

Storage Information Security

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

Course Highlights

Training will be delivered by an experienced trainer with 25+ years of career experience imparting education and training services both locally and internationally and have served international enterprise technology vendors including IBM, Fujitsu, and ICL.

Our instructor holds various industry professional certifications in the space of enterprise servers and storage technologies, Information Security, Enterprise Architecture, ITIL, Cloud, Virtualization, Green IT, and a co-author of 10 IBM Redbooks.

The training course flow will be a mix of lectures & classroom discussions so that participants can have a detailed understanding of various components of Storage security and data protection technologies best practices.



The storage training course is vendor neutral and it makes the attendee completely familiar with lot of technologies surrounding storage security and various complex issues and solutions thereof due to explosive growth of data.

Nevertheless, several issues are important when considering a security method for a security data on your storage devices using different storage protocols. Generally, storage security is the group of parameters and settings that make storage resources available to authorized users and trusted networks - and unavailable to other entities.

info@tlcpak.com

Prerequisites:

Participants attending this course should be familiar with basic Information Technology (IT) concepts and the role of general storage systems technology.

About the workshop:

This two-day face-to-face instructor led class is designed to develop storage security skills and data protection strategies associated with managing the explosive growth of business data across the enterprise in today's networked economy.

In a nut shell, two criteria can help determine the effectiveness of a storage security methodology. First, the cost of implementing the system should be a small fraction of the value of the protected data. Second, it should cost a potential hacker more, in terms of money and/or time, to compromise the system than the protected data is worth.

Unit 1 – Information Security Awareness

- Our world – and how we interact with it – is changing.
- The Evolution of Data increases storage security threats.
- Exponential Data Growth – Some key facts and figures.
- The Evolution of Storage technologies and future.
- What is Information Security and Information Storage.
- Information Security and Dependability.
- Business Drivers for Data Security.
- Security Vs. Safety in a view from threat perspective.
- Security – Defense in depth.
- Anti-Virus, Anti-Spyware and Firewalls.
- Avoid Social Engineering, Malicious Software and Hacker tricks.
- Understand Fraud and Pulling fraud out of the shadows.
- Top Security Concerns for Cloud-Based Storage Services
- Keep your Storage Security policy simple.
- 5 Questions you should ask to your storage Services Provider
- Top 5 Storage Security Challenges.
- Generalized Security Framework & Traditional and Enterprise Approach to Security.
- Understand Multifactor Authentication with scenarios.
- Unit 1 Assessment.

Unit 2 – Storage Security and Threats

- Threats and Storage Security Challenges – Business Context.
- Types of Threats, Motives and Methods.
- Understand 9 layers of IT Infrastructure Foundation from Security POV.
- To address security, leaders must avoid common myths.
- Use five fundamental security principles to help guide you.
- Understanding the role of Risk Management.
- Understanding Storage Security.
- Understanding Layer 2 of Fibre Channel – A weakest link.
- Issues that needs attention from storage security POV.
- Criteria that determine effectiveness of a storage security.
- Best principles for storage security & Best Practices defined.
- Variety of technologies to ensure data storage security.
- Different types of data needs different storage security.
- Hardening of the platform as a part of common practice.
- Storage security strategy and guiding principles.
- The Storage Threat Model – ISO/IEC 27040.
- The Storage Threat Model – ISO/IEC 27040 & Storage Security Management.
- Understanding different threat levels.
- Storage Network Points of Attacks – Unauthorized Access, Spoofing and Sniffing.
- Unit 2 Assessment.

Unit 3 - Storage Data Protection Best Practices

- Why Data Protection is important?
- Knowing the three Sides of Data Protection.
- Personal Data Defined.
- Five phases of the data protection life cycle.
- Examining the Cost of a Data Breach – A small exercise.
- Understanding Data Protection – Executive Summary.
- Knowing the three Sides of Data Protection.
- Understand Fault Tolerance and Fault Resilience.
- Data Protection from ISO/IEC 27040 Point-of-View.
- Guidelines for Securing Backups from ISO/IEC 27040 POV.
- Data Replications technologies, Discussing Pros & Cons of data replication methodologies & Industry Best Practices.
- Considerations before setting up Data Replication Services.

