The Briefing

July 13, 2026

Updates and analysis from the Government & Leadership Office of the Venice Area Chamber of Commerce

INSIDE

Our Demystifying AI initiative
Week 5 of 6

Hot Topic – "The Drone Economy"

Did You Know?

Candidates TAB

Demystifying AI Week 5 of 6

AI Risk, Ethics, Data Privacy

&

Governance

What We Cover This Week:

Understanding AI's capabilities is only half the leadership equation. This session addresses the full risk landscape: where AI can fail your business, how to protect customer and employee data, what cybersecurity threats AI enables, and how to navigate the evolving regulatory environment as a responsible business leader.

1. Learning Objectives

- Identify the primary categories of AI risk — bias, hallucination, over-reliance, and reputational harm — and understand how each manifests in a business context
- Understand the data privacy principles most relevant to small businesses using AI tools, including basic data stewardship practices
- Recognize AI-enabled cybersecurity threats — including deepfakes and AI-powered phishing — and understand defensive countermeasures
- Apply the principles of ethical AI — transparency, fairness, and accountability — to your own organization's AI use
- Understand the current state of U.S. federal and Florida state AI regulatory guidance and its implications for small business compliance

2. Session Overview

Every powerful tool carries risk, and AI is no exception. The most effective executives are not those who avoid risk — they are those who understand it clearly enough to manage it deliberately. This session is designed not to alarm, but to equip. The risks of AI adoption are real and manageable. The risk of uninformed AI adoption — of deploying tools without understanding their limitations, data practices, or governance requirements — is considerably greater than the risk of thoughtful, informed adoption.

By the end of this session, you will have a clearer picture of what your business's actual AI risk profile looks like, and a practical framework for managing it. We will also complete the AI Risk Assessment Checklist together, which you will carry into Week 6 as a foundation for your AI strategy.

3. Core Content Areas

a. Understanding AI Risk for Businesses

Bias: AI systems learn from data — and if that data reflects historical biases, the AI system will replicate and potentially amplify those biases. In a hiring context, an AI trained on historical hiring decisions may systematically disadvantage qualified candidates from underrepresented groups. In a lending context, it may replicate historical patterns of demographic discrimination. For business leaders, the key principle is: AI does not create unbiased decisions simply because it is algorithmic. Human oversight of AI-assisted decisions in high-stakes domains — hiring, lending, pricing, service access — is an ethical and often legal requirement.

Hallucinations: AI language models can generate responses that are confident, fluent, and completely wrong. This phenomenon — called "hallucination" — occurs when an AI generates plausible-sounding text that is factually inaccurate or entirely fabricated. Business leaders have faced reputational harm from publishing AI-generated content containing false statistics or fabricated citations. The mitigation: treat all AI factual claims as unverified until confirmed against authoritative sources. Never publish AI-generated factual content without human fact-checking.

Over-Reliance: As AI tools become more capable and more embedded in business workflows, there is a real organizational risk of teams deferring to AI outputs without applying human judgment. This is particularly dangerous in domains where AI errors have significant consequences: medical advice, legal interpretation, financial projections, and customer-facing communications. Establish explicit policies specifying which AI outputs require human review — and hold those policies.

Pro Tip

One of the most effective risk management practices for small businesses using AI is the "human in the loop" rule: for any AI output that will be seen by a client, customer, or regulatory body, or that will influence a significant business decision, a qualified human reviews it before it goes out or is acted upon. This single practice mitigates the majority of AI-related business risk.

b. Data Privacy Essentials

When you or your team enter information into an AI tool, that information may be used to train future AI models, accessed by vendor support staff, or stored in ways that are not immediately obvious from the user interface. Understanding what data you are sharing with AI platforms — and what your obligations to clients and employees are regarding that data — is a foundational business responsibility.

Key principles for small business AI data privacy:

- Never enter personally identifiable information (PII) of clients or employees into a public AI platform unless you have reviewed the vendor's data processing agreement and confirmed appropriate protections

- Health information (PHI) subject to HIPAA, financial account data, and Social Security numbers should never be entered into AI platforms not explicitly HIPAA or financially compliant
- Florida's data privacy legislation (Florida Digital Bill of Rights) established Florida consumer rights regarding personal data — including data shared with or processed by AI systems. Florida businesses may have compliance obligations under this legislation.
- Enterprise versions of AI platforms (ChatGPT Enterprise, Microsoft Copilot for M365, Google Workspace AI) typically include data protection agreements that prevent your data from being used for model training — these are meaningfully different from free consumer versions

c. Cybersecurity & AI — The Evolving Threat Picture

AI is simultaneously a powerful defensive cybersecurity tool and a capability that malicious actors are deploying against businesses. Business leaders need to understand both dimensions.

AI-enabled threats your business may face:

- **AI-powered phishing:** Attackers now use AI to generate personalized, convincing phishing emails at scale — eliminating the grammatical errors and generic language that historically made phishing attempts easier to detect. Train your team to treat any unexpected email requesting credentials, wire transfers, or sensitive data with heightened skepticism, regardless of how professional it appears.
- **Deepfakes:** AI can now generate convincing audio and video of real people saying things they never said. Business executives have been impersonated in fraudulent video calls requesting wire transfers. Establish verification protocols for any communication requesting financial action or sensitive data — verify through a second, independent channel.
- **Social engineering at scale:** AI enables attackers to conduct research on targets and craft highly personalized manipulation attempts that exploit public information about your business, your team, and your relationships.

AI-powered defenses: Many cybersecurity platforms now incorporate AI for real-time threat detection, anomaly identification, and automated incident response. For small businesses, AI-enhanced security tools from platforms like **CrowdStrike**, **Microsoft Defender**, and **SentinelOne** bring enterprise-grade protection to small and medium size business price points.

d. Ethical AI Practices for Business Leaders

Ethical AI is not an abstract philosophical concern — it is a practical business responsibility with real implications for your reputation, your customer relationships, and your legal exposure. Three core principles apply to every business using AI:

- **Transparency:** Be honest with customers and employees about when and how AI is used in your business. When a customer is interacting with a chatbot rather than a human, they should know. When AI has influenced a significant decision affecting an employee or customer, that should be documentable and explainable.
- **Fairness:** Regularly review AI-assisted decisions for patterns of disparate impact across demographic groups. This applies to hiring, pricing, service availability, and any other domain where AI influences outcomes for people.
- **Accountability:** AI does not eliminate organizational accountability — it shifts the accountability to the humans who designed, deployed, and oversee it. Your business is responsible for the outcomes of AI tools you deploy, even when those outcomes are unexpected. Document AI use cases, review processes, and governance decisions as you would any significant business practice.

e. The Regulatory Landscape — What Business Leaders Need to Know in 2026

AI regulation at both the federal and state level is evolving rapidly. The regulatory landscape for small businesses as of 2026 is characterized by emerging frameworks rather than comprehensive mandated compliance — but that is changing.

At the **federal level**, the FTC has issued guidance on deceptive uses of AI in advertising and consumer-facing communications, and sector-specific regulators (HHS for healthcare, CFPB for financial services) have issued AI-specific guidance within their domains. The AI Executive Order landscape has shifted with changing administrations, but the underlying principles of safety, transparency, and accountability remain foundational.

At the **Florida state level**, the Florida Digital Bill of Rights (effective 2024) established consumer privacy rights for Floridians — including rights relevant to AI-driven profiling and automated decision-making — for businesses meeting certain revenue and data thresholds. Business leaders should consult legal counsel to determine whether their organizations are subject to this legislation's requirements.

The practical guidance for small business leaders: stay informed, document your AI practices, prioritize transparency with customers, and establish a relationship with a legal advisor familiar with AI compliance so you are not navigating regulatory changes in isolation.

4. AI Risk Assessment Checklist

☑ **AI Risk Readiness Checklist – Audit Your Organization's Current Position**

Risk Area

In Place?

Priority

AI Acceptable Use Policy documented and distributed to all staff

□ Yes □ No

High

List of approved AI tools maintained and communicated to staff

□ Yes □ No

High

Policy in place prohibiting entry of PII/PHI into public AI platforms

□ Yes □ No

High

Human review required for AI-generated external communications

□ Yes □ No

High

Human review required for AI-assisted HR decisions (hiring, performance)

□ Yes □ No

High

Staff trained to recognize AI-powered phishing and social engineering

□ Yes □ No

High

Verification protocol in place for wire transfers and financial requests received via email or phone

□ Yes □ No

High

Data Processing Agreements reviewed for all AI vendors used

□ Yes □ No

Medium

AI use cases documented for compliance and audit purposes

□ Yes □ No

Medium

AI governance reviewed by legal counsel or HR professional within past 12 months

□ Yes □ No

Medium

Policy for AI transparency/disclosure with customers established

□ Yes □ No

Medium

Incident response process defined for AI-related errors or breaches

□ Yes □ No

Medium

5. Week 5 Key Takeaways

- AI risks — bias, hallucinations, over-reliance, and data exposure — are real, manageable, and far less dangerous when understood clearly than when ignored
- Data privacy is a non-negotiable AI governance requirement; never enter sensitive client, employee, or business data into public AI platforms without appropriate data protection agreements
- AI is actively being weaponized by cybercriminals — staff training and verification protocols are your first line of defense against AI-enabled fraud and social engineering
- Ethical AI is not idealism — it is practical risk management with direct implications for reputation, customer trust, and regulatory compliance

6. Action Items — Complete Before Week 6

✍ Action Items

1. **Complete the AI Risk Assessment Checklist** for your organization. Be honest.
2. **Conduct a 15-minute cybersecurity briefing with your team** focused specifically on AI-powered phishing and deepfake fraud. Use your favorite AI to help generate a brief, specific, role-appropriate briefing script if you need one.
3. **Review the data practices of two AI tools** your business currently uses or is evaluating. Find the vendor's privacy policy or data processing agreement and identify: (a) whether your data is used for model training, and (b) how long your data is retained.

7. Discussion Questions

Discussion Questions

1. Of the risk categories covered — bias, hallucination, data privacy, cybersecurity, and regulatory compliance — which one feels most immediately relevant and concerning for your specific business? What specific scenario worries you most?

2. How confident are you that your team currently understands the difference between the data protections offered by free AI tools and enterprise AI tools? What would it take to make that distinction organizational knowledge?

3. If a significant AI-related error occurred in your business tomorrow — a hallucinated fact published externally, a data privacy incident, or a deepfake fraud attempt — do you have a response process? If not, who in your organization should own building one?

Looking Ahead to Week 6:

We have built the foundation (Weeks 1–2), explored the applications (Weeks 3–4), and confronted the risks (Week 5). In our final session, we bring it all together into something you can actually use: a personalized AI strategy framework and 90-day action plan that reflects your unique business, your goals, and your appetite for AI adoption.

Hot Topic – The Drone Economy – Nicolas Liberoni

The world is vastly different from what it was five years ago. An often-overlooked facet of the American economy is the defense driven economy. The United States has the largest defense budget in the world by a wide margin, spending nearly $1 trillion annually. In fact, the United States spends as much money on defense as the next six countries combined.

Beyond the various debates about how much money goes to defense, the sector sometimes produces innovations that have uses beyond the military. Examples of military inventions that later became mainstream include GPS, the microwave, and the ambulance.

More recently, drones have become an increasingly important part of warfare. In the ongoing Russia-Ukraine war, both militaries have struck infrastructure in the opposing nation through drone warfare. Ukraine has seen growth in domestic low-cost drone production and has used this sector to target Russian oil refineries.

Domestically, drone technology is now being used to provide services. Florida law enforcement and fire service agencies use drones to gather information and improve public safety during emergencies. Drones can provide law enforcement officers with information about suspects and assist in solving missing persons cases. Additionally, law enforcement, fire, and emergency management can use drones to survey land after devastating natural disasters such as tornadoes, wildfires, and hurricanes.

Large companies are experimenting with drone technology as well. Tech giant Apple has reportedly explored using drones to update its geospatial data and improve its Apple Maps service. Uber, UPS, DHL, and JD.com have also tested or deployed drones to make small deliveries, which could help speed up package transportation.

Other companies, such as ZenaTech, SkySpecs, and Cyberhawk, use drones to inspect infrastructure including wind turbines, gas pipelines, and other critical assets. This allows for quicker inspections and reduces the need for humans to perform potentially dangerous tasks. These companies are part of the growing drone-as-a-service (DaaS) industry.

According to PR Newswire, the DaaS industry could grow from approximately $8–10 billion in 2025 to more than $80 billion within the next decade. As drone technology continues to improve and becomes more cost-effective while nations increase defense spending, the drone industry and DaaS sector could reshape the economy and the way people live.

Did You Know?

The VACC, in early support of the planned candidate forum slated for July 29th, invited candidates to come into the Chamber for a quick and easy "Get to Know You" video. Several candidates took advantage of the opportunity during a two-week period. The videos are now part of candidate information that you can locate on a tab on our website. Several other candidates provided information and links to their campaign information. We hope you find this information useful during this busy election season.

CANDIDATE FORUM

Meet the Candidates Tab