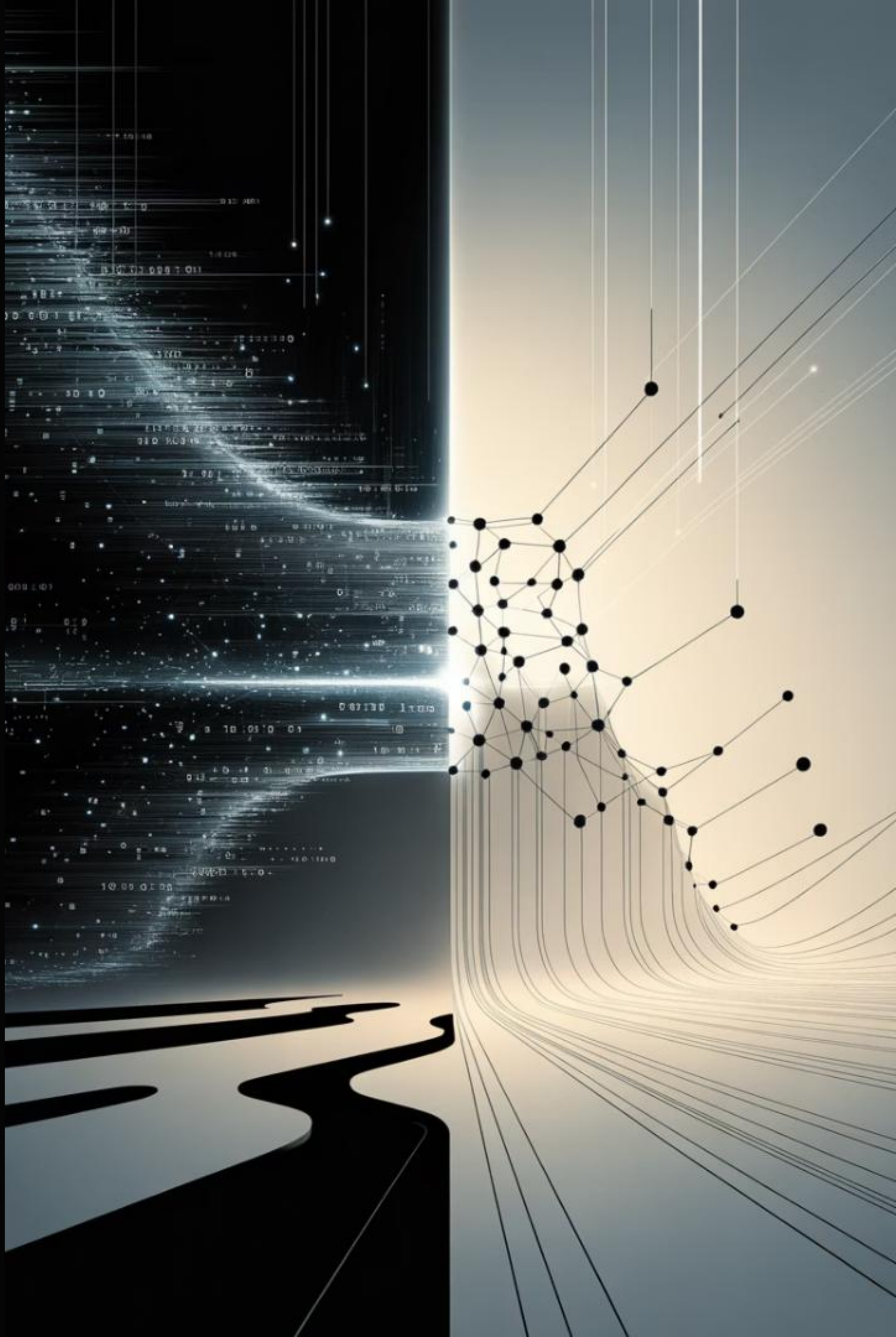
AI as a Cyber Advantage versus a Cyber Risk

The Dual Worlds of AI: Navigating Dystopia and Utopia

Privacy + Security Forum

May 8, 2025



The Presenters

Introduced by AI Lauren

LAUREN WINCHESTER
Head of Cyber Risk Services
Travelers
LWinches@travelers.com

MATT WELLING
Partner
Crowell & Moring
MWelling@crowell.com

DOUG HOWARD
CEO & Board Member
Pondurance
doug.howard@pondurance.com

AI in Action: Current Applications and Implications

Security Benefits

Enhanced threat detection, automated response, and consistent security policy enforcement

Security Risks

Advanced phishing, accelerated vulnerability discovery, sophisticated deep fakes

Human Readability Benefits and Concerns

Large Language Models ability to interpret and translate large data sets and complex details into consumable knowledge … but is it accurate

Privacy Concerns

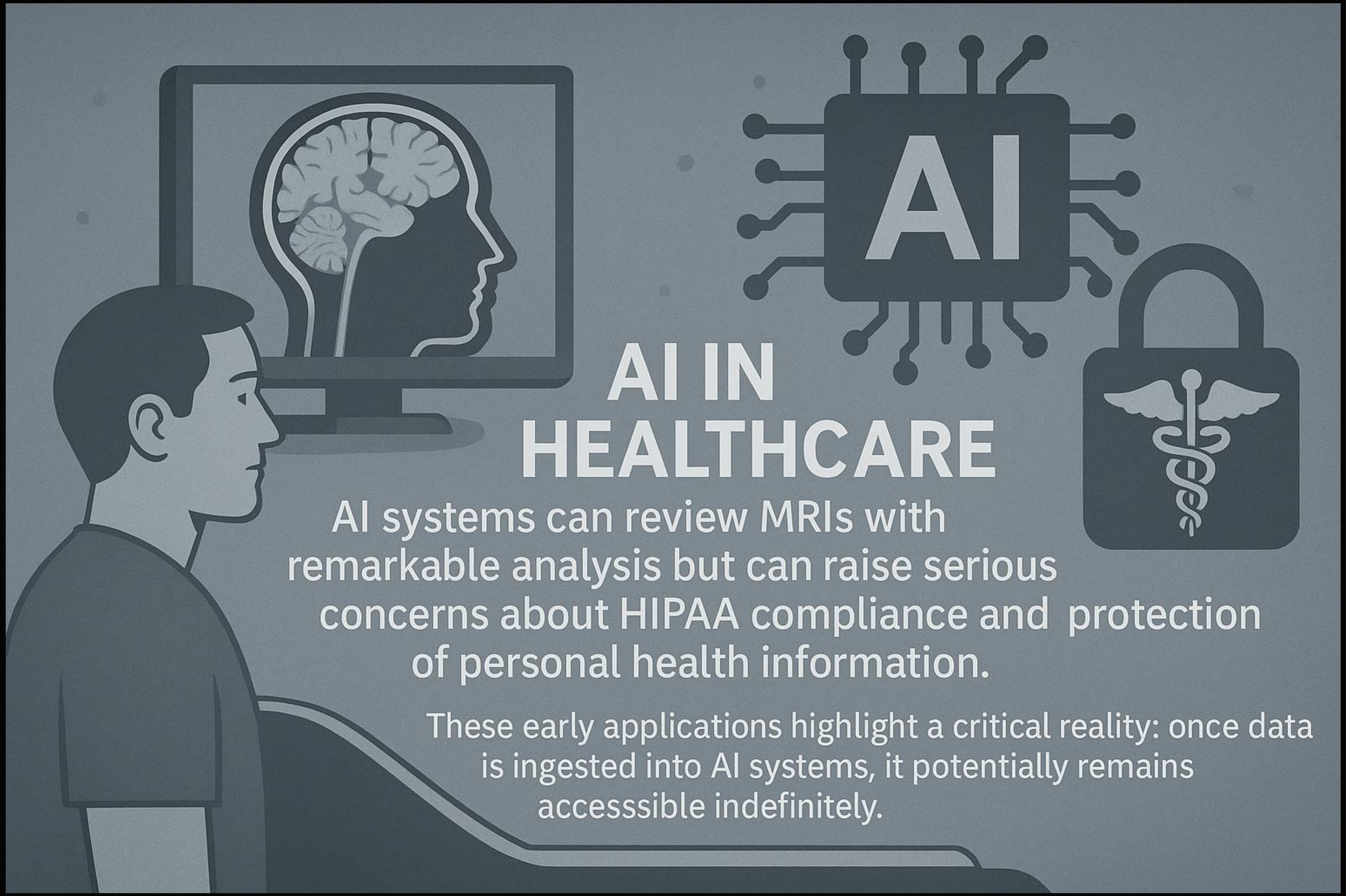
PII/PHI risks, permanent data integration and retention, and unauthorized use

Where and How is my data being used

Current AI and LLM use data in ways that are often unchecked and once in a model, cannot be removed.

Sample Healthcare AI Application Use Case

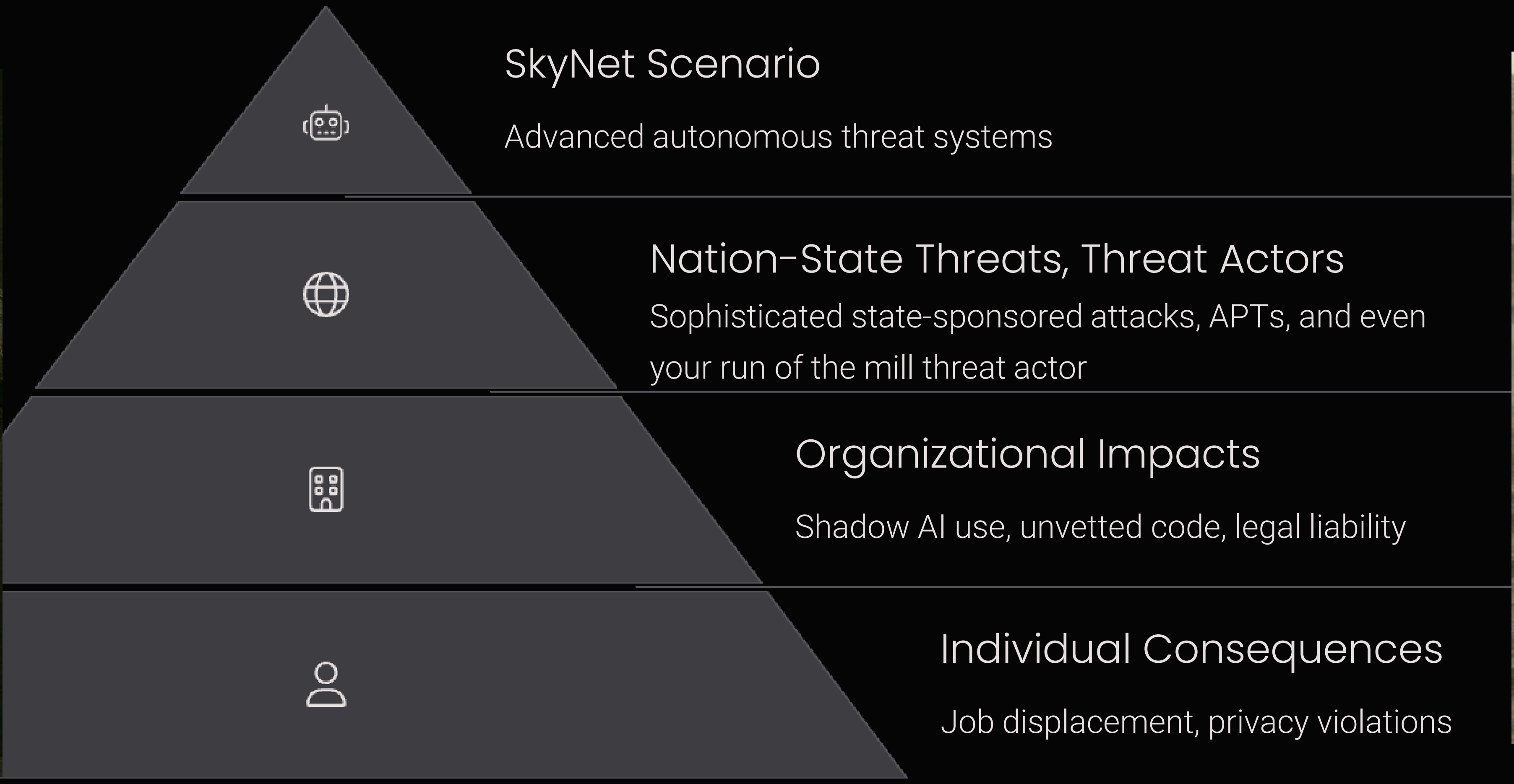
MRI analysis, diagnostic assistance, and clinical decision support



AI systems can review MRIs with remarkable analysis but can raise serious concerns about HIPAA compliance and protection of personal health information.

These early applications highlight a critical reality: once data is ingested into AI systems, it potentially remains accesssible indefinitely.

World 1: The Dystopian Scenario



SkyNet Scenario

Advanced autonomous threat systems

Nation-State Threats, Threat Actors

Sophisticated state-sponsored attacks, APTs, and even your run of the mill threat actor

Organizational Impacts

Shadow AI use, unvetted code, legal liability

Individual Consequences

Job displacement, privacy violations

AI Cyber Threats In The Wild

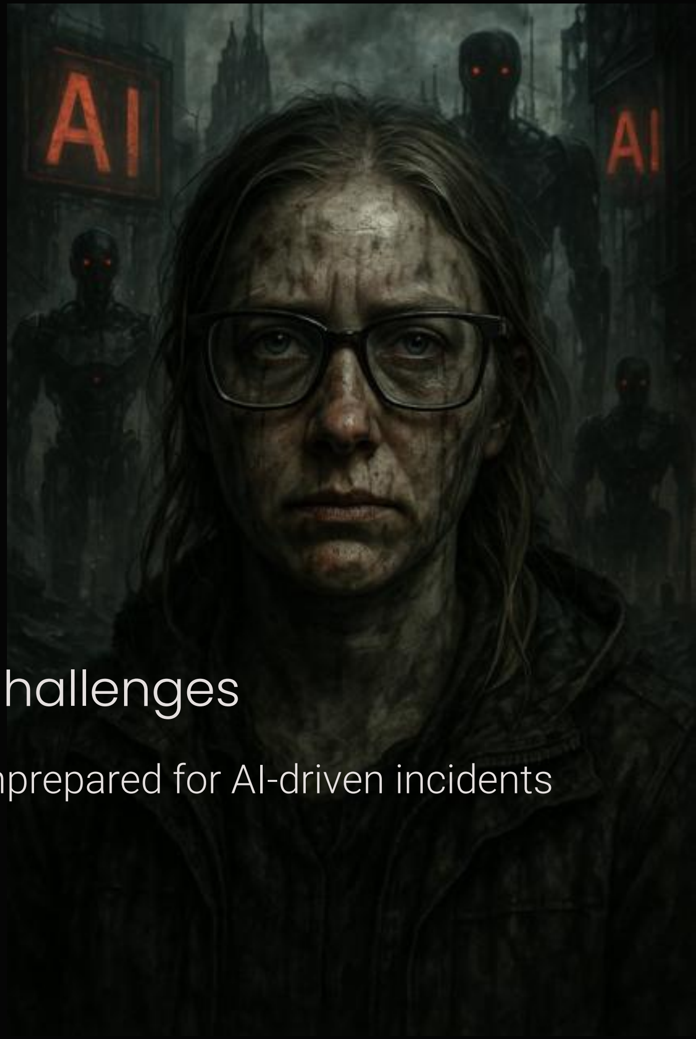
Existing Threats

- Efficiency gain – automating reconnaissance, execution and intrusion
- Improved social engineering – deepfake audio and video; drafting more convincing content for social engineering; customization
    - $25M loss following a video call with a deepfake impersonation of an executive
    - Extortion demands from deepfake audio calls for fake kidnappings
    - NK operatives leverage deepfake tech to pose as IT professionals and secure remote work positions in Western companies
- Malware creation - vibe coding for bad guys
- Hacktivism or Revenge – former school athletic director created a deepfake audio of the principal making racist and antisemitic remarks, leading to public outrage and threats against the principal; political deepfake robocalls
- Data mining for sensitive information

On The Horizon

- Data Poisoning – if attackers poison training data, can they create blind spots for cybersecurity tools relying on the data; are there supply chain risks if many companies rely on the same set of data
- AI-powered password cracking
- AI-powered encryption breaking

The Regulatory and Compliance Quagmire



Compliance Gaps

Existing frameworks inadequate for AI capabilities

Insurance Challenges

Cyber policies unprepared for AI-driven incidents

Legal Liability

Uncertain responsibility for AI-generated content

Risk Assessment

Traditional models failing to capture AI threats

World 2: The Utopian Vision within Cyber Risk

Enhanced Monitoring, Detection and Protection

AI accelerates identification of sophisticated attacks and anomalies in a continuous manner

Improved Analysis

Advanced pattern recognition reveals previously hidden threats

Streamlined Compliance

Automated assessment and documentation of regulatory requirements

Workforce Augmentation

AI handles routine tasks while humans focus on strategic initiatives

The Efficiency Revolution

Examples

Contract Analysis

AI systems can review thousands of contracts in hours instead of weeks, identifying potential risks and compliance issues with remarkable accuracy. This enables legal and security teams to focus on addressing findings rather than manual review.

Process Development

Security teams leverage AI to draft comprehensive processes and procedures based on industry best practices, organizational requirements, and regulatory frameworks. Human experts then customize these drafts to their specific environment.

Code Assistance

Developers utilize AI to generate initial code frameworks and security controls, accelerating development while potentially reducing common vulnerability patterns when properly reviewed and implemented.

Workforce Transformation

Accelerated Learning

AI condenses years of knowledge acquisition into months through personalized, adaptive learning experiences

New Skill Development

Security professionals develop AI prompt engineering and system design skills to maximize defensive capabilities

Innovative Approaches

New security paradigms emerge as AI and human creativity combine to address previously intractable challenges

Collaborative Defense

Human-AI teams form the foundation of next-generation security operations centers

Navigating Our AI Future

Establish AI Governance

Create clear policies and oversight mechanisms

Develop Hybrid Skills

Build both human and AI capabilities

3

Implement Safeguards

Deploy technical controls and monitoring

Advocate for Balance

Support effective regulation without hindering innovation

An entire new generation of cyber defenders adapting and accelerating the use of AI

Join the AI Evolution