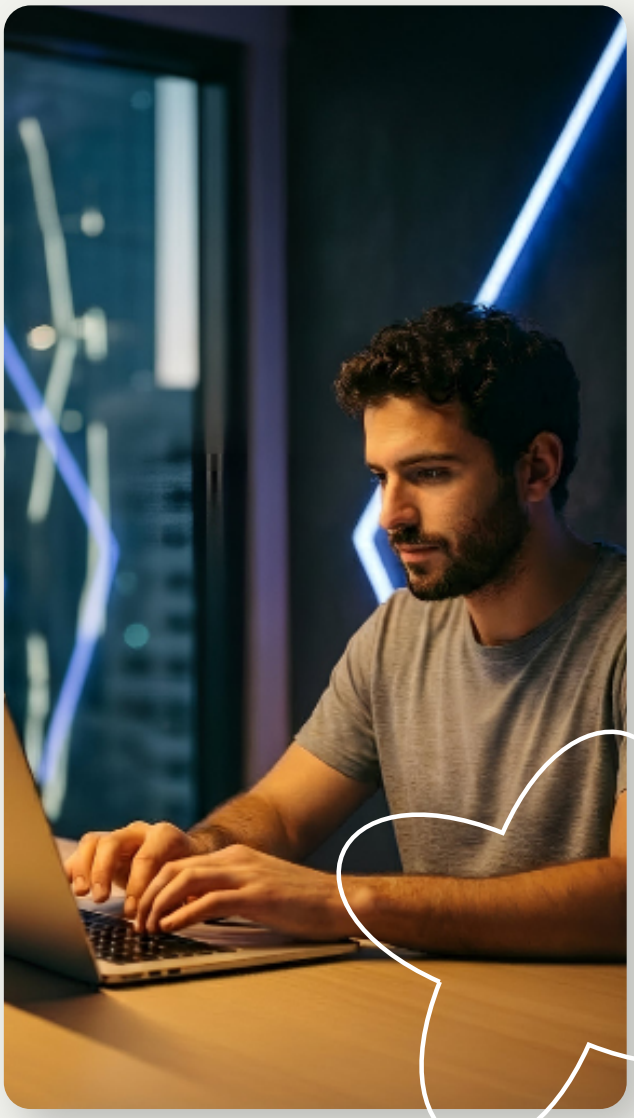
Hacker.U
מזניקים אותך לקריירה בהייטק

Quantum Cyber Readiness



Overview

The technological world is facing a revolution. Quantum computing brings tremendous opportunities, but also an existential threat to the classical encryption systems that currently protect an organization's most sensitive data. This course provides Information Security Managers (CISOs) and technology leaders with critical knowledge and practical tools to prepare for the day encryption is broken. The course focuses on the "**Harvest Now, Decrypt Later**" threat, reviews emerging regulations (NIST 2030), and provides a structured methodology for building an organizational action plan for the transition to **Post-Quantum Cryptography (PQC).**

Duration

32 Academic Hours

Target Audience

The course is designed for role-holders in organizations that possess sensitive data and must comply with strict regulations (Finance, Health, Critical Infrastructure, Government).

- **CISOs and Risk Managers.**
- **Senior IT teams and System Architects.**
- **Internal Auditors and Directors required to understand business risks.**

Prerequisites

The course is designed for role-holders in organizations that possess sensitive data and must comply with strict regulations (Finance, Health, Critical Infrastructure, Government).

- **Professionals with a background in Information Security Management or IT Infrastructure.**
- **Familiarity with the cyber world and Risk Management (GRC).**
- **Basic understanding of encryption infrastructures (PKI, SSL/TLS) – Advantage.**
- **Technical level English.**

Instructor & Partnership

The training was built in collaboration with PQCLayer, an American cyber company providing a platform for cryptographic risk management and quantum threat readiness.

> The quantum threat is no longer a distant future scenario, but an immediate managerial challenge. The question isn't 'if' encryption will be broken, but whether your organization will be caught prepared at the moment of truth. In this course, we will not only learn about the risk—we will implement a methodology that makes quantum defense an integral, easy-to-implement part of your organizational security core.

Shabi Dagan

Co-Founder & CTO PQCLayer.
Expert in Information Security in the Quantum Era.

Course Syllabus (Modules)

MODULE 01

The Quantum Revolution & Emerging Threat

Understanding the technological basis and the business urgency today.

- **Introduction to Quantum Computing**: What makes it different from classical computing and how it threatens RSA and ECC encryption.
- **Technological Timeline**: Review of technological progress and expected schedules for encryption breaking.
- **Harvest Now, Decrypt Later:** Why now? Understanding the immediate threat to data being stored today.
- **Costs & Implications:** The cost of non-readiness vs. the cost of early preparation.

MODULE 02

Regulation, Standards & Risk Management

Mapping the emerging regulatory landscape and organizational implications.

- **Regulator Guidelines (NIST):** Familiarity with emerging standards and readiness requirements for 2030.
- **International Compliance:** The impact of the quantum transition on meeting GDPR, HIPAA, and PCI-DSS standards.
- **Global Bodies' Stance:** Reference to CISA, ENISA, and leading global regulators.

MODULE 03

Practical Action Plan

Leave the course with a Playbook and Checklist for immediate organizational implementation.

- **Discovery:** Locating critical assets and sensitive data requiring quantum protection.
- **Gap Analysis:** Analyzing existing encryption mechanisms and their vulnerability levels.
- **Building a Roadmap:** Planning the transition to Post-Quantum Cryptography (PQC) solutions.
- **Crypto Agility Policy:** Setting procedures that allow for the rapid replacement of algorithms when needed.

MODULE 04

Management, Control & Technological Tools

How to manage the event at the executive/ board level and use advanced tools.

- **Management Aspects:** How to present the threat to the Board of Directors and build a business case for investment.
- **Audit & Control:** Applied audit questionnaire for testing organizational readiness (Readiness Assessment).
- **Innovation & Tools:** Review of tools for managing Crypto Posture and introduction to solutions (such as PQCLayer).
- **Practical Steps for Tomorrow:** Integrating PQC into the Risk Register and starting a POC with new algorithms (Kyber, Dilithium).