and processes that enable that service. Celebrate quick wins (e.g., "We moved to multi-factor authentication for staff logins – a big step for security!"). Make tech governance a standing item in board agendas or GM reports, even if brief, to keep it top of mind. When budgeting, allocate funds for IT upgrades annually, not just once a decade – treating it as ongoing infrastructure maintenance akin to golf course upkeep or clubhouse repairs. And ensure accountability: assign clear responsibility for technology strategy execution (whether it's the CFO, an IT Manager, or an external consultant reporting to the GM). The board's role is to hold that person accountable while providing support and resources.

In executing these actions, leverage the partnership of Jonas Club Software and Pulsar Security where applicable. **Jonas Club Software** can assist with platform optimization, training, and infrastructure modernization. They have decades of experience with over 2,300 clubs using their solutions[58], and can often share best practices from other clubs of similar size or complexity. **Pulsar Security**, as a specialist in offensive cybersecurity, can provide services like penetration testing, dark web monitoring, and cybersecurity education tailored to club environments. Their philosophy, as quoted earlier, is to meet organizations at their current security maturity and elevate them[7] – an approach well-suited for clubs that might be early in their cyber journey. CMAA and NCA can also be partners – through webinars, publications, and perhaps facilitating peer discussions (e.g., forming a small council of club board members focused on technology governance to share experiences).

Final Thoughts

Technology has become a core pillar of private club management and thus a core concern for club governors. Where once a board's oversight might stop at finances and facilities, it must now extend to firewalls and phishing drills, from websites to "web3" (**s**hould that become relevant!). This 2026 Technology Governance supplement t is aimed to arm board members and club

executives with an updated understanding of the landscape – highlighting new challenges like AI and ever-present ones like cybersecurity, as well as practical guidance to strengthen your club's tech posture.

Importantly, it emphasizes that technology governance is ultimately about risk reduction and enabling club success. Secure, reliable systems free up management and staff to focus on delivering exceptional member experiences (instead of firefighting IT issues). Modern data analytics and AI can uncover opportunities to personalize services or save costs (with proper oversight). Conversely, neglected tech can undermine even the best-run club – a data breach or prolonged outage can erode member trust and financial stability.

The board's fiduciary duty to safeguard the club absolutely encompasses digital assets and infrastructure. By following the recommendations herein – from independent cyber validation[54] to ethical AI frameworks[22], from cloud migrations[6] to pointed boardroom questions – club leaders will be better equipped to fulfill that duty. It bears repeating that this is a continuous process, not a one-time project. "Cybersecurity is a journey, not a destination," as Pulsar's team underscores[59], and the same is true for overall tech governance. Each year the board should evaluate progress, address new risks, and push the club to maintain a forward-looking stance.

In closing, the tone from the top is critical. If the board is visibly engaged in and enthusiastic about technology initiatives (whether it's a new member app or a cybersecurity drill), the whole organization will prioritize them accordingly. Use this guide as a conversation starter with your fellow directors and management team. Identify 2-3 top priorities for your club from these pages and commit to them in your strategic plan. And remember, you're not alone on this path – your software and security partners, and the broader club industry network, are there to support. With sound governance, the right technology, and vigilance, clubs can innovate securely and continue providing the extraordinary experiences that members expect, well into the digital future.

References

- Jonas Software Insights – *"AI in Cybersecurity: Helping or Harming?"* (Nov 20, 2025)[1][22]

Cybernews – *"Ransomware gang claims San Francisco's Cal Club, exposing members' data"* (Oct 8, 2025)[2][8]

- Reuters – *"Casino giant MGM expects $100 million hit from hack"* (Oct 6, 2023)[10][11]
- CMAA Chapter Digest – *"Pulsar Security Renews Commitment to CMAA Partnership"* (May 2025)[7]
- Pulsar Security Blog – *"Cyber Insurance Isn't Enough: What Businesses Still Need to Do"* (Apr 11, 2025)[12][16]
- Corporate Compliance Insights – *"Board Oversight of AI Triples Since '24"* (Oct 31, 2025)[3][13]
- Jonas Club Software – *"Hosting Solutions – Migration Made Simple"* (2025)[6][30]
- Jonas Club Software – *"Jonas Synergy – A Modern Platform"* (2025)[33][27]
- OnBoard Board Management Survey (2025) via CCI[18]
- KPMG/University of Melbourne – *"Trust in AI – Global Study 2025"* via Reuters Practical Law[5]

(Additional references available in the full Jonas & Pulsar webinar materials and CMAA/NCA publications.)

[1] [22] AI In Cybersecurity - Is AI Helping or Harming? - Jonas Software

https://jonassoftware.com/ai-in-cybersecurity-is-ai-helping-or-harming

[2] [8] Hackers hit California Golf Club of San Francisco | Cybernews

https://cybernews.com/news/cal-club-ransomware-attack-california-golf-club-san-franscico-qilin-claims/

[3] [13] [17] [18] [23] [57] Board Oversight of AI Triples Since '24 | Corporate Compliance Insights

https://www.corporatecomplianceinsights.com/news-roundup-october-31-2025/

[4] [5] [19] [20] [21] [24] [25] Board Oversight of AI Risk Through an Ethical Lens | Practical Law The Journal | Reuters

https://www.reuters.com/practical-law-the-journal/transactional/board-oversight-ai-risk-through-an-ethical-lens-2025-11-01/

[6] [28] [29] [30] [31] [32] [35] Jonas Hosting Solutions - Jonas Club Software

https://www.jonasclub.com/jonas-club-software-hosting/

[7] Outlook Issue April 25, 2025 | CMAA | Publications

https://www.cmaa.org/outlook/outlook-issues/april-25-2025/

[9] Average Cost of a Healthcare Data Breach Falls to $7.42 Million

https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-2025/

[10] [11] Casino giant MGM expects $100 million hit from hack that led to data breach | Reuters

https://www.reuters.com/business/mgm-expects-cybersecurity-issue-negatively-impact-third-quarter-earnings-2023-10-05/

[12] [14] [15] [16] [54] Cyber Insurance Isn’t Enough: What Businesses Still Need to Do

https://blog.pulsarsecurity.com/cyber-insurance-isnt-enough-what-businesses-still-need-to-do

[26] Leadership/Legislative Conference 2025 | CMAA | Events

https://www.cmaa.org/learn/past-meetings-and-events/llc-2025/

[27] [33] [34] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] Jonas Synergy - Jonas Club Software

https://www.jonasclub.com/synergy/

[36] [53] Looking Ahead Together - Jonas Club Software

https://www.jonasclub.com/looking-ahead-together/

[50] [51] [55] [58] Jonas Club Software to Showcase 30 Years of Innovation at the 2025 PGA Show in Orlando - Jonas Club Software

https://www.jonasclub.com/jonas-club-software-to-showcase-30-years-of-innovation-at-the-2025-pga-show-in-orlando/

[52] Request Governance Guide - Jonas Club Software

https://www.jonasclub.com/request-governance-guide/

[56] 10 Questions for a Board Member to Ask About Cybersecurity

https://www.nacdonline.org/all-governance/governance-resources/governance-research/boardroom-tools/10-questions-for-board-member-ask-about-cybersecurity/

[59] Advanced Offensive Cybersecurity Services | Pulsar Security

https://www.pulsarsecurity.com/

TECHNOLOGY GOVERNANCE **PLUS**

JONAS
CLUB SOFTWARE

1-800-352-6647
8133 Warden Avenue, Suite 400
Markham, Ontario
Canada, L6G 1B3
support@jonasclub.com