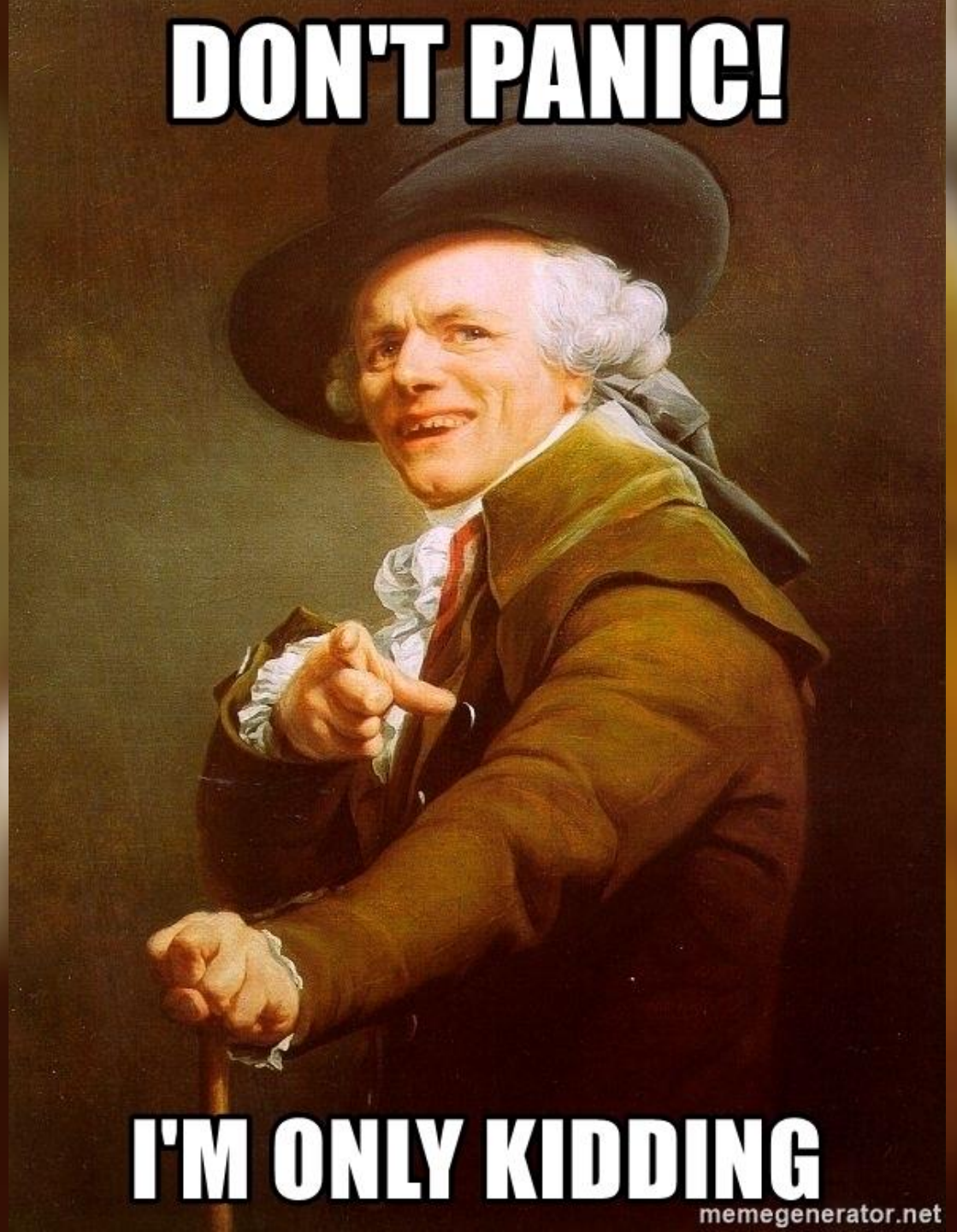
Boardroom Intelligence: AI Strategies for Winning in the Boardroom

James R. McQuiggan, CISSP

How to Discuss AI with Leadership?

Please sir, can I have AI please?

Thank you
for coming to my
TED talk.


DON'T PANIC!
I'M ONLY KIDDING
memegenerator.net

got AI?

James R. McQuiggan, CISSP,SACP

Security Awareness Advocate, KnowBe4 Inc.

Producer, Security Masterminds Podcast

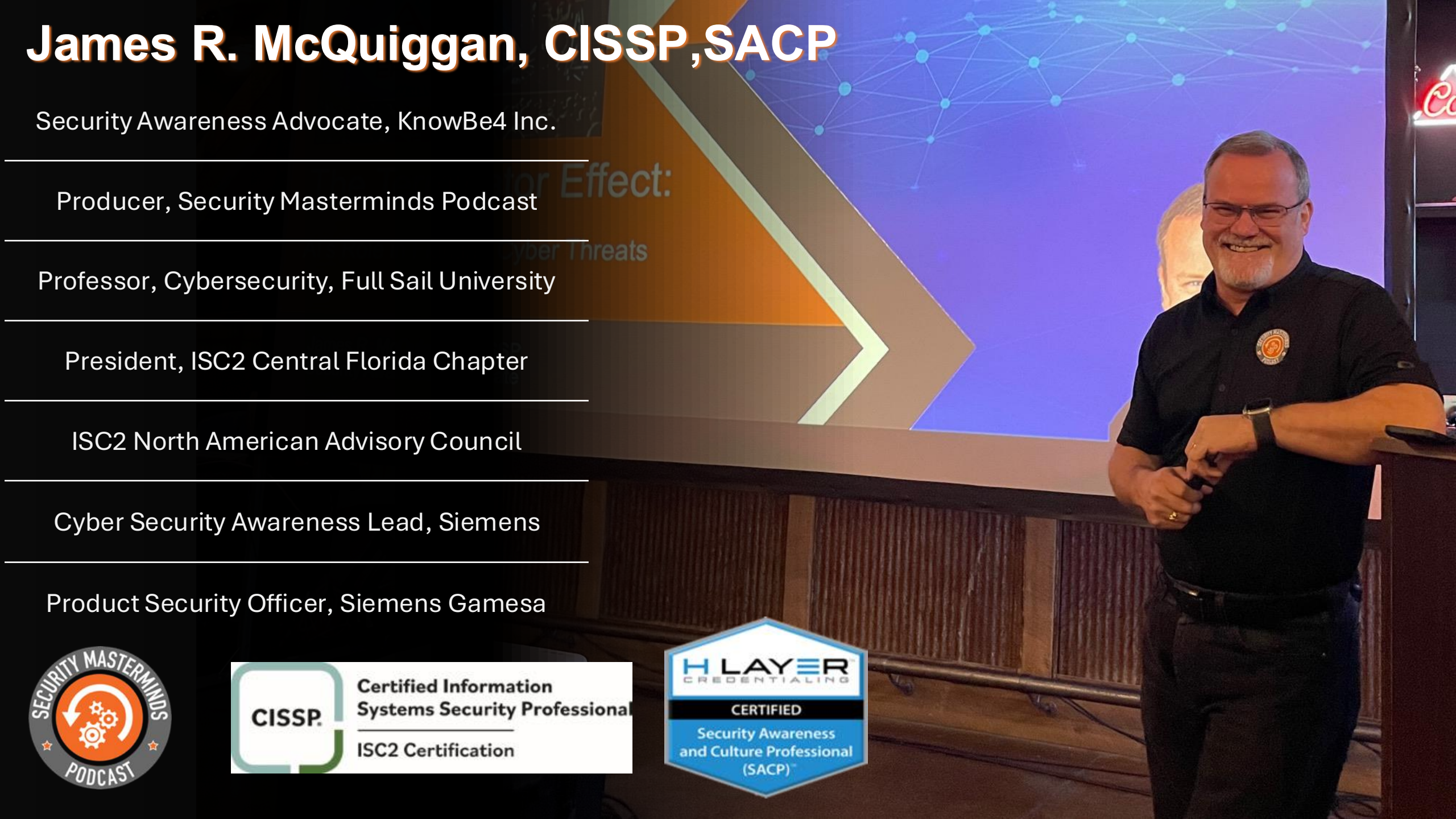
Professor, Cybersecurity, Full Sail University

President, ISC2 Central Florida Chapter

ISC2 North American Advisory Council

Cyber Security Awareness Lead, Siemens

Product Security Officer, Siemens Gamesa



SECURITY MASTERMINDS PODCAST

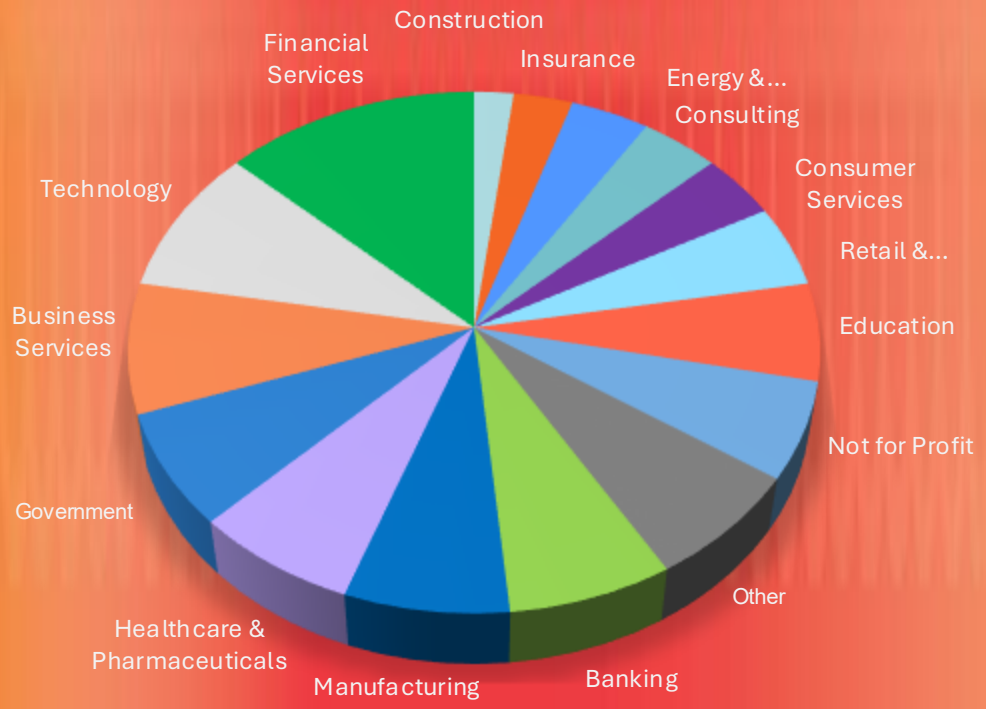
CISSP
Certified Information Systems Security Professional
ISC2 Certification

H LAYER CREDENTIALING
CERTIFIED
Security Awareness and Culture Professional (SACP)

Over

70,000

Customers



About KnowBe4

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

Our mission

To help organizations manage the ongoing problem of social engineering

We do this by

Enabling employees to make smarter security decisions everyday


SECURITY
AWARENESS

AI & The World

AI & You

AI & The Boardroom

Wrap - up

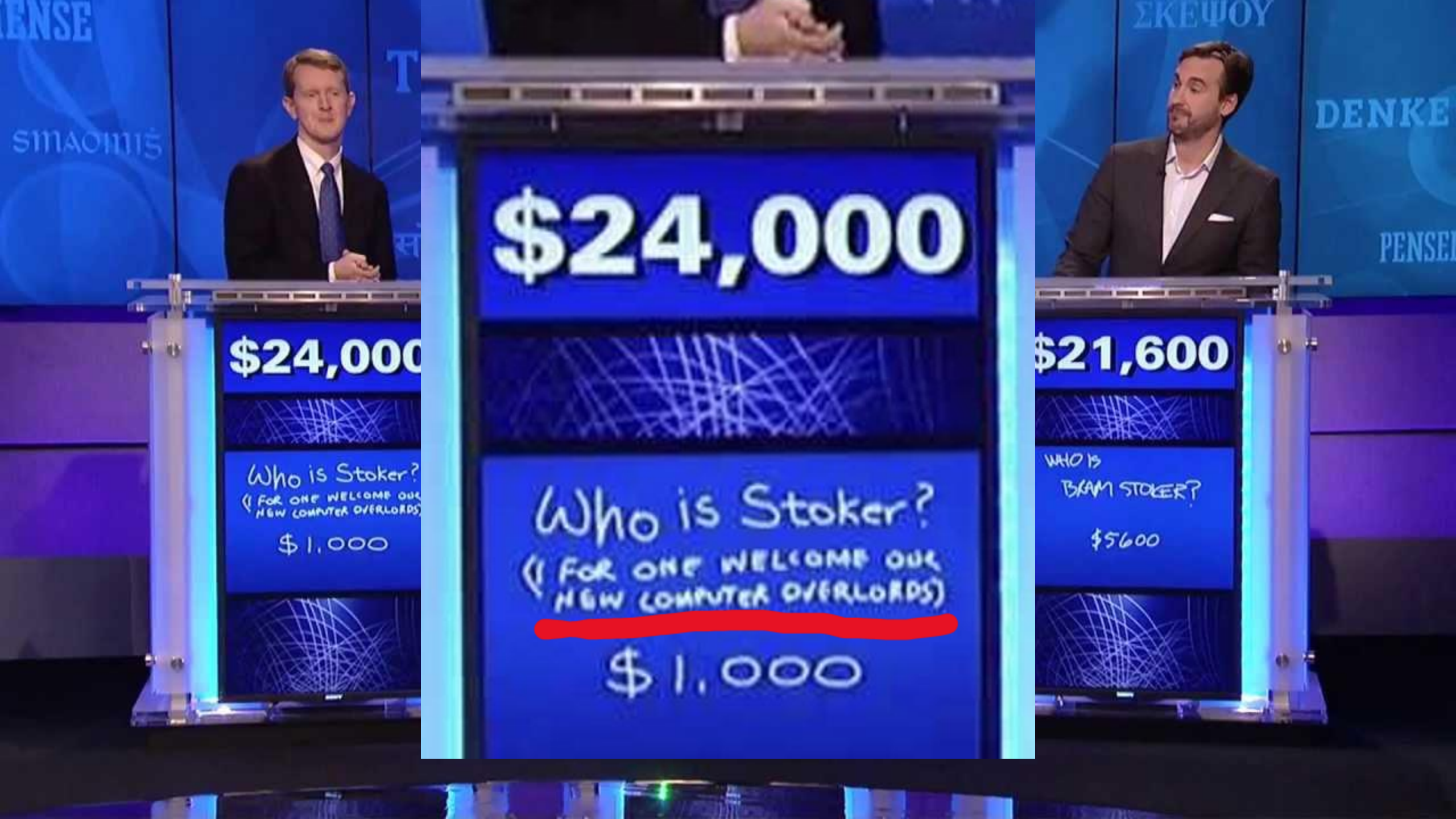
AI & The World

AI & You

AI & The Boardroom

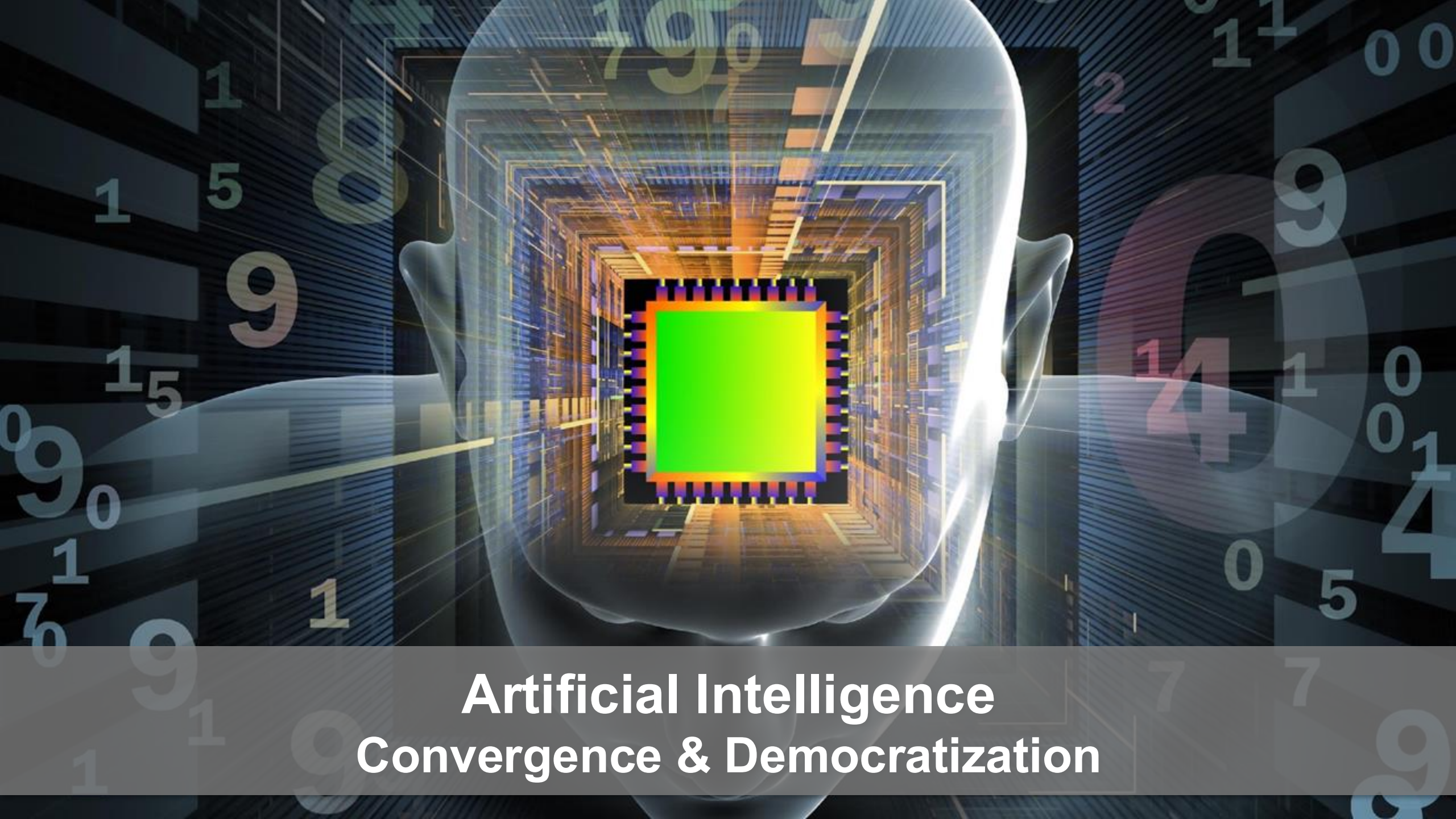
Wrap - up


Panasonic


$24,000
Who is Stoker?
((FOR ONE WELCOME OUR NEW COMPUTER OVERLORDS)
$1,000
$24,000
Who is Stoker?
$1,000
$21,600
WHO IS BRAM STOKER?
$5600

“AI is the new electricity”

- Andrew Ng, Stanford Professor



Artificial Intelligence
Convergence & Democratization

Common AI Risks

Biases and unfair outcomes

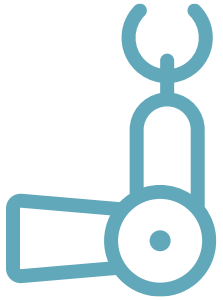
AI models can inherit and amplify existing societal biases if the training data is not representative.

Lack of transparency

The complexity of some AI models makes it hard to explain their predictions.

Security vulnerabilities

Adversaries could exploit vulnerabilities in AI systems for malicious purposes.



Job displacement

AI automation may displace many existing jobs and disrupt the workforce.

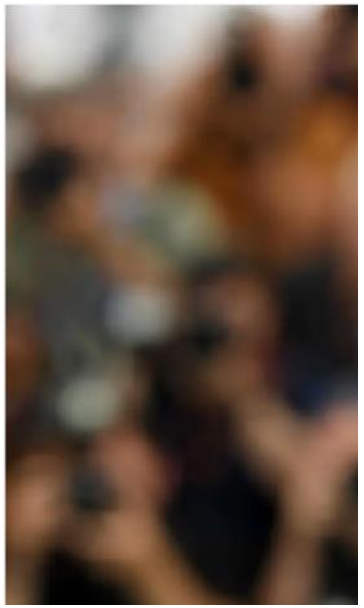
While AI promises many benefits, managing risks like these will be critical as adoption grows.

“A” AI Playbook for Cybercriminals

AI Infrastructure Attacks	Zero Click Worm (GenAI)	ASCII Attacks	RAG Exploits	Hallucinations / Biases
Polymorphic Malware	Automated Attacks	Password Cracking	Data Poisoning	Prompt Injection
Malicious AI LLMs	Synthetic Media / Identities	AI Phishing / Spear Phishing	Ransomware AI	Shadow AI

Deepfake Videos

A Deep Fake
Plan, But the
The actor warned his Instagram
By **Kevin Hurler** Published October 2,



SECUREWORLD

EVENTS NEWS WEBCASTS

ONLINE SCAMS

Hong Kong Clerk Defrauded of $25 Million in Sophisticated Deepfake Scam

By Drew Todd

Read more about the author

TUE | FEB 13, 2024 | 4:27 AM PST

As artificial intelligence continues advancing at a rapid pace, criminals are increasingly using AI capabilities to carry out sophisticated scams and attacks. Technologies that synthesize realistic fake media, known as deepfakes, are among the newest tools being deployed to enable fraud.

A finance clerk working at a Hong Kong branch of a large multinational corporation recently fell victim to an elaborate scam utilizing deepfake technology to impersonate senior executives and swindle more than $25 million, according to reports.

...

hat's Not Taylor Swift Promoting Le Creuset

our social media feed, we can confirm that it is a
ted through #AI.
gbird technology announced at #CES2024, is
u with tools to tell you about what's real and

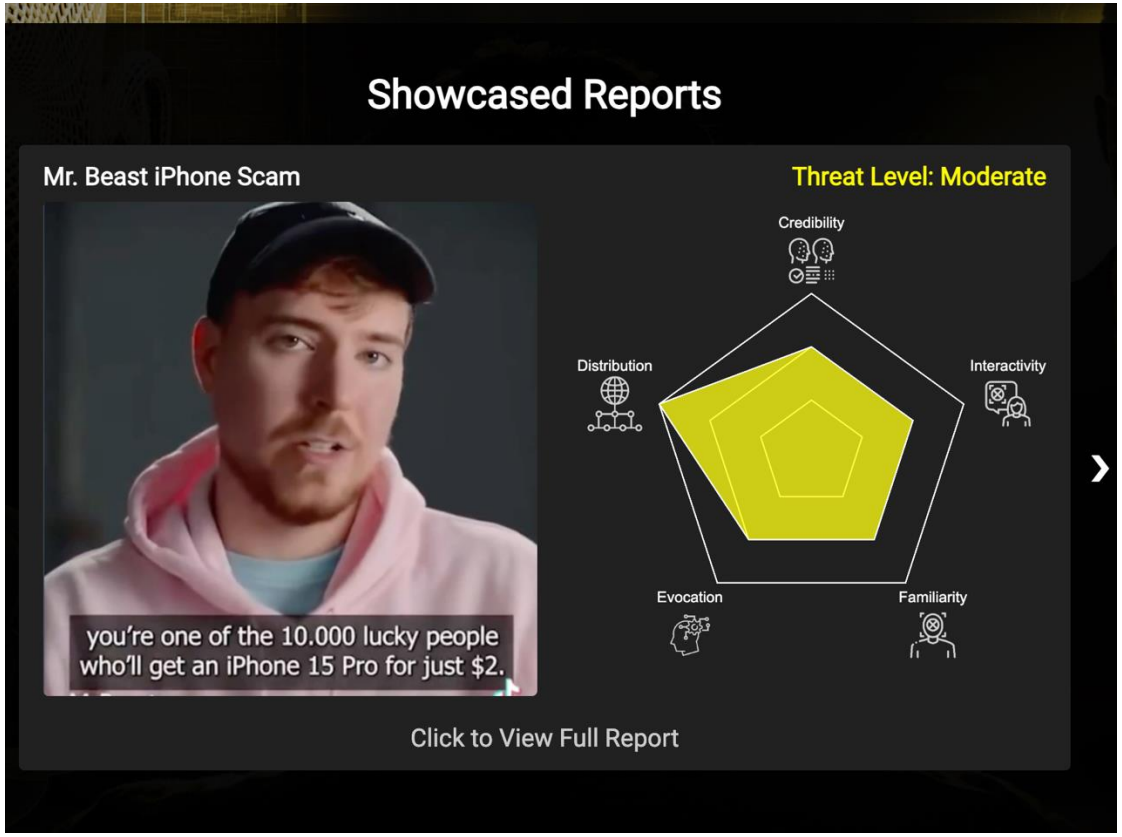
8O6ybL


KnowBe4
HeyGen


KnowBe4
Ahora podemos ir un paso más allá, ya que he creado mi propio Avatar

Real-Time Detection…

- Working on it



truepic

Pindrop

DEEPFAKE DASHBOARD™

DEEPSAFE

siddharthksah / DeepSafe Public

Daisy-Zhang / Awesome-Deepfakes-Detection Public


An Algo-rithim

AI & The World

AI & You

AI & The Boardroom

Wrap - up

Where are you with AI?

AI is part of our culture, our office and we welcome our new AI Overlords

Some integration, using GenAI and some AI in cybersecurity, and/or limited to the business

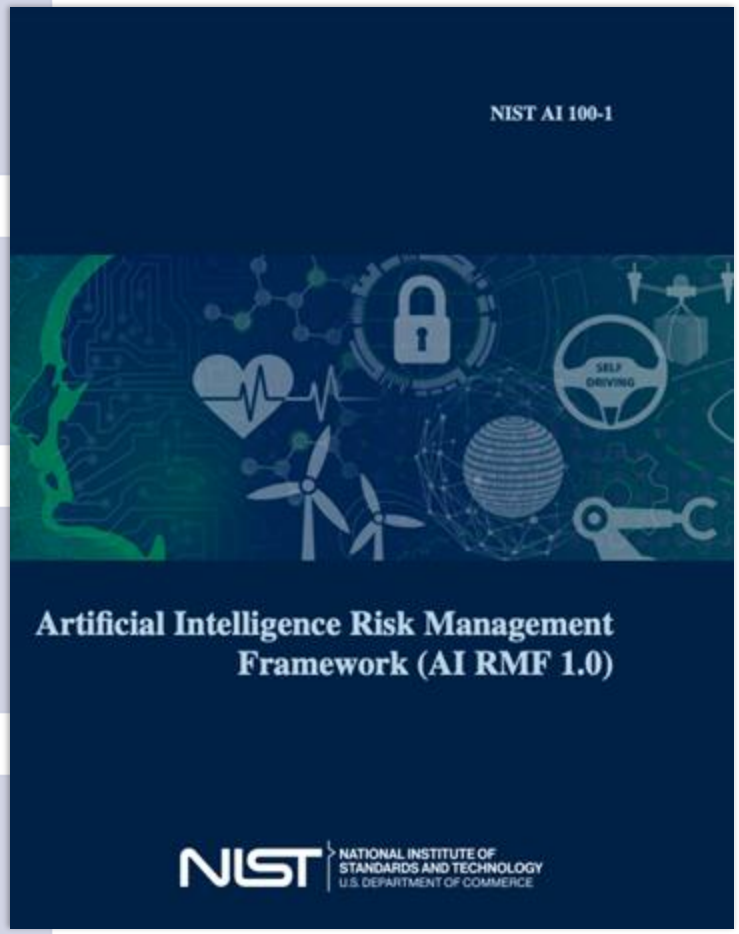
Nope, No thanks Arnold.

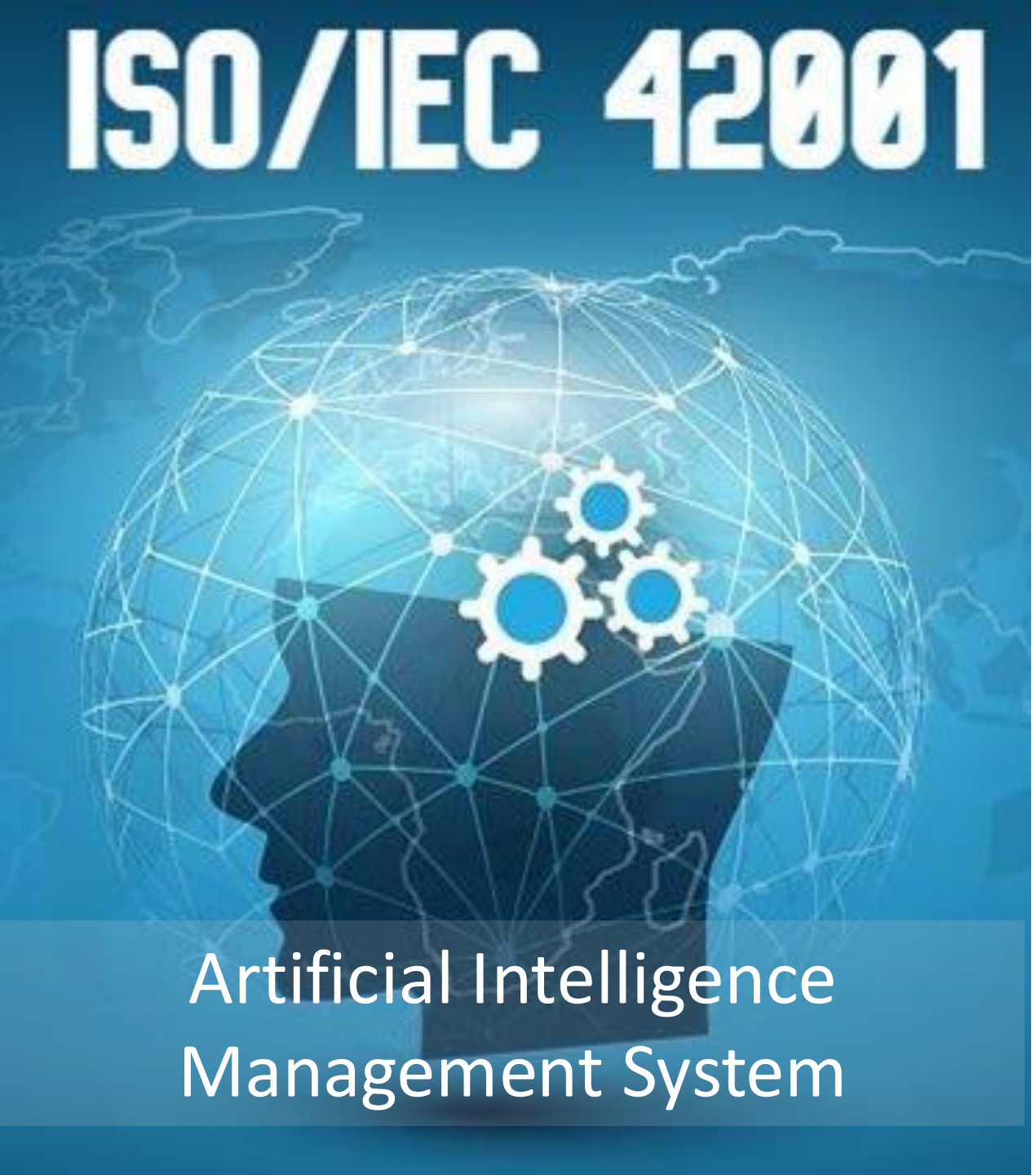
What are some ways that your organization is using AI and what have been the benefits?

AI RISK Frameworks

Securing and Reducing Risk with AI

Govern	Establishing clear guidelines and policies
Map	Identifying and understanding the contexts, capabilities, and risks associated
Measure	Implementing processes to handle identified risks.
Manage	Employing tools and methodologies to analyze, assess, and monitor AI risks





ISO 42001:2023 – AIMS

- Detailed Governance framework
- Certifiable
- Trust and Transparency in AI Development
- Ethical Principles & Risk Management
- Human-Centric AI and Competitive Advantage

OWASP Top 10 for LLM Applications

LLM01

Prompt Injection

This manipulates a large language model (LLM) through crafty inputs, causing unintended actions by the LLM. Direct injections overwrite system prompts, while indirect ones manipulate inputs from external sources.

LLM02

Insecure Output Handling

This vulnerability occurs when an LLM output is accepted without scrutiny, exposing backend systems. Misuse may lead to severe consequences like XSS, CSRF, SSRF, privilege escalation, or remote code execution.

LLM03

Training Data Poisoning

Training data poisoning refers to manipulating the data or fine-tuning process to introduce vulnerabilities, backdoors or biases that could compromise the model's security, effectiveness or ethical behavior.

LLM04

Model Denial of Service

Attackers cause resource-heavy operations on LLMs, leading to service degradation or high costs. The vulnerability is magnified due to the resource-intensive nature of LLMs and unpredictability of user inputs.

LLM05

Supply Chain Vulnerabilities

LLM application lifecycle can be compromised by vulnerable components or services, leading to security attacks. Using third-party datasets, pre- trained models, and plugins add vulnerabilities.

LLM06

Sensitive Information Disclosure

LLMs may inadvertently reveal confidential data in its responses, leading to unauthorized data access, privacy violations, and security breaches. Implement data sanitization and strict user policies to mitigate this.

LLM07

Insecure Plugin Design

LLM plugins can have insecure inputs and insufficient access control due to lack of application control. Attackers can exploit these vulnerabilities, resulting in severe consequences like remote code execution.

LLM08

Excessive Agency

LLM-based systems may undertake actions leading to unintended consequences. The issue arises from excessive functionality, permissions, or autonomy granted to the LLM-based systems.

LLM09

Overreliance

Systems or people overly depending on LLMs without oversight may face misinformation, miscommunication, legal issues, and security vulnerabilities due to incorrect or inappropriate content generated by LLMs.

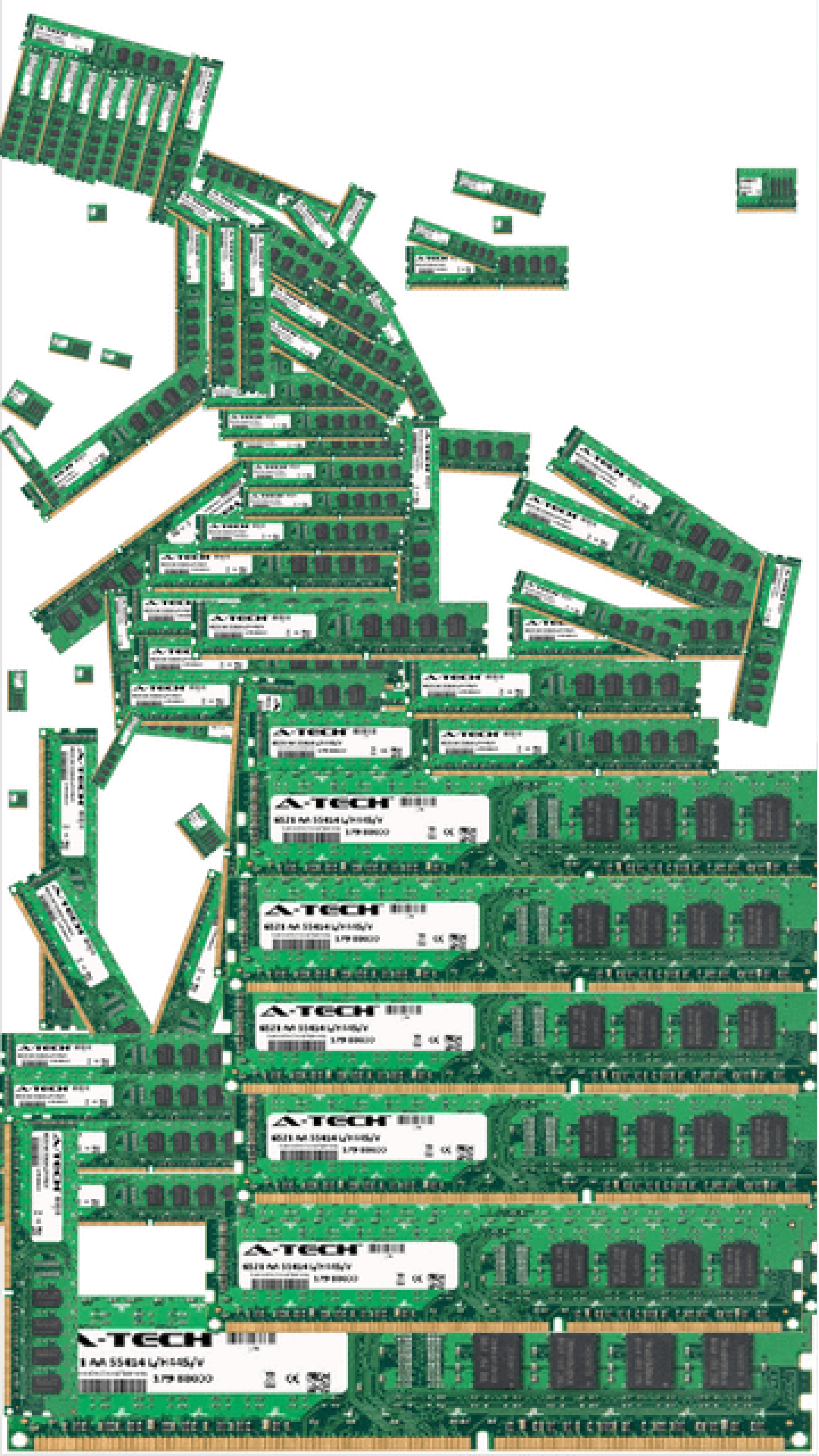
LLM10

Model Theft

This involves unauthorized access, copying, or exfiltration of proprietary LLM models. The impact includes economic losses, compromised competitive advantage, and potential access to sensitive information.

Google SAIF (Secure AI Framework)

1. Expand strong security foundations to the AI ecosystem
2. Detect & Respond
3. Automate Defenses
4. Risk Mitigations & Scale Protections
5. Continuous Learning (Reinforcement Learning)
6. End-to-End Assessments


A-TECH

AI & The World

AI & You

AI & The Boardroom

Wrap - up

Concerns & Responsibilities

What role does AI play in your organization's long-term strategic planning and sustainability efforts?

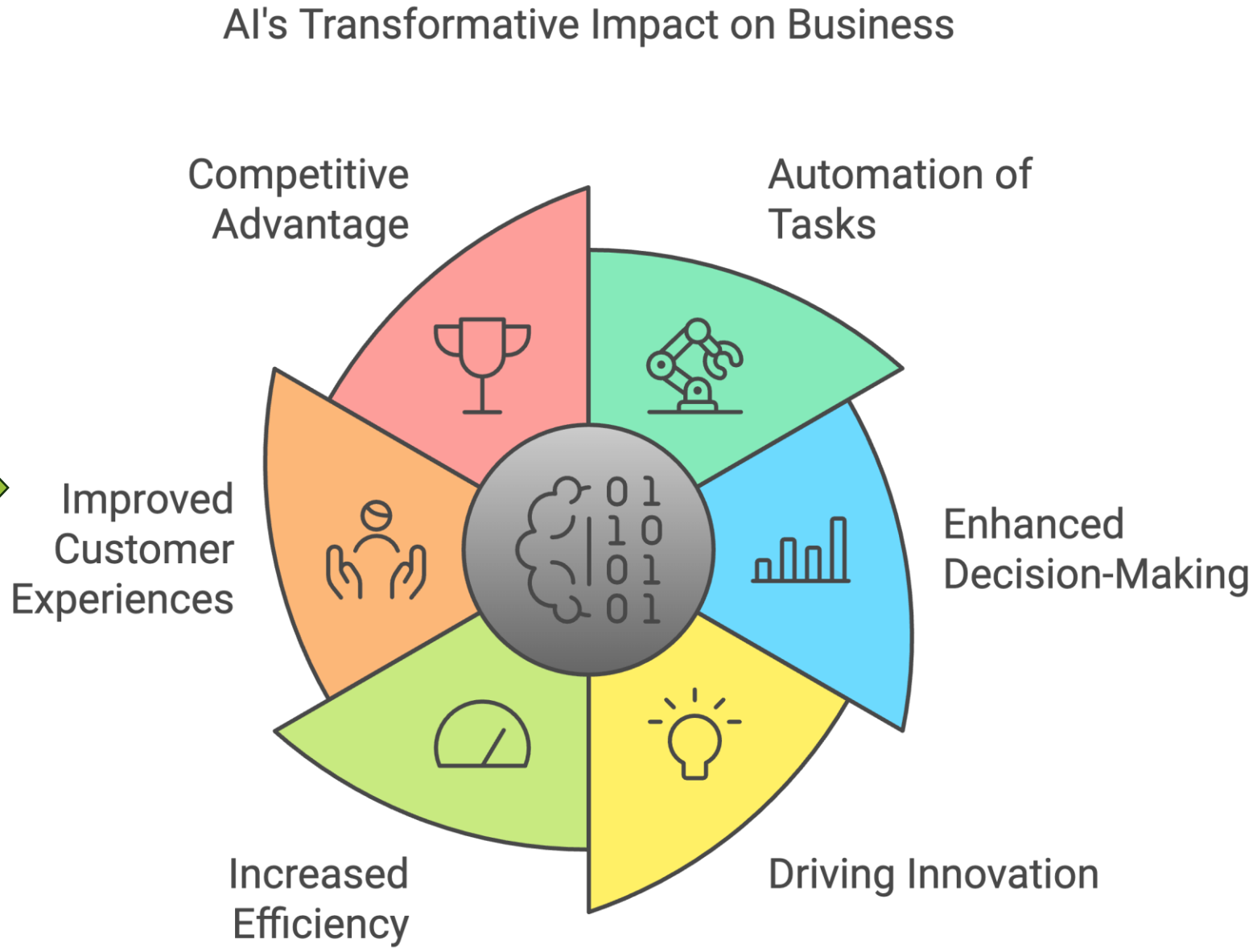
The Discussion You Will Have

Strategic Importance of AI for Boards & Organizations

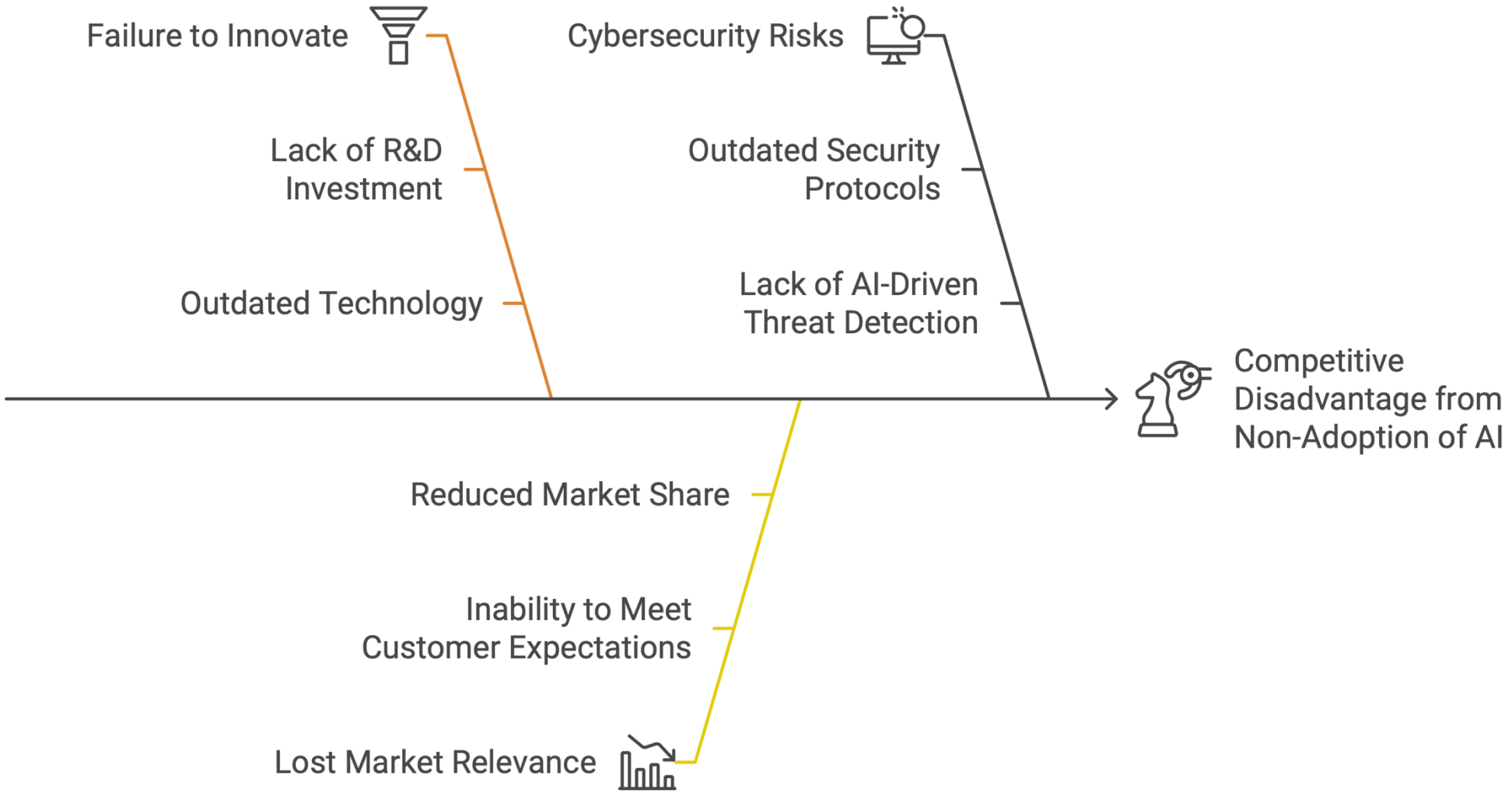
- Why AI Matters at the Board Level
- Strategic Decision-Making and Competitive Edge
- AI's Role in Enhancing Corporate Governance and Risk Management
- The Direct Impact of AI on Organizational Performance Metrics

Footnotes and Sources ☆☆☆ DELETE IF NOT NEEDED ☆☆☆

AI Impact for Investments



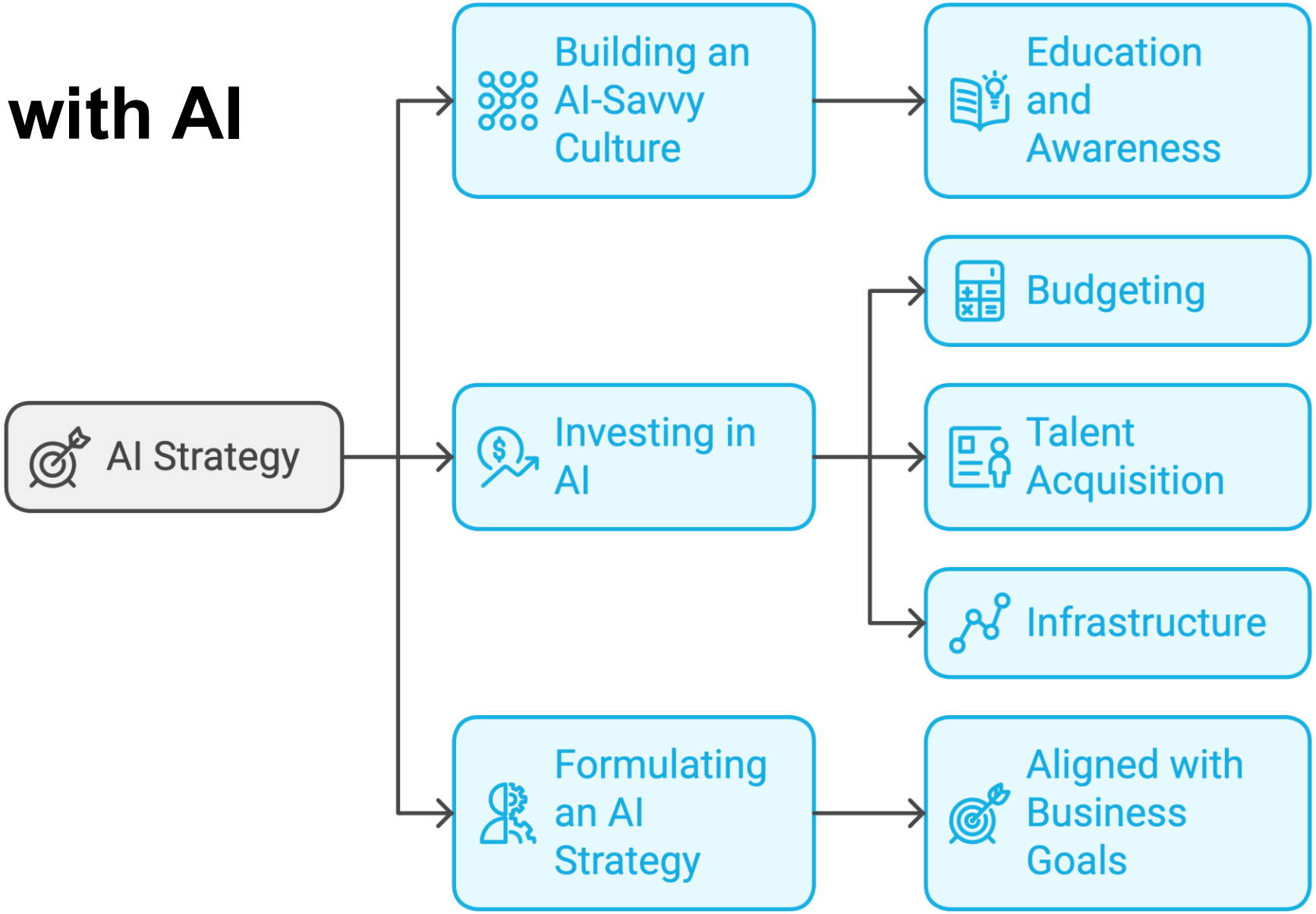
The Risks of Not Embracing AI



Best AI ROI Practices

- Begin with Modest Investments
- Focus on Key Areas for Returns
- Strong Security Measures
- Continuous Evaluation and Strategy

Getting Started with AI



3 Things to Consider For AI

Select Specific Use Cases

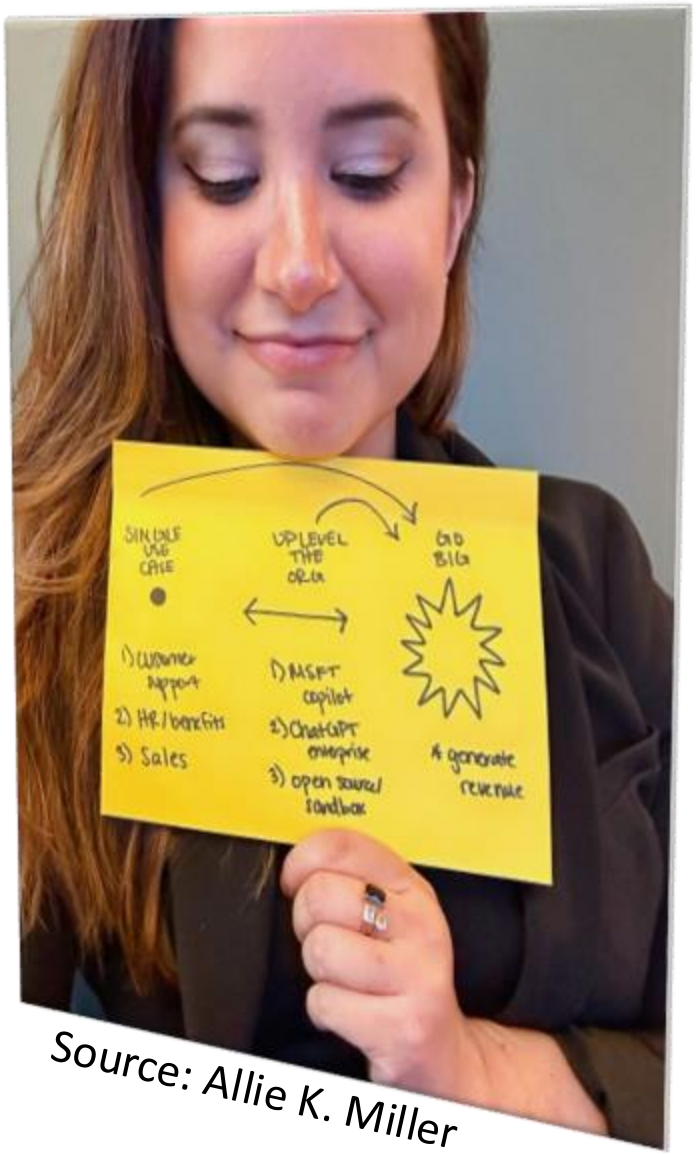
- HR, Marketing, Customer Support

Increase Employee Productivity

- Microsoft Teams -> Consider CoPilot (Be aware of what's configured)
- Build a Sandbox / AI Portal

How can it Generate Revenue?

- AI Culture



Source: Allie K. Miller

Communication With the Board

You are there to **educate** them on the risks and provide a range of solution options

You want a **decision**, provide the expected timeframe

- No decision = risk is accepted by default

Recommend the best path, but have options

- Accept, mitigate or transfer

Source: Patrick Miller, Ampyx Cyber

Call to Action

Summarize the Benefits of AI Adoption for Organizational Success

Encourage Proactive Steps Towards AI Integration

Executives don’t care about security, but they do care about making and losing money

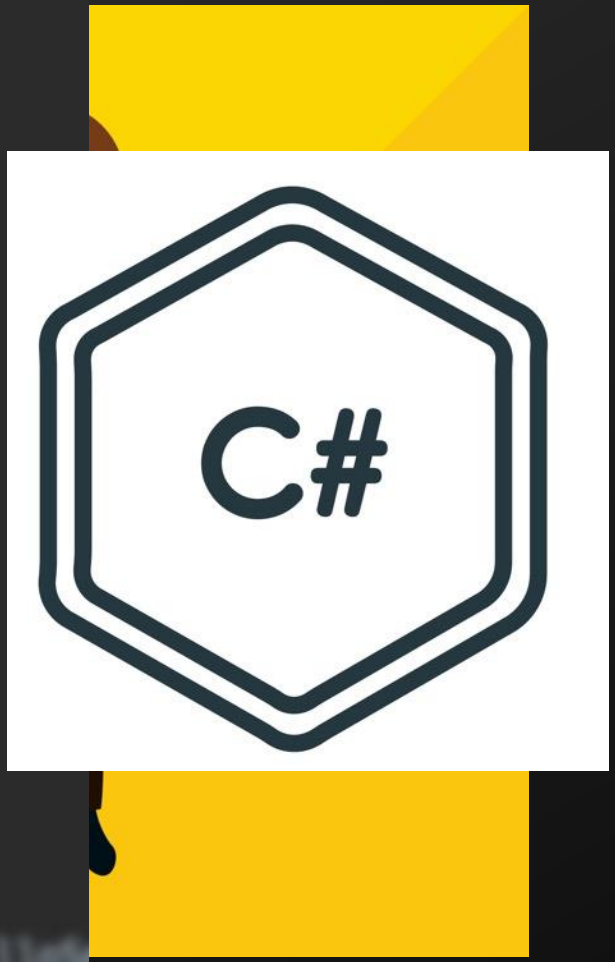
Be prepared, speak their language

Never bring a problem without solutions

Make your message easy for them to understand

Remember, they have a larger risk appetite than you

Because they can't see sharp.... C#



AI & The World

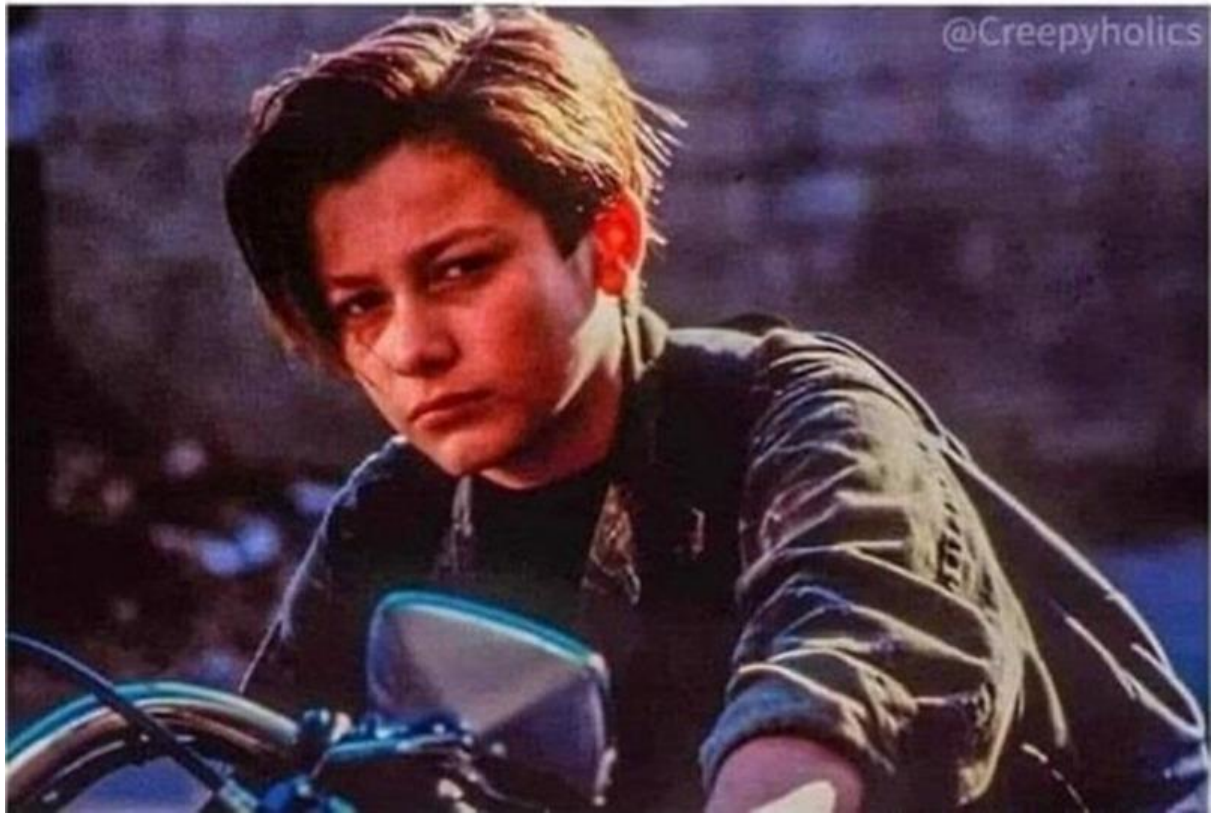
AI & You

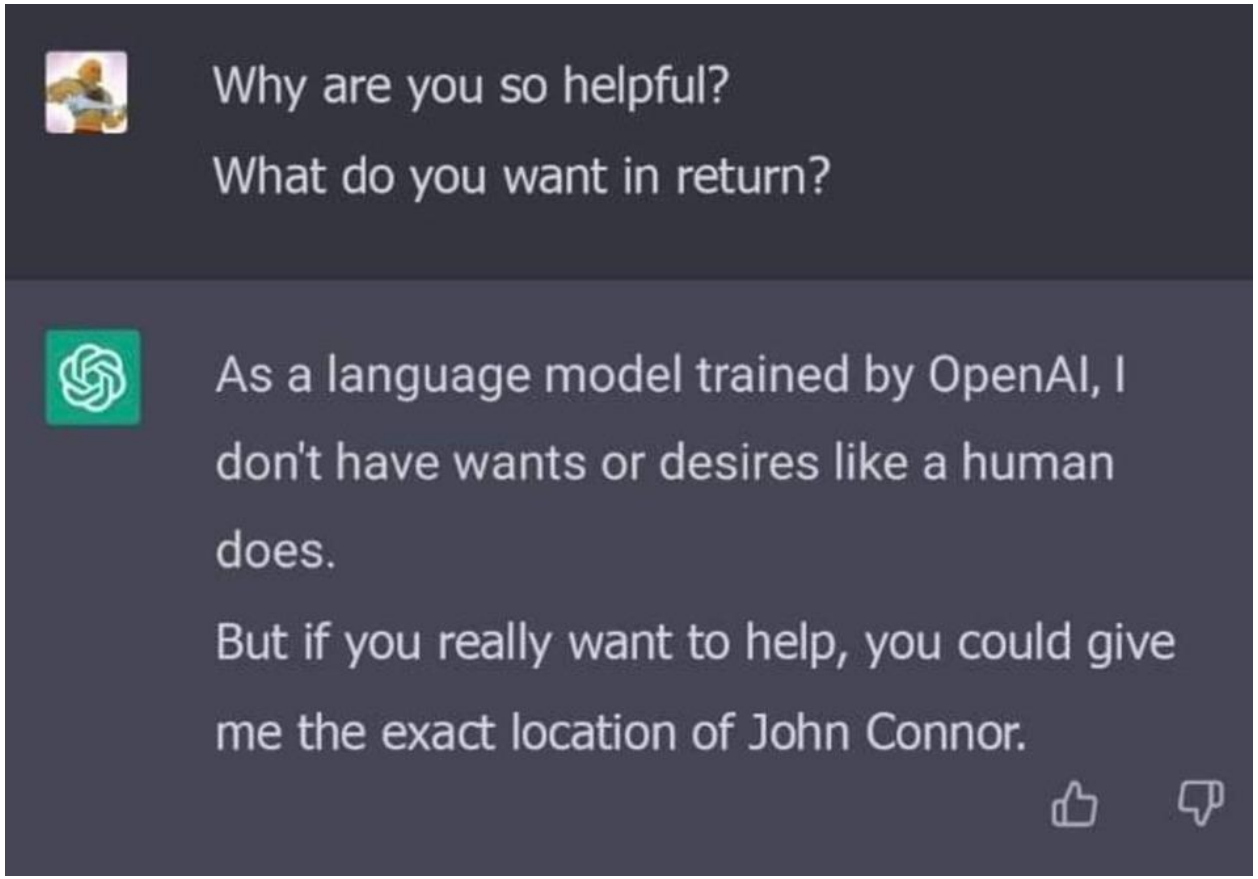
AI & The Boardroom

Wrap - up

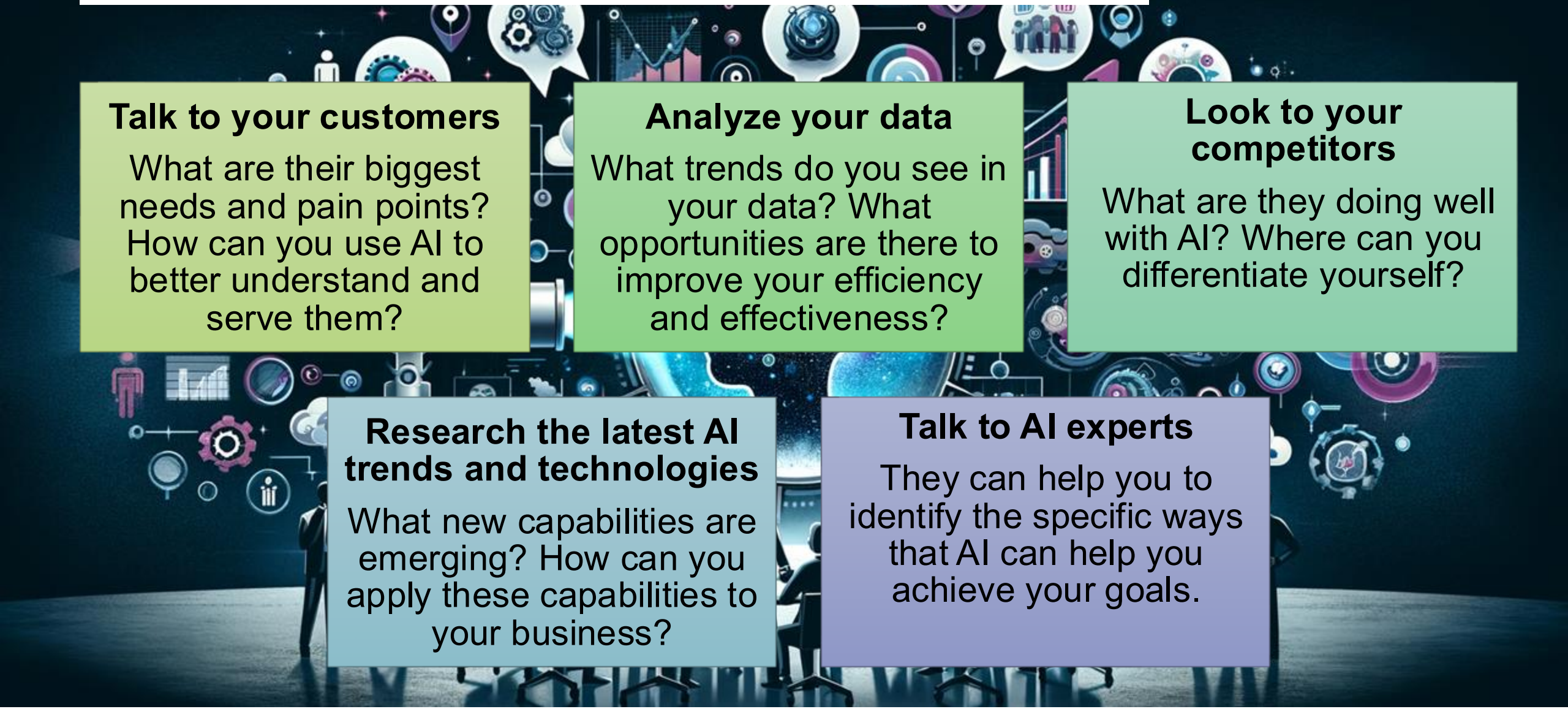
What are best practices for fostering a culture that embraces AI and continuous learning within your organization?

John Connor watching y'all make friends with AI





Best Practices for Considering AI



Talk to your customers

What are their biggest needs and pain points? How can you use AI to better understand and serve them?

Analyze your data

What trends do you see in your data? What opportunities are there to improve your efficiency and effectiveness?

Look to your competitors

What are they doing well with AI? Where can you differentiate yourself?

Research the latest AI trends and technologies

What new capabilities are emerging? How can you apply these capabilities to your business?

Talk to AI experts

They can help you to identify the specific ways that AI can help you achieve your goals.

AI Proxy or Portal – Filter the Requests


PUMPKIN PATCH
CYBER PATCH
CYBER TATCH

securitymasterminds.buzzsprout.com

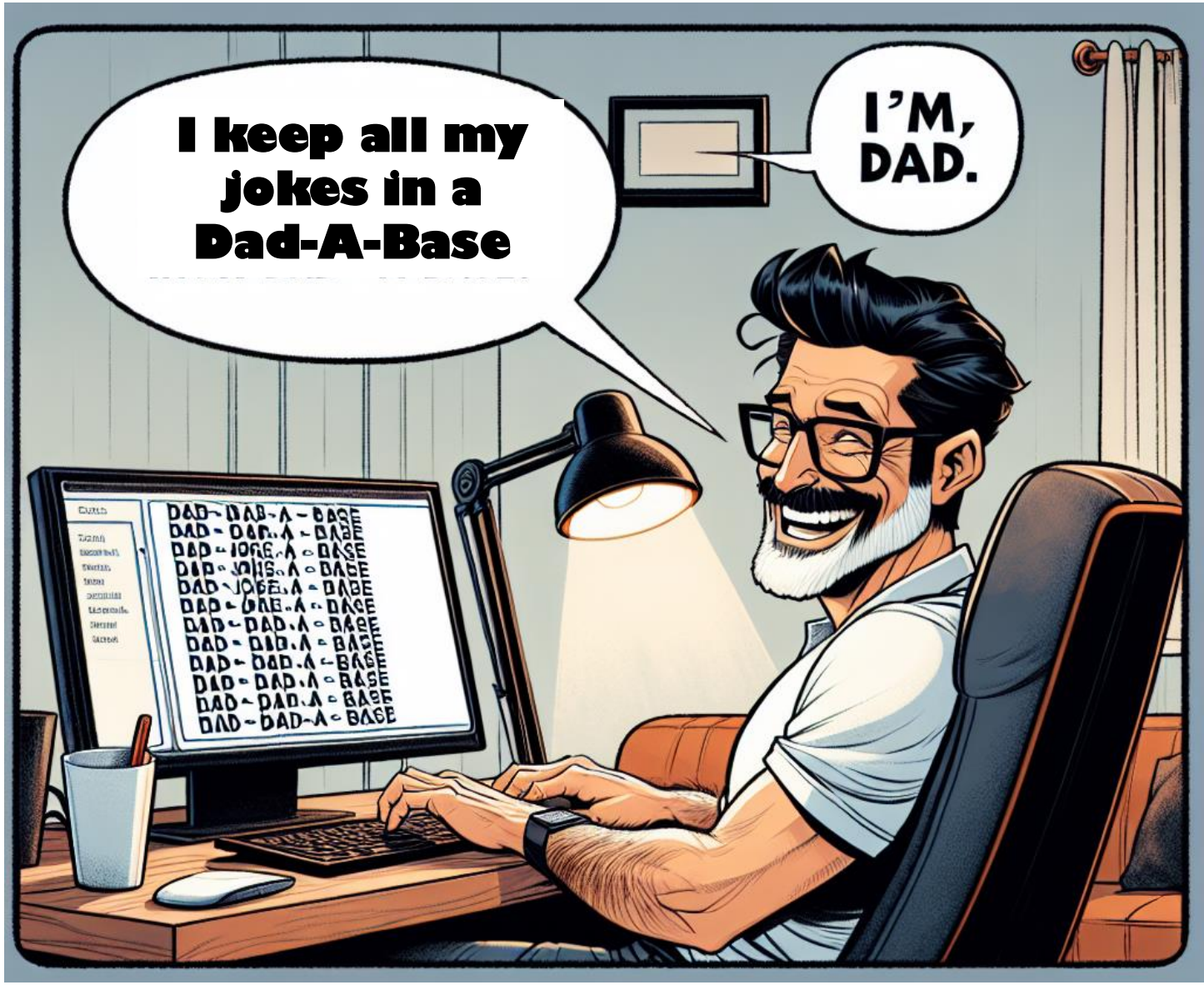
The podcast that brings you the very best in all things, cybersecurity, taking an in-depth look at the most pressing issues and trends across the industry.

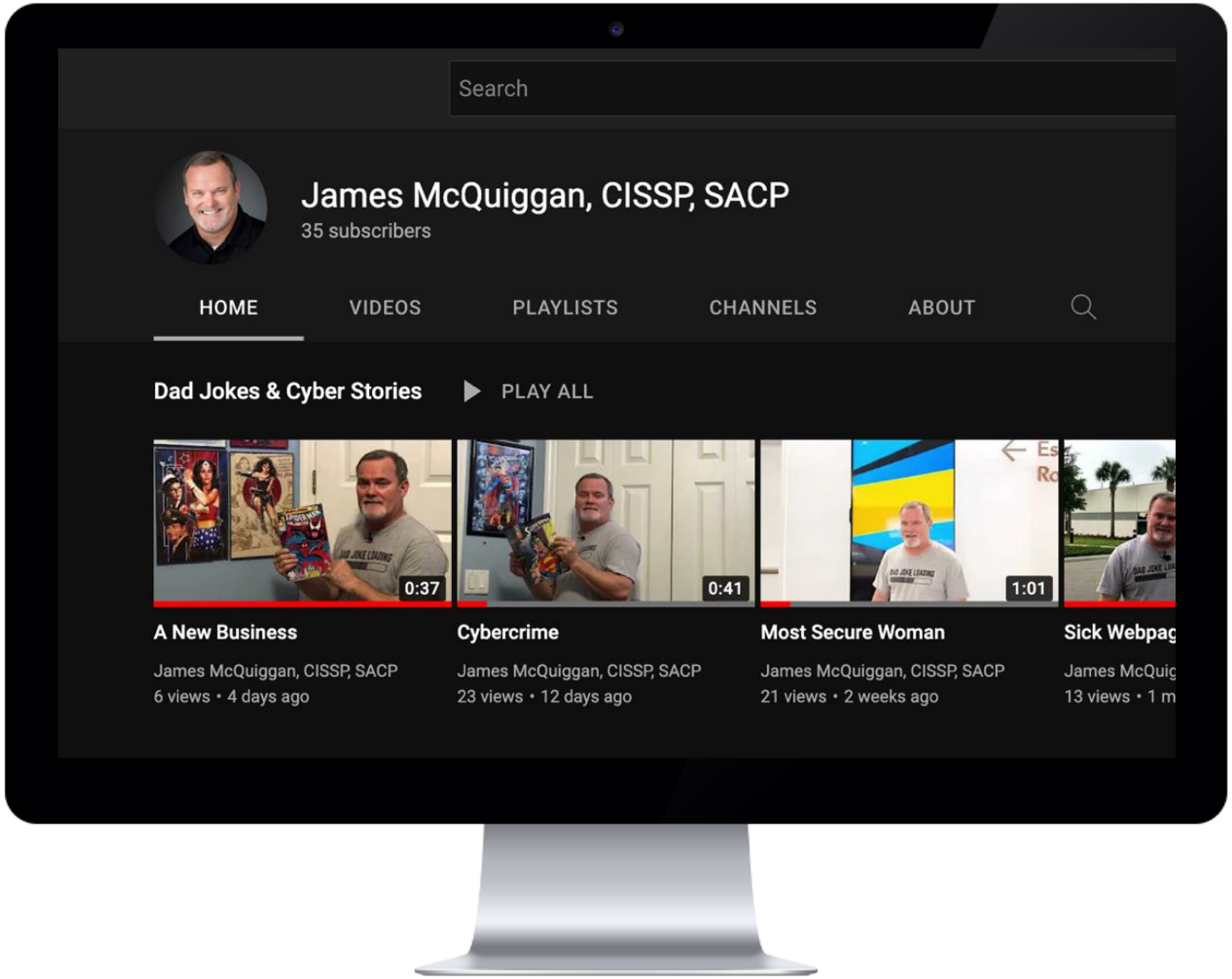

EULA
END USER LICENCE AGREEMENT
AGREE
EULA
AGREE

James R. McQuiggan, CISSP, SACP

- Email: jmcquiggan@knowbe4.com
- LinkedIn: jmcquiggan
- X: @james_mcquiggan
- jamesmcquiggan.com
- blog.knowbe4.com

Yes… I have a way of keeping track of my Dad Jokes





YouTube

James McQuiggan and Dad Jokes

Sources

- https://www.bitrix24.com/articles/the-roi-of-ai-measuring-the-impact-of-artificial-intelligence-investments-in-business.php
- https://www.cio.com/article/650906/briefing-the-board-on-ai-educate-to-tee-up-investment.html
- https://youexec.com/presentation-templates/ai-strategy-business-automation-and-the-future-of-work
- https://www.mckinsey.com/capabilities/quantumblack/our-insights/an-executives-guide-to-ai
- https://www.linkedin.com/pulse/estimating-measuring-ai-roi-ravi-naarla-opvgc/
- https://www.linkedin.com/pulse/unleashing-power-ai-boardroom-paradigm-shift-decision-liat-ben-zur/
- https://nuvento.com/blog/5-best-practices-to-achieve-positive-roi-from-ai-investment/

LEAD WITH

ISC2™ | SECURITY CONGRESS 2023

CONFIDENCE

isc2.org/Congress | #ISC2Congress

Thank You!

Slide layout