SHARPE CONSULTING LLC

"THE ROLE OF AI BOMS IN PROVIDING THE TRANSPARENCY NECESSARY TO FOSTER THE SAFETY AND SECURITY OF AI AND OUR CRITICAL INFRASTRUCTURE."

6 May 2024

Alex Sharpe
Principal

Agenda

- Why
  - Risk Assessment on the front end
  - Maintenance and Monitoring along the way
  - Response and Mitigation
- What history shows us.
- A Nutrition label for AI
- Dimensions to Consider
- Cautions

Slides are designed to live past the webinar - feel free to share.
Please site the source.

Alex Sharpe
“Sharpe like a knife”™

alex@Sharpe42.com

www.linkedin.com/in/alex-sharpe-3rd/

- Big 4 Trained Management Consultant with Real World Operational Experience
- Advisor, Practitioner, Speaker, Author
- 35+ years Cybersecurity
- 25+ years Digital Transformation

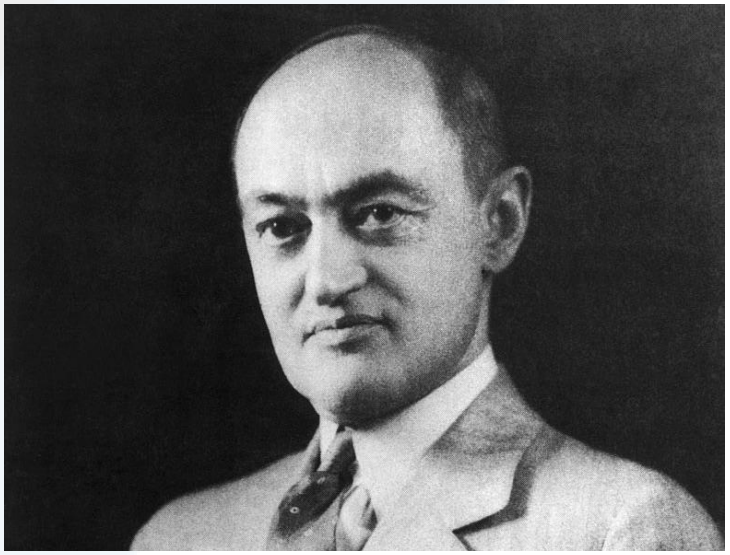
“Value Creation While Managing Cyber Risk”™

Father of Modern Innovation

“Innovation is new combinations of old ideas.”

Lessons learned and advances from other areas.

Good ideas are often behind a few bad one.



Joseph Schumpeter

Nutrition Label

Food labeling decreased:

- Calorie intake by 6.6%
- Total fat by 10.6%
- Other unhealthy by 13.0%
- Sodium by 8.9%
- Artificial trans fat by 64.3%

Increased vegetable consumption by 13.5%

Transparency benefits the consumer but costs the seller

New Label

Nutrition Facts

8 servings per container

Serving size **2/3 cup (55g)**

Amount per serving

Calories **230**

	% Daily Value*
Total Fat 8g	**10%**
Saturated Fat 1g	**5%**
Trans Fat 0g	
Cholesterol 0mg	**0%**
Sodium 160mg	**7%**
Total Carbohydrate 37g	**13%**
Dietary Fiber 4g	**14%**
Total Sugars 12g	
Includes 10g Added Sugars	**20%**
Protein 3g	
Vitamin D 2mcg	10%
Calcium 260mg	20%
Iron 8mg	45%
Potassium 240mg	6%

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

Dimensions to Consider

Not all food labels are created equal; neither should AI BOMs

1. Service Delivery Model
2. Modality
3. Use Case
4. Mitigation

Service Delivery Model

1. Home Grown
2. Service (e.g., ChatGPT)
3. Embedded (e.g., Co-Pilot)

Modality

- Text
- Voice
- Video
- Image(s)
- Experiential
- Decision Support
- Diagnosis
- Etc…

Use Case

- Not all use cases are created equal
- Impact Human Life
- Decision Support
- Medical
- Bias

Mitigation/ Incident Response (IR)

- All efforts to:
  - Confine Blast Radius
  - Detect quickly
  - Respond faster
- Can you mitigate?
- How to mitigate?

Two quotes

”…when it’s wrong, it’s wrong in ways that no human would ever be.”

Dr. A. Prabhakar

Director of the Office of Science and Technology Policy (OSTP), Director DARPA (former)

“The only thing growing faster than the adoption of AI is the number of long-term AI experts.”

Anonymous

Some Resources

- **International: Establishing GRC practices for AI** DATA PROTECTION LEADER, Volume 6, Issue 1, January 2024, dataguidance.com
- **AI Resilience: A Revolutionary Benchmarking Model for AI Safety**, https://cloudsecurityalliance.org/artifacts/ai-resilience-a-revolutionary-benchmarking-model-for-ai-safety
- **AI Resilience: A Revolutionary Benchmarking Model for AI Safety,** https://cloudsecurityalliance.org/artifacts/ai-resilience-a-revolutionary-benchmarking-model-for-ai-safety
- **CISA Roadmap for AI**, https://www.cisa.gov/resources-tools/resources/roadmap-ai

Do not hesitate to call

Alex Sharpe

“Sharpe like a knife”

Sharpe Consulting LLC

www.SharpeLLC.com

alex@SharpeLLC.com

Free Consultation

We promise you two good ideas

SHARPE CONSULTING LLC

BIG ENOUGH TO DO THE JOB
AGILE ENOUGH TO DO IT *RIGHT*

THANK YOU.