Quantum AIdea

Cyber Risk

Quantum Computing Risk in Cyber Security

Material:

- Presentations PDF
- R
- Python

Duration: 40 h

Price: 6.900 €

COURSE OBJECTIVE

Basel explains that quantum computers, if they get big enough and powerful enough, can break the encryption schemes widely used today to ensure secure financial data and transactions. This makes quantum computing one of the most significant cybersecurity threats facing the financial system, potentially exposing all financial transactions and much of our existing stored financial data to attack.

While it is not yet clear when quantum computing technology might be adopted on a large scale, its potential as a cyber threat to the financial system is already a cause for concern. Malicious actors can intercept and store classically encrypted sensitive data with the intention of decrypting it later when quantum computers are powerful enough to do so.

Recognizing these potential risks to its systems and data, the financial sector needs to preemptively implement robust quantum communication and data protection technologies. Given the long-term sensitivity of financial data and the complexity of central bank IT systems, a transition phase must be initiated well in advance so that quantum-resistant encryption schemes can be implemented.

We believe that the recent discovery of the new material for building superconductors LK 99, at room temperature, could accelerate the quantum leap.

The objective of the course is to expose the impact and risks of computing and quantum technologies in the cybersecurity of financial institutions, to achieve the objective we explain what quantum computing, quantum algorithms, quantum mechanics and quantum and post-quantum cryptography, lattice based are. , to defend against possible quantum threats.

The course explains in detail the interaction between geopolitics, reputational risk and cybersecurity, the possible scenarios that are expected with the progress of quantum computers.

The use of artificial intelligence to strengthen the cybersecurity of banks is explained. The XOI methodology for measuring cyber risk is briefly explained.

The global vision of CyberRisk, cyberattacks and losses suffered by financial institutions, methodologies and good practices on cybersecurity in business processes are exposed, and some technical standards for management and control are explained, such as NIST, Cobit 5. and ISO 27001.

Cyber Risk Appetite, Cyber Risk Limits and Cyber Risk Tolerance methodologies for the governance and control of Cyber Risk are exposed.

Traditional methodologies such as logistic regression and other, innovative, machine learning methodologies are exposed, such as: decision trees, naive bayes, KKN, LASSO logistic regression, random forest, neural networks, Bayesian networks, Support Vector Machines, gradient boosting tree, etc

The use of artificial intelligence and in particular machine learning and deep learning to strengthen cybersecurity is explained, advanced models are shown to detect anomalies, transactional fraud, phishing, cyber attacks, intrusions and malware.

Advanced deep learning is explained, with convoluted neural networks for facial recognition, the powerful Generative Adversarial Network (GAN) to detect adverse attacks from machine learning algorithms, recurrent neural networks for the classification of CyberRisk events and the multilayer perceptron for detection of intrusions and anomalies.

WHO SHOULD ATTEND?

This program is aimed at directors, managers, consultants, regulators, auditors and risk analysts, operational risks, cyber risks, as well as those professionals who are implementing cybersecurity measures. Professionals who work in banks, savings banks and all those companies that are exposed to cyber risks.

Cybersecurity in Basel III

Module 1: Cyber Resilience

- Cyber risks in banking
- CyberRisks in Latin America and Europe.
- Cyber Resilience Standards and Guidelines
- Case Study 1: Recent Regulatory Initiatives: Australia, Germany and the US Minimum Requirements
- Cybergovernance
    - Cybersecurity strategy
    - Management roles and responsibilities
    - Recognition of the importance of the board of directors and senior management
    - Variety of supervisory approaches regarding the second and third lines of defense (3LD)
    - Case Study 2: Roles and responsibilities of chief information officers (CISOs) in cyber governance
    - Cyber risk awareness culture
    - Architecture and standards
    - Cybersecurity Workforce
    - Case Study 3: Frameworks for professional cybersecurity training and certification programs
- Risk management, testing, and incident response and recovery approaches
    - Methods for monitoring cyber resilience
        - Risk specialists assess information security management and controls
        - Jurisdictions are increasingly engaging with industry to address cyber resilience
    - Testing of information security controls and independent assurance
        - Mapping and classification of business services should inform testing and assurance
        - Penetration Test
        - Taxonomy of cyber risk controls
    - Response and recovery and exercise tests
        - Service continuity assessment, response and recovery plans, and continuous learning
        - Joint public-private exercise
        - Case Study 4: “Exercise Resilient Shield”
    - Cybersecurity and resilience metrics
        - Cybersecurity and resilience metrics
        - Emerging Resilience Indicators
- Communication and information exchange
    - Overview of cross-jurisdictional information sharing frameworks
    - Sharing information between banks or peers
    - Case Study 5: FS-ISAC: key features and benefits
    - Sharing from banks to regulators
    - Sharing between regulators
    - Case Study 6 - Bilateral exchange of cybersecurity information between the Hong Kong Monetary Authority (HKMA) and the Monetary Authority of Singapore (MAS)

Cyber Risk Management

Module 2: Cyber Risks

- Current Vision of Cyber Risk
- Identification of cyber risks
    - Malware and other threats
- Cyber-Security in practice
    - Security Government
    - Risk management
    - Security politics
    - Safeguards Policy
    - Contingency Plans
- Security Audits
- Some Cyber risks
    - Exploit Kits
    - Information leakage
    - phishing
    - DDoS attack
    - internet of things
    - infrastructure attack
    - botnets
    - trojans
    - Advanced Malware
    - Ransomware
    - APT's
- Avoidance, Acceptance, Mitigation or transfers of Cyber-Risks (Cyber-Insurance)
- Incident Response
- Legal Aspects of Incident Response
- Computer forensics
- Digital Compliance
- Intelligence in Open Sources
- Brand Defense. Intellectual Property Rights
- Digital Reputation. Crisis Communication
- Fraud and Online Identity Management
- Computer Law and ICT's
- Procedural Law and Human Rights in Cyber-Space
- Penal responsibility of juridical persons
- Cryptography and Authentication Systems
- Industrial Cyber-Security (IT/OT)
- Logic Cyber-Security
- Assurance
- Cyber risks in banking
- financial robberies
- Attacks on banking transactions
- credit card theft
- Wholesale Banking
- Lazarus cyber attack on the SWIFT system
- Bank resources allocated to cybersecurity
- Cloud service provider (CSP)
- Analysis of the main CSP providers
- Analysis and duration of blackouts in the Cloud service

Module 3: Cyber Risk Management

- Enterprise Risk Management in cyber risk
- Involvement of senior management
- Cybersecurity in business processes
- Identification of:
- Critical bank assets
- critical business functions
- Critical business partners: customers, suppliers, outsourcing
- Critical data, critical connections
- Main threats to the bank
- Framework for Improving Critical Infrastructure Cybersecurity NIST
- Main technical standards
    - NIST 800-53
    - Cobit 5
    - ISO 27001
- Policies and control of cyber risk
- Governance of Cyber Risk in practice
- Lines of defense
- risk analysis
- Probability and impact maps
- CyberRisk mitigation strategies
    - Identity and access management
    - data protection
    - Security analytics using machine learning
    - NIST CSF pillars
    - safety hygiene
    - Recovery time objective
    - Recovery point objective
    - SSDLC
    - Risk management of third-party technology
- Security architecture
- Cloud environment and mobile security

Module 4: Measuring Cyber Attacks using XOI Approach: Exposure, Occurrence and Impact

- Exposure definition
- Selection of KRIs
- Exposure modeling and conditioning
- Definition of hypothesis
- Modeling and conditioning of the occurrence
- Occurrence quantification
- Impact quantification
- Types of indicators
- Indicator predictability
- Bayesian networks
- The Bayesian Network Scenario Model
- graphic interpretation
- Simulation using Bayesian networks
- XOI modeling for Cyber risks in banking
- Cyber Risk Scenarios
- Banking cyberattacks
- **Exercise 1:** XOI modeling in cyberattacks using Bayesian networks in Python and R

Module 5: Cyber Risk Appetite

- Principles of an effective Cyber Risk Appetite methodology
- Definitions and analysis:
    - Risk appetite framework
    - Risk Appetite Statement
    - Risk Tolerance
    - Risk Capacity
    - Risk Profile
- Establishment of Limits in Cyber Risk
- Principles of Effectiveness of the Cyber Risk Appetite Statement
- Establishment of Limits and Metrics in Cyber Risks
- Establishment of risk limits and tolerance in CibeRiesgos
- Incorporation of Cyber Risk Appetite in decision making, new products, new lines of business, etc.
- Mitigation plans

Machine Learning and AI for Cybersecurity

Module 6: Machine Learning

- Artificial intelligence
- Definition of Machine Learning
- Machine Learning Methodology
    - Data Storage
    - Abstraction
    - Generalization
    - Assessment
- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning
- Deep learning
- Typology of Machine Learning algorithms
- Steps to Implement an Algorithm
    - Information collection
    - Exploratory Analysis
    - Model Training
    - Model Evaluation
    - Model improvements
    - Machine Learning in consumer credit risk
- Machine Learning in credit scoring models
- Analysis of main tools: R, Python, Microsoft Azure, SAS Enterprise Miner, SAS Visual Analytics, Knime, IBM SPSS Modelller, Spark, etc.

Module 7: Artificial Intelligence AI for Cyber Security in Banking

- AI artificial intelligence for cybersecurity
- Detection of cyber security anomalies
    - Advanced deep learning models
- Use of Supervised Learning in cybersecurity
- Use of Unsupervised Learning in cybersecurity
- Detection and mitigation of Phishing
    - SVM
    - Clustering
- Deep Learning for the detection of attacks and malware
    - Recurrent Neural Networks
- Intrusion detection

- Network Traffic Analysis
- botnet detection
- Machine learning to detect DDoS attacks
- Detection of fraud in financial transactions
- Detection on sensors
- Banking fraud analytics
- Advanced machine learning techniques for cybersecurity
- Main vendors of AI for cybersecurity
- Visualization tools
- Benefits of AI in cybersecurity
- Growth of AI in cybersecurity
- Challenges and limitations

Module 8: Cybersecurity and Advanced AI

- Suspicious Activity Detection
- Machine learning algorithms for intrusion detection Malware detection using transformers and BERT
- Detection of fake reviews
- Machine generated text detection
- Fake news detection with graphical neural networks
- Attack models with adversarial machine learning
- Developing robustness against adversary attacks
    - Adversarial machine learning
    - Adverse attacks for cybersecurity
    - Adverse attack typology
    - adversary samples
    - Generative Adversarial Network (GAN)
    - Fast Gradient Sign Method (FGSM)
- Creation of adversarial malware samples using GAN
- User privacy protection with machine learning

Quantum computing

Module 9: Quantum computing and algorithms

Objective: Quantum computing applies quantum mechanical phenomena. On a small scale, physical matter exhibits properties of both particles and waves, and quantum computing takes advantage of this behavior using specialized hardware. The basic unit of information in quantum computing is the qubit, similar to the bit in traditional digital electronics. Unlike a classical bit, a qubit can exist in a superposition of its two "basic" states, meaning that it is in both states simultaneously.

- Future of quantum computing in insurance
- Is it necessary to know quantum mechanics?
- QIS Hardware and Apps
- Quantum operations
- Qubit representation
- Measurement
- Overlap
- Matrix multiplication
- Qubit operations
- Multiple Quantum Circuits
- Entanglement
- Deutsch Algorithm
- Quantum Fourier transform and search algorithms
- Hybrid quantum-classical algorithms
- Quantum annealing, simulation and optimization of algorithms
- Quantum machine learning algorithms

Module 10: Introduction to quantum mechanics

- Quantum mechanical theory
- Wave function
- Schrodinger's equation
- Statistical interpretation
- Probability
- Standardization
- Impulse
- The uncertainty principle
- Mathematical Tools of Quantum Mechanics
- Hilbert space and wave functions
- The linear vector space
- Hilbert's space
- Dimension and bases of a Vector Space
- Integrable square functions: wave functions
- Dirac notation
- Operators
- General definitions
- Hermitian adjunct
- Projection operators
- Commutator algebra
- Uncertainty relationship between two operators
- Operator Functions
- Inverse and Unitary Operators
- Eigenvalues and Eigenvectors of an operator
- Infinitesimal and finite unit transformations
- Matrices and Wave Mechanics
- matrix mechanics
- Wave Mechanics

Module 11: Quantum Number Error Correction Circuits

- Classical error-correcting code versus quantum error
- Correction code
- Quantum error correction circuit
- Quantum Error Correction Code Operation
- Types of Blunder in Quantum Computer
- Bit Flip Code
- Stabilizing elements that detect errors
- Barriers in the existing error correction method
- Flip Code Phase
- Phase Flip Code Quantum Circuit Implementation
- Bit Flip and Phase Flip Code
- Bell States
- QCL implementation of quantum error correction code
- Applications of quantum error correction circuits
- Simulation setup
- Implementation of hardware systems
- Quantum key distribution
- Spin or polarization
- Quantum cryptography using the XOR operator
- Pseudocode for the proposed quantum cryptography
- Random substitution
- Main highlights of arbitrary replacements
- Key development calculation in XOR encryption
- Hybrid replacement
- Advantages of the proposed quantum cryptography
- Error detection

- Hardware configuration
- Pseudocode
- Receiver code flow
- Transmitter code flow
- Simulation setup
- Receiver Configuration

Post-quantum and quantum cryptography

Module 12: Quantum Communications

- Information Theoretical Security
- RSA-129
- Grover's algorithm
- Shor's algorithm
- Fourier Transform algorithm
- Quantum Key Exchange
- Quantum networking
- SIGINT and encryption adoption
- Secret sharing
- Quantum Random Number Generation (QRNG)
- The NIST Randomness Beacon
- Quantum key distribution
- BB84
- How QKD works
- Why QKDI is secure
- Quantum Money
- Quantum Computing and Bitcoin
- QKD gains momentum
- QKD Commercialized, Miniaturized
- Quantum internet

Module 14 : Quantum proof of the financial system

- The quantum cyber threat to central bank IT systems
    - Why quantum computing poses a cyberthreat
    - The potential threat to current cryptographic techniques
- How to defend against the quantum threat
    - An international cooperation organized by NIST
    - Solutions can be implemented now
- How to prepare and create safe quantum environments
    - Post-quantum cryptography vs quantum cryptography
    - Central banks must prepare now
- Project Leap
    - Objectives and scope
    - solution designs
    - Implementation and testing
- Findings
    - Cryptographic agility
    - Performance
    - Security
- Conclusion and next steps
- Need for a migration plan
- Implementation challenges
- Next steps

Module 15: Quantum cryptography and quantum key distribution

- Fundamentals of Quantum Cryptography
- Heisenberg's uncertainty principle
- Quantum entanglement
- Photon polarization
- Quantum no cloning theorem
- Quantum key distribution
- Quantum key distribution based on prepare and measure
- BB84 protocol
- Other protocols based on prepare and measure
- An entanglement-based quantum key distribution
- Ekert's protocol
- Tangled BB84 variants

Module 16: Post-quantum digital signatures and Lattice Based Cryptography

- Introduction
- Digital signatures and their security
- Secure signatures in ROM
- Modeling of the quantum adversary
- NIST PQC Standardization Competition
- Lattice Based Cryptography
- Introduction to Ring-LWE
- Discrete Gaussian sampling
- NTRUSign
- GPV Framework
- Fiat-Shamir with cancellations
- Scheme of signature CRYSTALS-DILITHIUM
- MQ-based signatures
- Hard MQ-based problems
- Oil and vinegar firms
- HFE signatures
- Signatures based on symmetric key techniques
- Signatures based on supersingular isogenies

Cloud computing

Module 17: Cloud computing and security risks

- Models Overview
- Security Risk Assessment Frameworks
- Cloud Risk Assessment Models
- Cloud Adoption Risk Assessment Model
- Consultative, objective and bi-functional risk analysis
- Cloud Risk Assessment Frameworks
- Cloud Security Risk Management Framework
- Information Security Risk Management Framework
- Security Risk Assessment Framework
- Performance analysis of existing models and frameworks

Physical Cyber Risks

Module 18: Physical cyber risk

- Cyber deterrence
- Understanding physical cyber risk
- The threat to business

- The art of the possible: what physical cyberattacks can and cannot do
- cyberphysical scenarios
- A note on the classification of cyber powers
- Scenario 1: Sharing Asymmetric Attacks: Ransomware on Critical Infrastructure
- Scenario 2 – Offensive Cyber Retaliation: Cyber-Physical Sabotage of Critical Infrastructure
- Scenario 3 – Sharing Symmetrical Attacks: Escalation of Destructive Attacks on Critical Infrastructure
- Cyber physical insurance

Module 19: Vulnerability Interdependence Assessment Risk Analysis In Cyber-Physical Systems

- Threat Control Perspective
- Methods to map the severity of the outbreak
- Outbreak severity quantitative method
- Quantitative method of probability of achieving an outbreak
- Impact of vulnerabilities and mode of use
- Attack modeling in a CPS
- Online monitoring in a cyber-physical system

Emerging Risks: Geopolitical and Reputational

Module 20: Cryptocurrency, cybersecurity and green energy

- The geopolitics of crypto currency
- Green energy impact
- Applying lessons from history to a new context
- Measurement of cybersecurity in geopolitical risk
- Climate change, renewable energy and geopolitical risk reconfiguration
- Cryptocurrency, decentralized finance, and the global balance of power

Module 21: Measurement of Geopolitical Risk

- Geopolitical risk measurement
- Artificial intelligence applied to geopolitical risks
- Machine Learning and Deep Learning
- Quantitative versus qualitative approaches
- Geopolitical risk ratings
- Identify early warning signs
- Identify key issues
- Interpretation of trends in financial and economic data.
- Manage information
- Creation of geopolitical indexes
- Analysis of the main indices
- Possible biases in the indices
- Typology of articles for index improvements

Module 22: Measurement of Reputational Risk

- Definition and nature of Reputation
- Identification of reputational risk
- Reputational risk assessment
- Stakeholder expectations
- Risk areas and stakeholder categories
- Internal Reputational Risk
- External Reputational Risk
- Assessment through scenarios and impact
- Use of Risk Control Self Assessment in reputational risk
- Important KRIs of Reputational Risk
- Practical case of presenting results to Senior Management

Module 23: Advanced Measurement of Reputational Risk (RR)

- Advanced modeling of reputational risk
- List of operational risk events
- Financial variables that influence the RR
- Probability of Reputational Risk
- Logistic regression modeling

Module 24: Advanced Reputational Risk Management

- Governance of reputational risk
- Roles and Responsibilities of the Board, CEO, CRO and CFO
- Expectations and Management of Stakeholders
- Integration of reputational risk in the Risk Appetite Framework
- Assessment through scenarios and impact
- Traffic Light analysis of probability and impact
- Reputational Risk Reporting
- Reputational Risk Mitigation
- Impact of the social environment
- Relations with NGOs and the Media
- Key points in reputational risk management
- Other themes:
- Online Reputation Management
- Social reputation in banking

Cybersecurity, Geopolitics and quantum technologies

Module 25: Cybersecurity, Geopolitics and Scenarios

- The global cyber landscape
- Geopolitics
- Emerging technology
- Emerging threats
- Laws and regulations
- Threat modeling
- Future scenarios of quantum technology
- Scenario 1: Superior and Dominant Government
    - Cryptanalysis
    - Forged signatures and legal systems
    - Attacks on Passwords and Other Authentication Systems
    - Remote sensing
    - QKD and the quantum internet
    - Secret and leak
    - Countermeasures in a Government-Dominated Setting: Disruption, Denial, Degradation, Destruction, and Deception
- Scenario 2: Quantum technologies could change governance and the law
    - Implications for human primacy
    - Quantum Technology and Space Law
    - Quantum Technology and Cybersecurity

- Quantum technology and privacy
- Secrets and their value in time
- decryption regulation
- Government Power Challenges
- The European approach to privacy rights
- quantum prediction
- Product development
- Justice
- Quantum Technology patent output
- Quantum computing winter is a likely scenario for 2030

- Stage 3: Public/Private, East/West Block
- Scenario 4: quantum winter
- Scenario 5: LK99 Super Drivers

www.quantumaidea.com

julia.tsedryk@fermacrisk.com