Insurance Board
Partners in Protection

The Steward

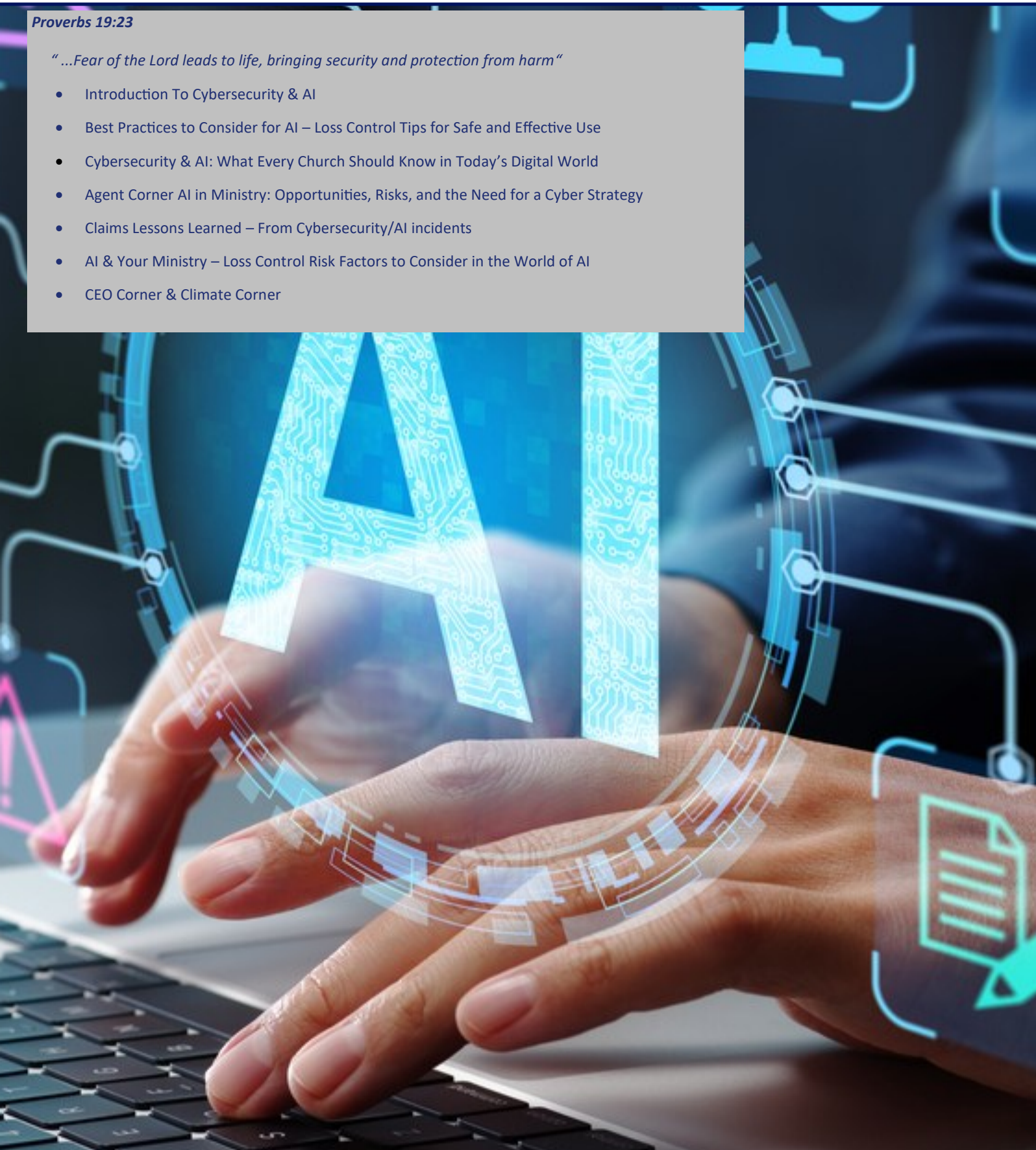
Fall 2025

Trustworthy Insurance Insights for Churches and Ministries

Proverbs 19:23

" ...Fear of the Lord leads to life, bringing security and protection from harm"

- Introduction To Cybersecurity & AI
- Best Practices to Consider for AI – Loss Control Tips for Safe and Effective Use
- Cybersecurity & AI: What Every Church Should Know in Today's Digital World
- Agent Corner AI in Ministry: Opportunities, Risks, and the Need for a Cyber Strategy
- Claims Lessons Learned – From Cybersecurity/AI incidents
- AI & Your Ministry – Loss Control Risk Factors to Consider in the World of AI
- CEO Corner & Climate Corner



Introduction To Cybersecurity & AI

Insurance Board

Cybersecurity and Artificial Intelligence have become essential elements for almost every business. In a world where technology tools are continually evolving, many have begun adopting artificial intelligence into their everyday practices.

At Insurance Board, staff are encouraged to find ways to utilize AI to enhance productivity, speed, and efficiency, while also maintaining best practices for Cybersecurity and technology safety.

According to NASA (National Aeronautics and Space Administration), Artificial Intelligence refers to computer systems that can perform complex tasks normally done by human-reasoning, decision making, creating, etc.

Cybersecurity, on the other hand, as defined by CISA (Cybersecurity & Infrastructure Security Agency), is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

For church ministries, you may be asking yourself how, if, or why cybersecurity matters to your organization and if your ministry should begin adopting AI technology.

Enclosed in this issue of The Steward are articles related to the risk factors of AI, but also the benefits of utilizing AI safely. There's also an article from Insurance Board's technology team, along with insight on best practices to consider for Cybersecurity.

In addition, in the near future, Insurance Board will be launching a new Cyber Insurance product that your ministry can consider for additional coverage. This special insurance coverage option would cover items like:

- Data Compromise Response Expenses
- A Computer Attack
- Cyber Extortion
- Identity Recovery

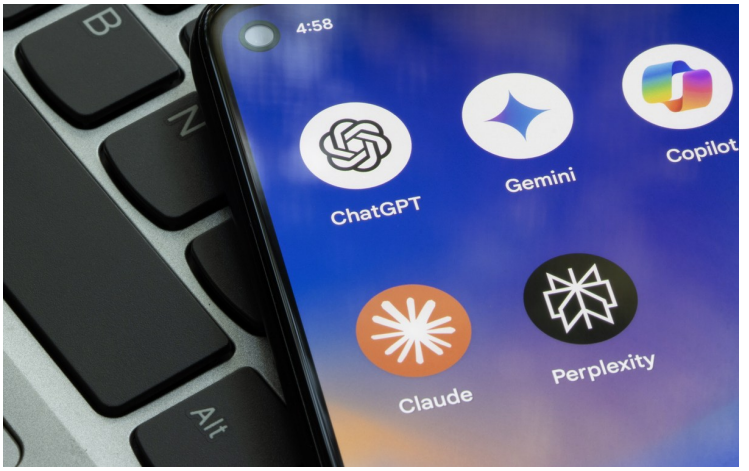
As you read this issue of The Steward, consider the ways that might make sense for your ministry to utilize AI or enhance Cybersecurity measures to protect your church's data.

Insurance Board also encourages you to visit the Online Learning page on our website to watch or re-watch prior videos with helpful information for your ministry. Contact your local Insurance Board agent today to discuss your specific needs regarding Cybersecurity, AI, and to learn more about the new Cyber product Insurance Board is offering.

www.InsuranceBoard.org/Online-Learning/

Best Practices to Consider for AI – Loss Control Tips for Safe and Effective Use

Insurance Board



Artificial Intelligence (AI) is a powerful tool that can enhance ministry operations—from automating repetitive tasks to improving communication and outreach. However, while AI offers convenience and efficiency, it also introduces new risks that ministries must manage carefully. By following best practices, ministries can use AI effectively while minimizing potential liabilities.

1. Understand the Tool

Before adopting any AI platform, understand what it does, how it works, and what data it accesses. Not all tools are created equal. Some may collect sensitive information, require third-party integrations, or store data in unsecured environments. Choose AI solutions with transparent privacy policies and robust security features.

2. Keep Human Oversight

AI should assist—not replace—human judgment. Always review AI-generated content before sharing it publicly or using it in decision-making. Whether you're using AI to draft emails, sermon illustrations, or create promotional graphics, human oversight helps ensure accuracy, tone, and alignment with your ministry's values.

3. Watch for Bias and Inaccuracy

AI can reflect biases present in its training data and occasionally generate incorrect or inappropriate content. Ministries must remain alert to outputs that could be misleading, insensitive, or legally risky. Review AI-assisted decisions—especially in areas like hiring, messaging, or member engagement.

4. Be Aware of Copyright Issues

AI-generated content may pull from copyrighted sources. Always check terms of service, and when in doubt, treat AI-created material as if it needs the same permissions or citations as any other third-party content.

5. Have a Clear AI Policy

Develop and communicate a written AI use policy. This should outline approved tools, usage guidelines, ethical boundaries, data protection measures, and who has access. A strong policy helps maintain consistency, accountability, and responsible use.

6. Train Your Team

Educate staff and volunteers about responsible AI use. Clear guidelines and awareness can prevent misuse, protect sensitive data, and reinforce ethical boundaries.

AI can be a helpful tool—but only when used with thoughtful planning, clear policies, and ongoing vigilance. With a loss control mindset, ministries can leverage AI's strengths while protecting their mission and community.

Cybersecurity & AI: What Every Church Should Know in Today's Digital World

How to protect your ministry as technology and threats evolve. Featuring Insurance Board's Technology Team

In today's digital age, churches are more connected than ever. Sunday sermons are streamed online. Tithes are given through apps. Events are organized via email and social media.

It's an incredible way to reach people where they are — but it also opens the door to new risks. As more of church life moves online, two big topics are becoming increasingly important: cybersecurity and artificial intelligence (AI).

Don't worry — you don't need to be a tech expert. This article is designed to explain what these terms mean, why they matter to churches, and what simple steps you can take to stay safe.

What Is Cybersecurity?

Cybersecurity is just a fancy word for protecting your church's digital information. Think of it like locking the church building — but for your emails, online donations, livestreams, and digital records. It helps prevent things like:

- ◊ Identity theft
- ◊ Email scams
- ◊ Website hacks
- ◊ Unauthorized access to member data

Why Are Churches Targeted?

You might not think of your church as a target — but unfortunately, many cybercriminals do.

Here's why:

- ◊ Churches store personal data, like names, emails, and donation history.
- ◊ Many churches have limited tech support, which makes them easier to exploit.
- ◊ Their open, trusting nature can make it easier for scammers to manipulate staff or volunteers.

Did You Know?

- ◊ In 2024, nonprofits experienced a 30% increase in cyberattacks, with over 1,600 attacks each week.
- ◊ 68% of data breaches involved human error — like clicking a phishing email.
- ◊ 32% of attacks happened because software wasn't kept up to date.

(Source: BDO & CyberPeace Institute Reports, 2025)

What About AI? Is It Helping or Hurting?

Artificial Intelligence (AI) is everywhere — even in church life. AI can be a blessing, but it can also be misused.

How Churches Use AI for Good:

- ◊ Spam filters: Automatically detect and block scam emails.
- ◊ Fraud alerts: Some donation platforms use AI to catch unusual transactions.
- ◊ Chatbots: Help answer basic questions on your website, even outside office hours.

But There Are Risks:

- ◊ AI-generated scams: Attackers now use AI to write convincing phishing emails.
- ◊ Deepfakes: Fake videos or audio that sound like someone you know.
- ◊ Targeted attacks: AI tools can scan your website and social media to learn how to trick your team.

Simple Steps to Protect Your Church

You don't need a tech team to be smart about cybersecurity. Here are easy, practical steps you can start today:

- ◊ Use strong, unique passwords
- ◊ Avoid short, common passwords. Consider using a password manager.
- ◊ Turn on two-factor authentication (2FA)

Cybersecurity & AI: What Every Church Should Know in Today's Digital World

How to protect your ministry as technology and threats evolve. Featuring Insurance Board's Technology Team

- ◊ Add an extra layer of security to logins with a text or app code.
- ◊ Train your staff and volunteers
- ◊ Teach them how to recognize suspicious emails and websites.
- ◊ Keep everything updated
- ◊ Updates often include important security patches. Don't skip them.
- ◊ Back up your data regularly
- ◊ Save copies of critical files in a secure cloud or offline location.

Final Thoughts

Your church already protects what matters — its people, its message, its resources. Cybersecurity is simply an extension of that in the digital world.

You don't have to fear technology. With a little awareness and some thoughtful planning, your church can use digital tools confidently and responsibly.

Whether you're the pastor, administrator, or the person who updates the church's Facebook page, your role in cybersecurity matters. And the good news is, you're not alone. There are simple, affordable ways to stay safe and keep your ministry moving forward.

Agent Corner

Michael Campbell, MinistrySure Agency

AI in Ministry: Opportunities, Risks, and the Need for a Cyber Strategy

In recent conversations with churches, I'm hearing more about Artificial Intelligence (AI)—not as a distant trend, but as a tool pastors, administrators, and volunteers are already using. From drafting newsletters and creating sermon visuals to organizing membership records, AI can help ministries accomplish more with limited time and resources.

The benefits are real—but so are the risks. Concerns about accuracy, bias, and the privacy of sensitive member or donor data are growing. Even more concerning is the rise of AI-enabled scams: emails or text messages that mimic a trusted leader's tone perfectly, deepfake videos that look real, and automated phishing campaigns that are harder than ever to detect.

That's why I encourage every ministry to go beyond simply "using" AI and instead develop a cyber/data strategy. This includes:

- **Setting clear policies** for what information AI tools are allowed to access.
- **Training staff and volunteers** to verify unusual or urgent requests before responding.
- **Keeping systems updated** and limiting access to sensitive data.
- **Pairing strong practices with cyber liability insurance** to help your ministry recover if a breach occurs.

As an agent, I've seen AI make my own work faster and more efficient—but I never skip the human review step. With the right safeguards and insurance coverage, churches can embrace AI's potential while protecting their people, their data, and their mission.

Claim Lessons Learned - From Cybersecurity & AI Incidents

Insurance Board

Crimes related to breaches in Cybersecurity continue to grow, and advances in technology have enabled cyber criminals to become more sophisticated in their tactics. In 2022, according to CISCO, 84% of organizations fell victim to identity-related breaches, with 96% reporting that the breach could have been avoided or minimized by implementing better security measures such as multifactor authentication and strong passwords.

Cyber criminals will either trick victims into disclosing sensitive information such as bank account pin numbers and passwords, or breach computer systems to directly obtain this information without the owner's knowledge or consent. The goal is to steal money directly or obtain information that can be used to easily steal from financial accounts. Participants in our program who are unaware of these tactics remain especially vulnerable.

In a recent claim, someone hacked into the church's bank account and stole more than $46k by making fraudulent ACH transfers. The hacker was able to gain access to the church bank account and was even able to transfer money within the accounts. It was never discovered how the hacker was able to access the church's accounts.

In another claim, the church treasurer's email was hacked, and a false email was created appearing to come from the chair of the trustees. The hacker was then able to access investment accounts and transfer funds without authorization. Emails from several individuals in two organizations were also hacked.

In a third claim, several church members received text messages that appeared to be from their pastor. The text messages requested the members to purchase gift cards and then text the gift card numbers back to the sender. Those who fell for the ruse ended up losing thousands of dollars from the scheme.

Here are common mistakes employees make that can leave organizations vulnerable to a cyber-attack:

- ◊ Opening emails from unknown sources
- ◊ Weak login credentials
- ◊ Lack of effective employee training to identify cyber criminal tactics.
- ◊ Not updating antivirus software
- ◊ Using unsecured mobile devices

Kaspersky Cyber Security offers the following solutions to reduce and/or prevent cyber-attacks:

- ◊ Never open emails from people you don't know, and avoid opening an unknown attachment or link.
- ◊ Employees should use unique passwords and include numbers and symbols for increased security.
- ◊ Change passwords regularly, especially if you suspect that they may have been compromised.
- ◊ Use password managing software for multiple apps, websites, and devices.
- ◊ Limit the accessibility and administrative privileges to company files.
- ◊ Require multi-level sign-offs for payments and other financial transactions to combat CEO fraud.
- ◊ Provide annual security awareness training.
- ◊ Set up automatic system updates and make this a requirement for employees.
- ◊ Never conduct confidential transactions using public WiFi.
- ◊ Make sure devices are password-protected.

As the threat of cybercrime continues to grow, churches and religious organizations must recognize their vulnerability. They will need to make sure they are current on ways to protect their ministries from a cyber event.

Sources:

https://www.kaspersky.com/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability

AI & Your Ministry – Loss Control Risk Factors to Consider in the World of AI

Insurance Board

Artificial Intelligence (AI) is rapidly transforming how ministries operate—from streamlining administrative tasks to enhancing digital outreach. However, along with these benefits come important risk considerations that ministries should address as part of their overall loss control strategy.

One primary concern is data privacy. Many AI tools collect, process, or store sensitive information such as Electronic Tithing details, volunteer background checks, and congregation member records. Ministries must ensure these tools comply with privacy regulations like HIPAA or General Data Protection Regulation (GDPR) and use secure platforms that align with their data protection policies.

Another area of risk is misinformation. Generative AI can create convincing but inaccurate content. Ministries using AI to generate social media posts, newsletters, or educational materials should implement robust review processes to prevent the accidental dissemination of incorrect or misleading information.

Copyright infringement is another emerging issue. AI tools trained on vast amounts of online data can produce images, music, or written content that unintentionally replicate copyrighted material. Ministries using AI-generated content for sermons, videos, or promotional materials should verify that the outputs do not violate intellectual property laws, which could result in costly legal claims.

There are also ethical considerations. AI tools may unintentionally reflect biases present in their training data. Three different types of bias that can be seen:

- ◊ Data Bias - when the information AI needs is limited, it can paint an inaccurate representation of a certain population.
- ◊ Algorithmic Bias - System response has unfair outcomes due to limited input data or partial algorithms.
- ◊ Confirmation Bias - When an AI system places excessive weight on existing patterns or biases within the data.

These biases can lead to discriminatory outputs, particularly in hiring processes or outreach strategies. Ministries must remain vigilant and promote fairness and inclusion in any AI-supported decision-making.

Dependence on AI can also create operational vulnerabilities. Overreliance may reduce critical thinking or lead to gaps in pastoral care if automated systems replace meaningful human interaction. Ministries should ensure that technology enhances—rather than replaces—personal engagement and spiritual support.

Lastly, cyber liability is a growing concern. AI increases the digital footprint of a ministry, which can make it a more attractive target for cyberattacks. Regular cybersecurity training, updated software, and incident response plans are essential safeguards.

As AI becomes more accessible, ministries must stay informed and proactive. Integrating AI responsibly, with a strong loss control mindset, can help ministries embrace innovation while safeguarding their people, purpose, and mission.

INSURANCE BOARD
Partners in Protection

CEO CORNER
TIMOTHY S. HARRIS, CPCU
PRESIDENT AND CEO

This edition of ***The Steward*** focuses on Artificial Intelligence (AI) and Cyber Risk. As the articles highlight, AI can be a very valuable tool. I was, initially, resistant to using AI largely because I thought it was a resource requiring hours of investment to use and, frankly, I simply did not have the bandwidth. One day while an electrician was installing a piece of equipment in my home, I got a brief glimpse of how AI could be helpful. After installing the equipment, the electrician needed to connect it to Wi-Fi to get it to interface with my cellphone. We tried several times using guidance from the manual yet continued to experience difficulty. The electrician regularly worked with his son and nephew who assisted him on projects. Watching the two of us struggle to figure things out, his son promptly pulled up AI on his phone and asked it to troubleshoot the problem. After a few inputs back and forth, AI directed him to another app (we were using the app provided on the packaging, which was specifically for installers to use during installation, not realizing there was another app necessary to operate the unit). From there, he was able to solve the problem in a couple of minutes. Unlike simply searching the internet, AI can both ask and be asked questions to clarify the information being sought.

Experiencing that, and hearing from other respected colleagues who were already using AI, I realized AI could be an effective tool to solve problems, assist with projects, and to promote efficiencies. That said, ***The Steward*** articles also emphasize the need for due diligence and review prior to simply accepting a result from AI as being correct or factual.

Along with AI, the articles tackle the topic of cyber risk, including cyber theft. As this edition points out, almost everyone has encountered cyber theft in some form or fashion, from attempted phishing or spoofing, to hacking, to social engineering, and others. The key to mitigating cyber security risk is through the layering of protections such as strong passwords and multi-factor authentication. And, often, a simple phone call to a known source can verify information and prevent traps often set by cyber thieves through email. Regular training of employees using examples of cyber risk is critical to heightening awareness of the various techniques being employed today by cyber criminals.

Cyber crime can also be an important issue during climate-inspired severe weather events. Cyber criminals often prey on victims of natural disasters, including in the wake of severe weather. Healthy suspicion can be a great first-alert to mitigating cyber related risk.