GLOBAL
INDUSTRIES
INTELLIGENCE

AIS247 AI SECURITY
ESSENTIALS FOR BUSINESS LEADERS

+44 2080 508 945 www.giintelligence.com training@giintelligence.com

COURSE OUTLINES

This course is designed to provide business leaders with a fundamental understanding of AI security and its importance in protecting business operations. It covers key concepts in AI

DAY 1: INTRODUCTION TO AI AND AI SECURITY

- **Understanding AI and Its Impact on Business**
  - What is Artificial Intelligence? Key types of AI: Machine Learning, Deep Learning, and Natural Language Processing
  - The role of AI in business transformation: Opportunities and challenges
  - Overview of AI security: Definition, relevance, and why business leaders should care

- **Key AI Security Threats and Risks**
  - Understanding AI-specific vulnerabilities: Adversarial attacks, data poisoning, model inversion
  - Privacy risks in AI systems: How AI can jeopardize user data and privacy Cybersecurity risks related to AI: Attacks on AI-driven systems and networks
  - Case studies: Real-world examples of AI security breaches

- **Ethics and Governance in AI Security**
  - Ethical considerations in AI deployment
  - AI governance frameworks and regulations: GDPR, CCPA, and other AI-related laws
  - The role of business leaders in ensuring ethical AI use and security compliance

DAY 2: IDENTIFYING AND MANAGING AI SECURITY RISKS

- **Risk Assessment for AI Systems**
  - How to assess the security risks of AI technologies in business operations
  - Frameworks and methodologies for AI risk management (e.g., NIST, ISO/IEC 27001)
  - Risk-based decision-making: How to prioritize security risks in AI systems

- **Threat Intelligence and AI Security**
  - Tools and techniques for monitoring AI systems for security threats
  - Using AI for cybersecurity: How AI can help detect and mitigate security threats in real time
  - Building a threat intelligence culture within the organization

- **Data Protection and Privacy in AI**
  - Protecting sensitive data used in AI systems: Best practices for data encryption and anonymization
  - Ensuring compliance with data protection laws in AI applications
  - AI and data privacy: How to handle data breaches and mitigate risks to user privacy

DAY 3: IMPLEMENTING AI SECURITY IN BUSINESS OPERATIONS

- **Securing AI Systems and Infrastructure**
  - Best practices for securing AI algorithms, models, and underlying infrastructure
  - Authentication, access control, and secure coding practices for AI developers
    Securing AI cloud services and third-party providers

- **Developing an AI Security Strategy for Business**
  - Key components of an AI security strategy for organizations
  - Creating a security policy for AI development, deployment, and monitoring
  - Defining roles and responsibilities for AI security within the organization

- **AI Security in the Supply Chain**
  - Addressing the risks posed by AI in the supply chain
  - Securing third-party AI vendors and partners
  - Best practices for managing AI-related risks across the business ecosystem

DAY 4: AI GOVERNANCE, COMPLIANCE, AND BUSINESS CONTINUITY

- **AI Governance Frameworks**
  - Building and implementing AI governance policies in the business
    Governance and transparency in AI decision-making
  - Aligning AI security with corporate governance and leadership priorities

- **Compliance and Regulatory Challenges in AI Security**
  - Navigating the evolving landscape of AI regulation and compliance
    Understanding legal frameworks for AI security and business accountability
  - Ensuring AI systems meet regulatory requirements (e.g., data protection, ethical standards)

- **Business Continuity and Incident Response Planning**
  - Developing a business continuity plan for AI systems
  - Incident response protocols for AI-related security breaches
  - Business leaders' role in crisis management during AI security incidents

DAY 5: LEADING AI SECURITY INITIATIVES AND PREPARING FOR THE FUTURE

- **Building an AI Security Culture in the Organization**
  - Leadership's role in fostering an AI security-first culture
  - Employee training and awareness programs for AI security
  - Promoting collaboration between AI, cybersecurity, and data privacy teams

- **Future of AI Security and Emerging Threats**
  - Key emerging trends in AI security: Explainable AI, Autonomous AI, and
  - AI-driven cyberattacks
  - The role of business leaders in shaping the future of AI security
  - Preparing for AI's growing role in the global cybersecurity landscape

- **Developing a Personal Action Plan for AI Security Leadership**
  - Setting personal and organizational goals for AI security leadership
  - Creating a roadmap for implementing AI security measures in your business
  - Leveraging AI security to gain a competitive advantage while mitigating risks

ADDITIONAL COURSE DETAILS:

- **Target Audience:**
  - Business executives and senior leaders responsible for AI strategy and implementation
  - IT and cybersecurity managers who are tasked with securing AI systems
    Legal and compliance officers handling data protection and AI-related regulations
  - Entrepreneurs and decision-makers looking to understand AI security risks and opportunities

- **Learning Methodology:**
  - The course will be delivered through a mix of interactive lectures, case studies, group discussions, real-world examples, and practical exercises. Participants will leave with a comprehensive understanding of AI security and the tools they need to secure AI systems, comply with regulations, and lead AI security initiatives within their organizations.

  - By the end of the course, participants will have the knowledge to effectively manage AI security risks, protect business-critical AI systems, and ensure their organizations are well-prepared for the future of AI and cybersecurity.