AIS247: **AI Security Essentials for Business Leaders™**

Self-Paced Program | 2 CPEs | Laptop Required

Skills Learned

- Identify common AI technologies, terminology, and use cases
- Understand how generative AI models work, including their risks and limitations
- Recognize and mitigate threats including prompt injection, deepfakes, misinformation, and more
- Implement responsible AI policy aligned with emerging legal requirements
- Govern AI systems using risk-based frameworks such as NIST AI RMF and EU AI Act guidance
- Evaluate your organization's AI maturity and create a roadmap for improvement
- Build fluency in agentic AI workflows, data security, and model governance

Business Takeaways

- Confidently oversee enterprise AI initiatives with risk-informed decision-making
- Accelerate AI adoption while reducing compliance, privacy, and reputational risk
- Support executive conversations around strategic, secure, and ethical AI use
- Establish a cross-functional AI leadership team and policy framework

Navigate the AI Revolution with Confidence

This course equips executives, business leaders, and key staff with the essential knowledge to understand, oversee, and govern AI adoption responsibly and securely. With practical insight into generative AI, AI literacy, technology trends, risk management frameworks, policy governance, and real-world security threats, AIS247™ ensures leaders are prepared to make informed decisions that align innovation with security and compliance.

Through actionable frameworks and engaging case studies, participants will develop fluency in AI across organizational strategy, risk, security, ethics, and operations.

As AI continues to reshape industries and redefine how work gets done, leaders are under pressure to make fast, informed decisions about adoption, governance, and risk. AIS247™ is designed to meet that moment. Whether you're shaping policy, evaluating vendors, or guiding your teams, this course delivers the foundational knowledge and practical insight you need to lead responsibly—without requiring a technical background.

Author Statement

"Artificial Intelligence is transforming business faster than anyone anticipated. As organizations race to adapt, leaders need clear guidance that cuts through the noise. My experience building products, leading engineering teams, and shaping AI policy has given me a unique perspective on what actually matters for business decision makers during this extraordinary shift.

"Since launching AIS247, I have been committed to making every part of this course both practical and future-focused. I have included dedicated sections on the top trends shaping AI and the essential elements of AI security, so you are equipped with the knowledge and strategies required right now. Most importantly, this course is designed to advance true AI literacy—a fundamental skill for every business leader. AIS247 breaks down complex concepts, demystifies the technology, and lays out actionable steps so leaders at all levels can understand and apply AI in real business contexts.

"My goal is to empower you with the clarity and confidence to harness AI's power effectively and securely. AIS247 will help you maximize productivity, manage risk, and lead with purpose as AI becomes a core part of your organization's strategy. AI is no longer optional. The companies that invest in AI literacy and approach this wave with both ambition and caution will set the standard for responsible innovation. I invite you to use this course as your roadmap for navigating AI's opportunities and challenges and to lead your teams with clarity as the landscape evolves."

—Dan deBeaubien

Section Descriptions

SECTION 1: Why AI, Why Now?

Section 1 examines the business, economic, and competitive forces driving generative AI into mainstream-use across every industry. Students will explore current usage statistics, investment trends, and how AI is being embedded into workplace tools, workflows, and decisions.

SECTION 2: Demystifying AI

In Section 2, you will better understand key terminology like LLMs, transformers, embeddings, and inference while using plain language and real-world examples. Learn how tools like ChatGPT actually work, how they generate answers, and why they sometimes get things wrong. Myths about AI being sentient are clarified and practical insights are provided to help separate hype from reality.

SECTION 3: Prompt Engineering

Through examples and scenarios, techniques for refining prompts, managing AI context windows, and controlling tone and format will be explored. Understand how prompt engineering plays a role in everything from productivity improvements to effective security and compliance.

SECTION 4: 2025 AI Technology Trends

Section 4 covers five foundational trends shaping the landscape: reasoning models, agentic workflows, AI-powered coding tools, drag-and-drop workflow platforms, and LLM-specific security tooling. Understand what is emerging as strategically relevant in corporate environments.

SECTION 5: AI Policy and Governance

Section 5 introduces key frameworks and legislative trends shaping AI regulation, including the EU AI Act, U.S. Executive Orders, and the NIST AI RMF. Learn how to build policies using practical templates and real-world examples to guide you through the process. Understand how good policy accelerates AI adoption responsibly by creating clarity, alignment, and organizational trust.

SECTION 6: AI Cybersecurity Essentials

Section 6 will explore cybersecurity risks specific to LLMs and GenAI systems, including prompt injection, model poisoning, data leakage, and excessive agency. Students will review the OWASP Top 10 for LLMs, learn about the MITRE ATLAS framework, and understand how to apply zero trust principles to AI workflows.

SECTION 7: Threat Actors and Abuse

Section 7 reveals how adversaries are using AI to generate convincing phishing attacks, clone voices, create deepfakes, and automate malicious code. By understanding the attacker's toolkit, you'll be better prepared to recognize warning signs and educate others within your organization.

SECTION 8: End-User Risk Mitigation

Section 8 examines how to reduce unintentional AI risks through training, policy enforcement, and data governance. Learn how to define acceptable use, prevent shadow AI, and implement safeguards that protect sensitive data from being leaked or mishandled.

SECTION 9: Explainability and Trust

In Section 8. you will understand and explore the concept of explainability—the ability to understand and trace how an AI system arrived at a given result. Learn when explainability is required, how it builds user trust, and why it's essential for audits, compliance, and informed decision-making.

SECTION 10: AI Maturity Model

Section 10 introduces a structured framework for evaluating your organization's readiness to manage and scale AI adoption responsibly. Learn how to assess eight key dimensions to identify gaps and build a roadmap for growth.

SECTION 11: Conclusion and Action Plan

This final section ties everything together with a concise, actionable roadmap and a prioritized checklist of immediate next steps: inventory your current AI usage, update policies, identify key stakeholders, train your people, and establish oversight.

Who Should Attend

- CISOs, CIOs, CTOs, CMOs
- Business leaders, unit leads, and managers
- Senior legal, HR, marketing, sales, and finance professionals
- InfoSec officers
- IT leaders, managers, and team leads
- Security directors, managers, and engineers
- Chief product officers and product managers
- Engineers, software developers, and analysts involved in AI adoption

Prerequisites

This training is designed for any business, technology, and security leader and is non-technical in nature.