AI-Driven Business Resilience and Data Protection Strategy

Skills and expertise to help you increase your knowledge in the field of securing digital technologies

TLC
Opportunities are made, not found

Key Benefits of an AI-Driven Approach:

Lower Breach Costs: Organizations utilizing AI and automation for security save an average of $2.44 million in breach costs compared to those that do not – Different survey reports published by several international technology consulting groups .

Enhanced Data Privacy and Compliance: AI helps ensure compliance with regulations like GDPR and CCPA by automating data classification, access governance, and ensuring privacy-by-design.

Improved Competitiveness: By enhancing operational stability, organizations can maintain customer trust and reputation during crises, which is essential for long-term growth.

In this workshop we will learn how to develop a business resilience strategy to deal with AI-Driven threats such as prompt injection attacks and data abuse, runtime manipulation and behavior tampering, and model and AI component thefts.

In a nutshell, AI changes the shape of mobile application risk because it introduces new **logic paths** inside the app, and it runs in environments defenders do not fully control.

Target Audience:

The targeted audience for this workshop includes CXO, Business Technology Leaders, IT Operation teams, Backup Recovery Operations teams, Disaster Recovery and Business Continuity teams, Information Security and Cybersecurity professionals, System Administrators, Lead Storage Architects, Solution Architects, Cloud Architects, Enterprise Architects, Business Technology professionals, Application and Database teams, Project Managers, GRC Professionals, IT Auditors and Legal teams, AI Architects, Business Analysts, IT Consultants, Strategy Builders, and Technical Writers.

About this workshop:

Developing an AI-driven business resilience and data protection strategy is now becoming a greater concern and considered as a critical component for organizations running mission critical 24x7 business operations. It is essential to transforms security from a reactive, manual function into a proactive, automated, and intelligent defense mechanism. As cyber threats become more sophisticated, faster, and often AI-powered themselves, traditional security methods can no longer keep pace.

Cyberattacks, nation-state hacking and geopolitical shifts dominated the headlines in 2025, but the year will also be remembered as a turning point where **artificial intelligence** blurred the lines between real and fake, and AI agents introduced new enterprise risks.

Moreover, as of 2026, over **95%** of cybersecurity professionals believe AI-powered solutions are crucial for elevating defenses against increasingly sophisticated attacks, with AI-driven threat detection identified as the top impact area.

About the Workshop Facilitator: This workshop will be delivered by an IBM Certified Specialists – Dynamic Infrastructure Business Resilience Technical Design, TOGAF Certified, IBM Certified Infrastructure Systems Architect, SNIA Architect - Assessment, Planning and Design.

Unit 1 – The Core Fundamentals of AI-Driven Business Resilience Framework

- New challenges of Digital Transformation.
- Pressures on Senior Executive Management – Key challenges.
- Defining Strategy and Strategic Planning – The Key Difference.
- Understand Fault Tolerance & Fault Resilience – Business Uptime.
- How SLAs and OLA's are measured?
- Understanding the three categories of Risks.
- Global Barriers to Achieving Business Resilience – A survey covering 4 Domains.
- The impact of Business Resilience and Data Protection.
- What is Business Resilience?
- How to Build Business Resilience and Types of Business Resilience.
- Business Resilience Strategy and subsequent types of plans.
- What drives a Business Transformation – A Roadmap for Success.
- Business Resilience and Business Transformation Objectives.
- Principles for Achieving the Business Resilience.
- AI-Driven Business Resilience Framework.
- Core Pillars of an AI-Driven Business Resilience Framework.
- Key Benefits of AI-driven Business Resilience Framework.
- Essential Requirements for an AI-Driven Business Resilience Strategy.
- AI-Driven BR Framework – The Human-AI Collaboration Model.
- Seven Principles of building a Business Resilience Strategy.
- Developing a Robust AI Strategy Framework & Implementation Considerations.
- Pros and Cons of AI-Driven Business Resilience Framework.
- Four Reasons Why AI cannot Replace Humans at Work.
- Use Cases of AI-Driven Analytics in Business.
- What is ISO 22301?
- Key Aspects of ISO 22301.
- Benefits of a Business Continuity Management System.
- Nine step process to implementing a BCMS based on ISO22301.
- Unit 1 Assessment.

Unit 2 – Information Infrastructure and Data Management Methodologies

- Understanding Information Infrastructure.
- Information Infrastructure Model and Critical Characteristics of Information.
- A Comprehensive Framework for Information Infrastructure by SNIA.
- Core Components of the SNIA Information Infrastructure Model.
- Understand Enterprise-scale Master Data Management.
- Data Archive – What is it and its importance.
- Common approaches to the implementation of Archiving Solutions.
- Criteria that Determines the Effectiveness of a Storage Security .
- Consequences of a data security breach – Reputational Loss.
- Understanding Data Management.
- The Data-driven Enterprise and its Challenges.
- Six Key Parts of the Data Management Process.
- Understanding core parts of the Data Management Process.
- Key Principle and Benefits of Data Management Process.
- Five ways to Optimize Data Strategy.
- Things you need to Know about Data Storage Management.
- Overcoming Storage Management Challenges.
- Understanding Data Lifecycle Management – DLM.
- Data Lifecycle – The Eight Stages, and Roles and Responsibilities.
- Understanding AI-Enabled Data Lifecycle.
- Information Lifecycle Management – ILM.
- ILM – Three Storage Strategies.
- Information Lifecycle Management – An Example.
- Difference between ILM and DLM.
- Storage Vs Data Classification.
- Unit 2 Assessment.

AI-Driven Business Resilience and Data Protection Strategy

Skills and expertise to help you increase your knowledge in the field of securing digital technologies

TLC
Opportunities are made, not found

Brief Overview:

In a nut-shell, this workshop summarizes the techniques used for storage data protection and business resilience methodologies to ensure continuity of operations by using backup recovery tools in the light of Data Protection best practices recommended by SNIA.

Moreover, this workshop is designed on the basis that you have got nothing to lose and everything to gain.

In this session we will explore how AI can analyze vast, diverse data streams in real time to spot anomalies—such as ransomware, credential stuffing, or insider threats—far faster than human analysts. This reduces the time threats remain hidden, significantly limiting potential damage and lowering breach costs.

What else we learn in this two-day workshop:

In this session we will learn how to combat AI-driven sophisticated malwares that are used today by the cybercriminals including polymorphic malware, how model inversion attacks breaks your privacy where an attack uses a trained machine learning models API, outputs, or confidence scores to reconstruct or assume sensitive personal training data. Also, how cybercriminals exploits patterns where attackers can reconstruct data like facial images, medical records used to train their weaponized models even without accessing the database directly.

For complete details on this workshop, please visit:
https://www.tlcpak.com/tn285.html

Unit 3 – AI Enabled Data Security and Threat Management Plan

- Top Cybersecurity Trends to Watch in 2026.
- Understand Nine Layers of IT Infrastructure from overall Security perspective.
- Threats, Motives and Methods.
- Threat Categories – Network-based, Host-based, & Application-based Threats.
- OSI Layers and types of Attacks.
- Threats to Information Security – Categories/examples.
- Why considering AI Enabled Data Security and Threat Management Plan.
- What Involves in developing AI Enabled Data Security and Threat Management Plan.
- Comprehensive framework for an AI-enabled Security Plan.
- Knowing the Ethical implications of using AI in Cybersecurity.
- Knowing the potential risks of relying on AI in Cybersecurity.
- How AI is Transforming Data Security Practices?
- Framework for an AI-enabled Data Security Plan.
- AI-enabled Security Plan Framework Key Considerations.
- How do AI Algorithms Detect and Prevent Cyber Threats?
- The Evolving Trends in AI and Data Security for the Future.
- Gaps in storage configuration causing threats & vulnerabilities.
- Data Storage Threat Management Plan.
- Issues that needs attention from storage security POV.
- Understand how can Businesses balance AI-Driven Security with Privacy Concerns.
- AI Enabled Storage Subsystem and Data Breach Risks.
- Practical Mitigations – What to prioritized.
- Quick Checklist you can run to ensure Data Consistency.
- What Criteria help determine the effectiveness of a Data Storage Security?
- Variety of technologies to ensure data storage security.
- Applying Storage Best Practices.
- Unit 3 Assessment.

Unit 4 – Setting up AI-Driven Data Protection Strategy

- Quiz – How to select the best storage technology?
- Storage Types, Subsystems and Services.
- IT Trends Vs Storage Management Challenges.
- Challenges and Needs – Where we stand today?
- Storage challenges faced by IT Managers.
- Business requirements & Traditional Technology Limitations.
- Consideration prior investing in new storage solution.
- Latency – Why it is an important fact to consider?
- Why Data Protection is important?
- Data Protection Overview – SNIA Point of View.
- Four key aspects of Data Protection Concepts.
- From data protection point of view, what are the key consideration for selecting the right Storage technology.
- About AI-Driven Data Protection Strategy .
- A Holistic Approach for Setting up an AI-Driven Data Protection Strategy.
- Essential activities involved in a Data Protection Strategy.
- Key Elements of a Data Protection Strategy.
- Key Concerns for building a Data Protection Strategy.
- Benefits of AI-Driven Data Protection Strategy.
- Disadvantages / Risks of an AI-Driven Data Protection Strategy.
- Mitigation Strategies and Best Practices.
- Understanding Data Protection Algorithms.
- Erasure Coding – A newer trend in Data Protection instead of RAID.
- Pros and Cons to the use of Erasure Coding and Best Practices.
- Considerations for using Data Protection in the Cloud.
- Top 8 Cloud Storage Security Challenges.
- SNIA Positions on Data Protection Best Practices.
- Unit 4 Assessment.

In 2026, approximately **4.8 million** additional cybersecurity professionals are required globally to close the skills gap and adequately defend organizations.

The global workforce needs to increase by nearly **87%** to meet the growing demand, bringing the total number of professionals needed to **10.2 million**, as the current workforce of 5.5 million is insufficient to combat rising threats.

40% of companies that suffer a massive data loss will never reopen – Gartner Group.

Moreover, this workshop is designed on the basis that you have got nothing to lose and everything to gain.

Detailed Information

Course Code	: TN285
Course Duration	: 2 Day
Course Location	: TLC, Online, and Customer On-site.
Terms & Conditions	:100% payment in advance.
Course Deliverable	: Comprehensive Student Guide and Course Certificate