
**3rd ICT Security in Financial Institutions Conference
Fighting Cyber Crime**

Co-organised by the Institute of Banking Education NBS and the
Banking Association for Central and Eastern Europe (BACEE)

6-7 June 2017, Bratislava

PROGRAMME

DAY 1 (6 June 2017)

OPENING SESSION

SESSION 1: FINANCIAL STABILITY RISKS FROM RISING CYBER SECURITY CHALLENGES

Evolving security landscape
Cyber Crime
Cyber Security

SESSION 2: ICT SECURITY INCIDENTS, BREACHES AND THEIR IMPACT ON FINANCIAL INSTITUTIONS

Account takeovers and identity theft
DRP issues, telecommunication network disruptions and third-party payment processor breaches
Malicious software
ATM skimming/point-of-sale attack schemes
Social engineering techniques: phishing, pharming, vishing and smishing
Banking trojan horses, available botnets and zombies

SESSION 3: ROUNDTABLE DISCUSSION: UNDERSTANDING THE SCOPE OF THREAT AND DESIGNING AND MANAGING EFFECTIVE INFORMATION SECURITY FRAMEWORKS AND PROGRAMS

Written information security policy, requirements on formalized security documentation
Information security audit frameworks and key risks indicators
PCI DSS requirements
Comprehensive communications plan to respond to inquiries in the event of a breach

SESSION 4: DATA PRIVACY AND INFORMATION SECURITY

The EU General Data Protection Regulation
Compliance and audit
Assessment and management of risk from third party vendors

DAY 2 (7 June 2017)

SESSION 5: PREVENTIVE SYSTEMS AND CONTROLS TO ADDRESS EMERGING THREATS

Spyware and malware detection
Firewalling, network segmentation principles
Server-based access control lists
Role-based access control
Network admission control

SESSION 6: CYBER DEFENSE: THE LATEST SECURITY TECHNOLOGY

Intrusion prevention and intrusion detection
Vulnerability scanning tools
Encryption for data in transit
Data loss / data leakage prevention
Fraud detection systems

SESSION 7: ROUNDTABLE DISCUSSION: ETHICAL HACKING

Bulding an effective pen testing function
Market for security audits
Potential risks of Darknet