The Core Fundamentals of Cybersecurity

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

TLC Education & Training Services

About this workshop

In the era of digital transformation, the importance for having substantial knowledge on cybersecurity is becoming essential skills to acquire for every technology professional today. The reason behind is the protection of information which is considered as one of the critical function for all enterprises. Cybersecurity is a growing and rapidly changing field and it is vital that the principal concepts that frame and define this increasingly pervasive field are clearly understood by technology professionals who are involved and concerned with the security implications of information Technologies.

This workshop is designed for this purpose, as well as to provide the insight into the importance of cybersecurity, and the integral role of cybersecurity professionals.

After completing this workshop, you will be able to:

- Understand basic cybersecurity concepts and definitions
- Recognize malware analysis concepts and methodology
- Distinguish system and application security threats and vulnerabilities
- Classify types of incidents (categories, responses and timelines of response)
- Outline disaster recovery and business recovery and business continuity planning
- Comprehend incident response and handling methodologies
- Understand security event correction tools and how different file types can be used for analytical behavior
- Be aware of the basic concepts, practices, tools, tactics, techniques and procedure for processing digital forensic data
- Recognize new and emerging information technology and information security technologies.

Workshop details:

Unit 1 – Introduction to Cybersecurity

- World is getting instrumented, interconnected & intelligent.
- The Evolution of Data increases storage security threats.
- The evolution of storage technology and future predictions.
- A world without cybersecurity.
- Most Frequently Targeted Industries in 2018.
- Top Security Concerns for the Executive Management.
- Hacker tricks to avoid – Recommendations.
- What is Cybersecurity? and Cyberspace defined.
- Differences between Information Security and Cybersecurity.
- Multiple layers of protection offered by Cybersecurity.
- Types of cybersecurity threats and Malware Detection.
- Why is Cyber Resilience needed.
- Top 11 ways poor Cybersecurity can harm you.
- Cyber Security Awareness – The 6 Layers.
- Blueprint for Cybersecurity Success.
- What are the objectives of Cyber Security?
- Suggestions for building stronger Cybersecurity defense.
- Adoption of Cybersecurity best practices.
- Questions you should ask your Services Provider.
- Typical Cybersecurity roles in the industry.

Unit 2 – Information Security Lifecycle Management

- Why Data Protection is important?
- The 8 Principles of Cybersecurity Laws.
- What is Information Security.
- The Information Security Management Lifecycle.
- IT Security Lifecycle Model.
- Information Security and Dependability.
- Generalized Security Framework.
- Traditional and Enterprise Approach to Security.
- Risks that turn your IT landscape into a hacker's gold mine.

To view the complete list of our courses, visit our education and training services program page.

https://www.tlcpak.com/educ.html

The Core Fundamentals of Cybersecurity

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

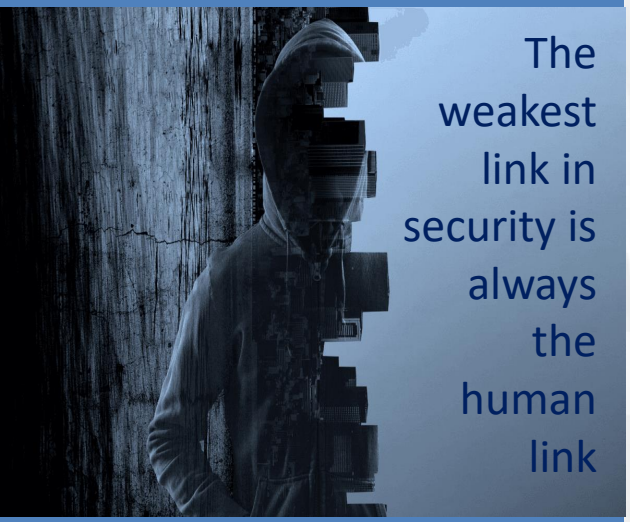
TLC
Education & Training Services

Target Audience

Business, application, audit, risk, compliance, information security, IT operations, project management, and legal professionals with a familiarity of basic IT/IS concepts who want to;

- learn new basic trends in cybersecurity.
- new to cybersecurity.
- interested in entering the field of Cybersecurity
- Students and fresh graduates.

This workshop is equally recommended for IT Consultants, Systems Integrators, Technology Consultants, Sales and Technical Sales resources who want to refresh their know in the field of Cybersecurity.



Workshop Methodology

The training course flow will be a mix of lectures & classroom discussions and videos so that participants can have a detailed understanding of various components and technologies used to combat against cyber attacks.

To see the list of all available courses , please visit: www.tlcpak.com/educ.html

Unit 3 – Managing Risks, Threats and Vulnerabilities

- Examining the Cost of a Data Breach.
- Security leaders must avoid common myths.
- Understand Incidents, breaches, risk & vulnerability.
- Fundamental security principles to help guide you.
- Threats, Motives and Methods.
- Knowing security threats and their channels.
- Risk Management: Know your risks and its role.
- Defense Planning – Risk Analysis and Assessments.
- A small backdrop on ISO 27001 & 12 sections of ISO 27002.
- Hardening of the platform – A common practice.
- Storage Security Management – ISO/IEC 27040 Overview.
- ISO/IEC 27040:2015 addresses storage risks & vulnerabilities.
- Qualitative Risk Assessment.
- Security risks & solutions in the DX age.
- Nine essential layers of IT Infrastructure foundation.
- Cyber incident recovery tools.
- Top 10 recommendations for closing the security gap.
- Outside Threat Protection –The bigger picture.
- Cyber incident recovery tools.
- A Layered Cyber Defense Approach.
- Top 10 recommendations for closing the security gap.
- Top 5 Security Challenges for customers opting Cloud services.

Unit 4 - Incident Response

- Describe Incident Response.
- The Role of Computer Security Incident Response Team.
- Seven key phases of an Incident Response Plan.
- Computer Forensics (Cyber Forensics).
- Cyber Incident Management Framework.
- Incident Management and Categorization.
- The role of Service Desk in Incident Management.
- Incident Response Planning.
- Security incident and Business Continuity.
- Critical Incident Recovery Plan & cyber attack quick response.
- Zero-day and your Security Strategy.
- Mitigating the effects of a Zero-day attack.

About the instructor

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 (an England based organization).

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 and have designed and developed 15 courseware's based on complete of stack of storage, information security, cybersecurity, enterprise architecture and digital technologies.

Detail Information

Course Code	: TN225
Course Duration	: 1 Day - Face- to-Face Workshop
Course Location	: TLC and Customer On-site.
Terms & Conditions	:100% payment in advance.
Course Deliverable	: Comprehensive Student Guide and Course Certificate

For additional information, please write to us at:
info@tlcpak.com

Opportunities are made, not found