HARPONIAN
INTERNATIONAL

Enterprise AI Security & Data Exposure

Understanding AI-Specific Security Risk

Format	Duration	Audience	Deployment	LMS / SSO	PO
Live / Recorded	**60 min**	**Executives / Security**	**Enterprise licensing**	**N/A**	**Supported**

Executive Overview

Enterprise AI Security & Data Exposure is a live executive briefing that explains AI-specific security and data risks in business terms. It reframes AI security as enterprise risk management, covering data leakage, access risk, misuse, traceability, and the controls leaders should expect without requiring deep technical knowledge.

Briefing Outcome

Help executives, board members, and security leaders understand how AI can expose data, amplify misuse, or weaken control visibility, and how leadership can support practical safeguards aligned to risk appetite.

Why This Matters

AI tools can change how information is accessed, summarized, reused, and shared. Without appropriate controls, sensitive data may move into prompts, files, outputs, or third-party systems in ways that are hard to monitor and difficult to explain after the fact.

Enterprise Risk Exposure Addressed

- Sensitive data exposure through prompts, uploads, outputs, or integrations
- Over-permissioned access that allows AI tools to surface inappropriate information
- Weak traceability for AI-assisted actions, summaries, or decisions
- Security controls that do not reflect how employees actually use AI tools

What the Organization Receives

- **AI Security Risk Briefing:** Executive-level explanation of AI-specific data exposure and control risks.
- **Data Exposure Scenario Guide:** Practical examples of how sensitive information can be leaked, overexposed, or misused through AI workflows.
- **Control Expectation Checklist:** Leadership checklist for access, monitoring, approved tools, prompt handling, and output review.
- **Security and Governance Alignment Notes:** Guidance for aligning AI use with security policy, compliance expectations, and risk appetite.
- **Incident Escalation Triggers:** Practical indicators for when AI-related security concerns should be elevated.