Entrepreneur & Family BUSINESS COUNCIL

AI Transformation

Responsible AI Use

Jon Pisani

PSM Partners

jpisani@psmpartners.com

Presenter Intro

Jon Pisani is a Solution Architect at PSM Partners with close to two decades of cybersecurity experience. Jon focuses his efforts on helping organizations and business owners identify gaps within their infrastructure and design roadmaps to allow businesses to smoothly and efficiently upgrade.

Organizational Use of AI

How is organizational use of AI different than personal use?

What are some different considerations?

PSM
TECHNOLOGY | TALENT

Public vs. Private Platforms

- **Public Platforms**
  - “Free”
  - Users become the products
  - Data becomes part of the training algorithms
- **Private Platforms**
  - Paid
  - More user protection
  - Data often not used for platform training*

“If you’re not paying for the product, then you are the product”

(The Social Dilemma)

*Always check the Terms and Conditions for specific details

PSM
TECHNOLOGY | TALENT

Personal vs. Business Use

Separation is key!

- ❌ Avoid using public or personal accounts for work
- ✅ Use a business account for business-related work
    - Better user / data protection
    - Better business protection
    - Better data governance
    - Better security

What happens when an employee leaves, but their business-related AI work is stored on their personal account?

PSM
TECHNOLOGY | TALENT

Common AI Challenges

Data Quality

End-User Reliance

Security Risks

Regulatory Challenges

PSM
TECHNOLOGY | TALENT

Data Quality

Inaccurate or biased data

- Large quantities of individuals feeding bad information into the platform
- Platforms rely on human intervention to assist with identification of biased data
- Biased data creates poor responses from the AI platform

No Accountability

- Platforms allow for anonymous or near anonymous interactions
- Difficult to determine the source of misinformation
- Using poor or biased data can lead to liability issues

End-User Reliance

User Understanding

- Atypical for end-user training to be provided during corporate onboardings
- Misconceptions regarding what AI can be used for and how the platform operates
- Users can develop an overreliance on AI platforms for critical tasks

Ethical Concerns

- Use of AI Platforms can lead to unethical interactions (over billing, info dissemination, etc.)
- Protected information can become exposed when utilizing public platforms
- Lack of human oversight for how users interact with the platform

PSM
TECHNOLOGY | TALENT

Security Risks

Data Breaches and Privacy Concerns

- Public AI platforms build on data being fed into the platform
- Sensitive data exposure is a real concern as AI platforms are asked to analyze data
- Regulatory compliances (HIPAA / GDPR / NERC) prevent protected information from being reviewed by public AI platforms

Vulnerability to Cyber Attacks

- Public AI platforms are highly targeted arenas
- Cyber criminals could access algorithmic data used by AI to make decisions

PSM
TECHNOLOGY | TALENT

Regulatory Challenges

AI Regulations

- Constantly evolving landscape
- Difficult to predict future trends
- Future trends require unforeseen governance techniques

Accountability

- Is the end user liable if misinformation produces negative outcomes?
- Will data misuse lead to limitations in the platform?
- Are there legal consequences for using AI in the enterprise?

Next Steps

Understand what your users are doing.

- Audit your company’s AI use.
- How are your people already using AI?
- What platforms or tools are being used, and how are they being used?

Define what they should be doing.

- Make a plan forward.
- Consult with IT and company leadership.
- Develop an appropriate AI use policy.

Get everyone on the same page.

- Educate users on responsible AI use and best practices.
- Enforce constraints so that AI platforms and tools can be used safely and effectively.

PSM
TECHNOLOGY | TALENT

Presenter Contact Info

Jon Pisani

PSM Partners

jpisani@psmpartners.com