Cyber Resilience Investigation

9-th Conference on Payment and Securities Settlement Systems
6-8th June 2016

Division of Supervision, Banking Regulations and Financial Stability
& Payment Systems Department

National Bank of the Republic of Macedonia

Agenda

1	**New trends, threats and risks**
2	Activity of the National bank
3	Cyber-risk preparedness tool and Investigation

New trends – threats and risks

- **Computer crime,** or **cybercrime**, is crime that involves a computer and a network. (**Wikipedia**)
- Cybercrime – **high income for relatively low price and risk** for criminals.
- Cybercrime damages trade, competitiveness, innovation, and global economic growth.
- The most important cost of cybercrime, however, comes from its **damage to company performance** and to **national economies**.

New trends – threats and risks

- Rapidly increased number of digital transactions worldwide and number of companies that performed their activities over internet (cheap processing power and available memory in cloud).

- Internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly.
  (Source McAfee: Estimating the Global Cost of Cybercrime-Economic Impact of cybercrime- Center for strategic and international studies, June 2014)

- 5 billions of devices are connected to Internet in 2015, 25 billions devices are forecast for 2020. (Gartner)

New trends – threats and risks

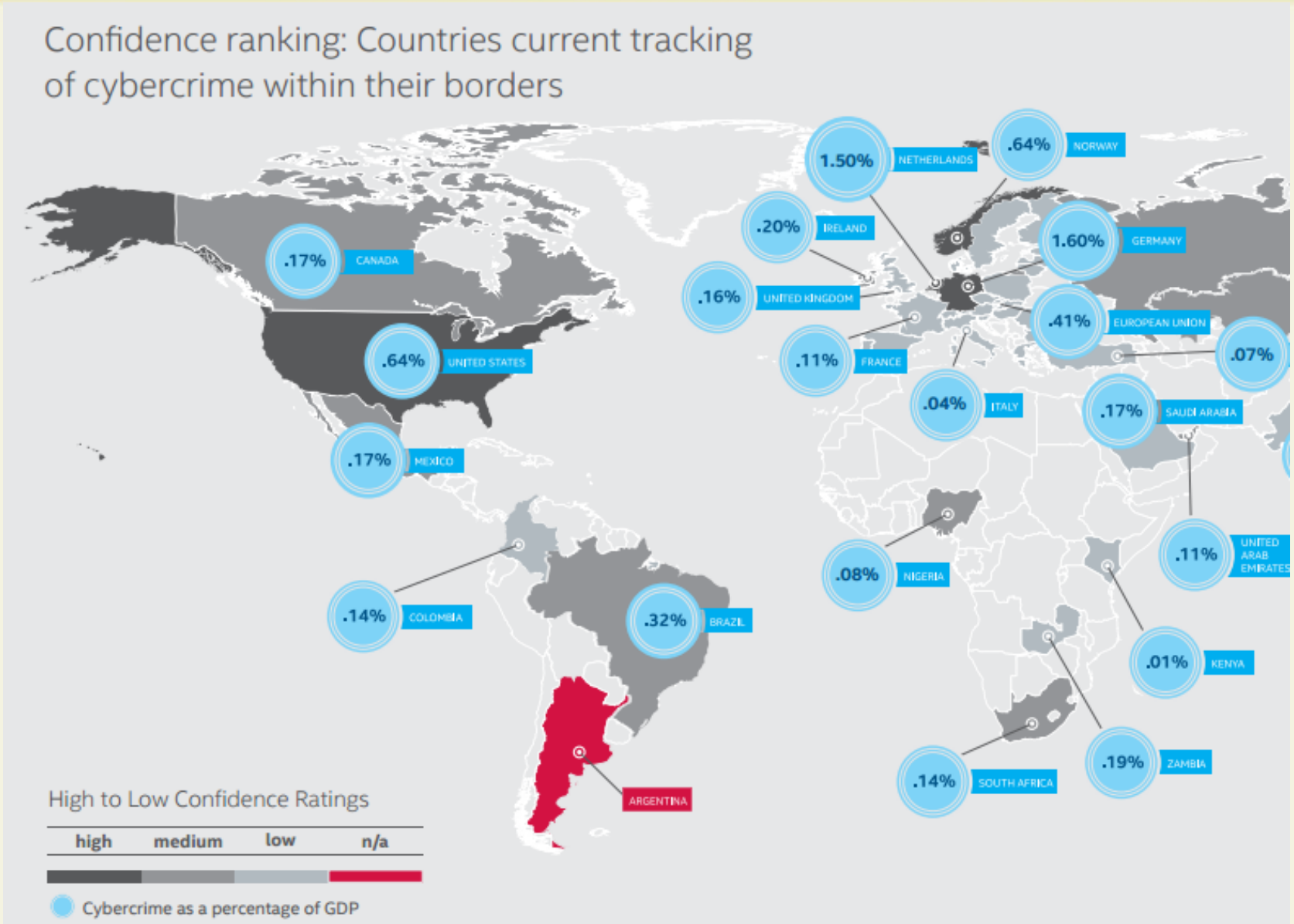
Cybercrime main targets:

- **Stealing of intellectual property** – main target are companies that are dominantly connected with research and development, industry and pharmacy (very hard to calculate loss in $-big losses in revenue and market)

- **Stealing of financial assets** through unauthorized access to financial institutions and merchants where big number of online transactions are made. Transfer of the cash is done by mules. Big organized group.

- **Stealing of confidential or privileged information** in order to make a manipulations to financial markets

New trends – threats and risks



New trends – threats and risks

- G20 nations and largest economies in the world suffer the bulk of losses and losses from cybercrime (the US 0.64%, China 0.63%, Japan and Germany 1.6% of GDP).

- Wealthier countries (avg. 0.9% of GDP) are more attractive targets for hackers but they also have better defenses. Less-developed countries are more vulnerable.

- Low-income countries (avg. 0.2% of GDP) have smaller losses, but this will change as these countries increase their use of the Internet and as cybercriminals move to exploit mobile platforms

- **Annual losses exceed 200 Bilion $** (10%-20% of total digital economy).

New trends – threats and risks

- Cybercrime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors.

- **Cybercrime is industry on rise.** Annual losses to global economies are estimated beyond 200 billions $ and are presented as % of state GDP.

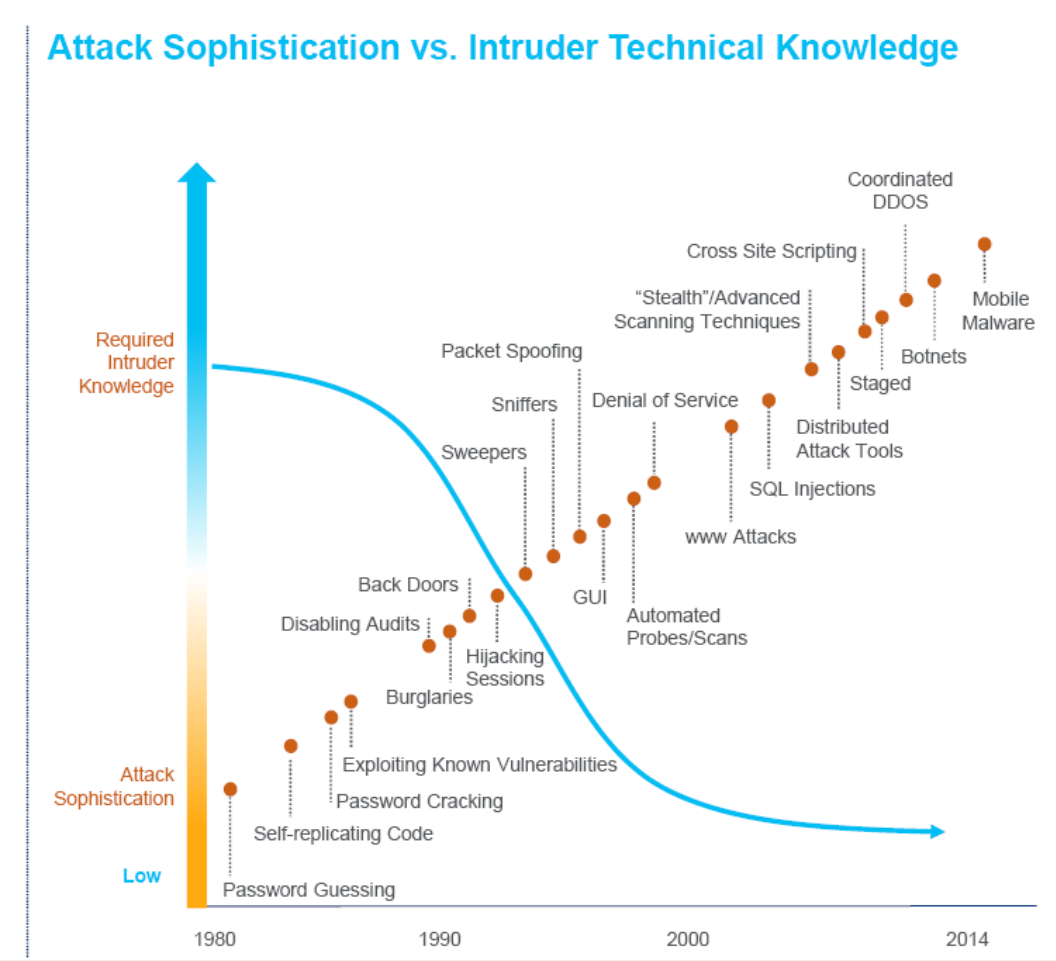
- Companies are not aware or they are not reporting losses suffered from cybercrime.

New trends – threats and risks

- Using old legacy systems and known weaknesses of IT systems that are not security patched
  - Regular security upgrades of security weaknesses it is not performed regularly
- New platforms are creating new possibilities for attackers and new risks are introduced
  - New ways to exploit IT systems of the banks and clients
- Very hard to find boundaries between crime actors (hacktivist, states, organized crime gangs, employees)
  - Commercialization of tools, resources and infrastructure
- More advanced tactics based on online behavior and social patterns
  - Social networks are introducing more efficient and targeted attacks (spear phishing)
- More advanced malicious applications
  - Destructive application and ransomware software

New trends – threats and risks

- Technical knowledge to make sophisticated attack is very low and threats are more instance and severe
- Recent attacks are showing that attackers are having good knowledge of infrastructure and systems who are attacked
- Hackers are attacking clients, but also suppliers and outsourcing companies

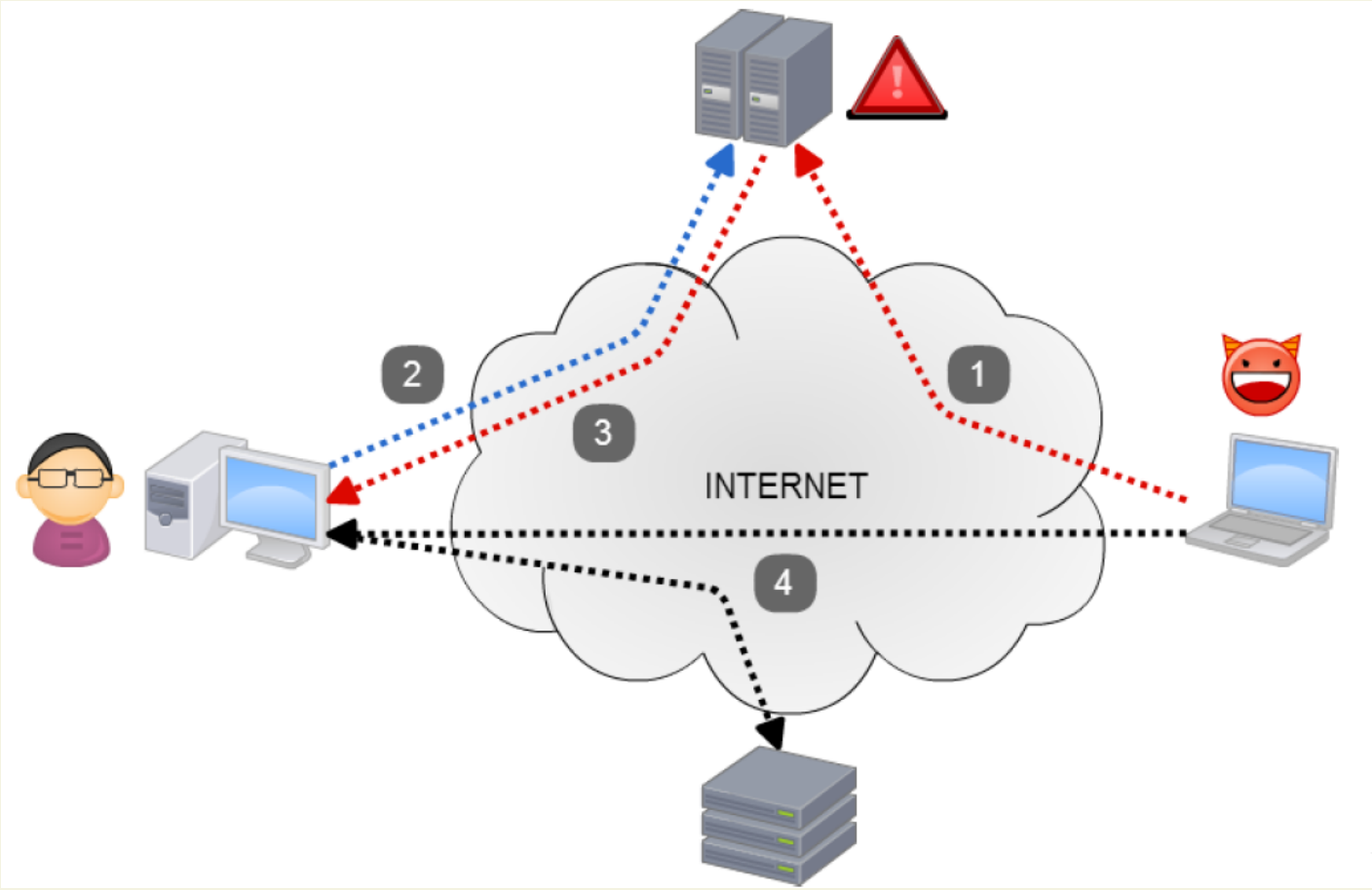


New trends – threats and risks

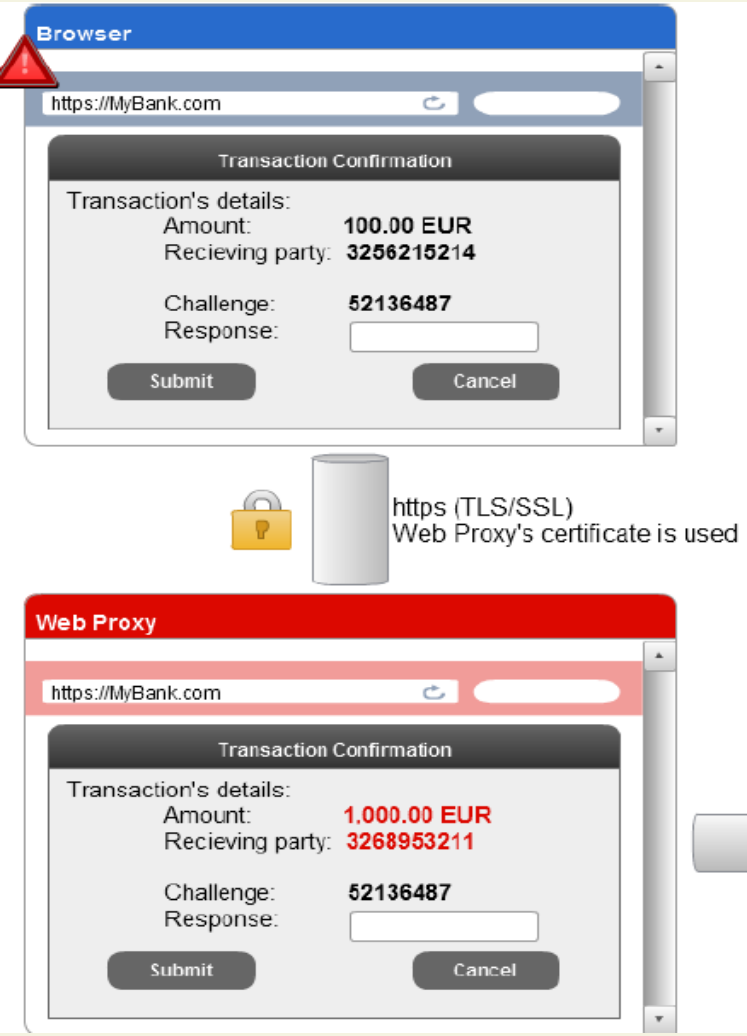
Man-in-the-Browser (MitB) Zeus Malware

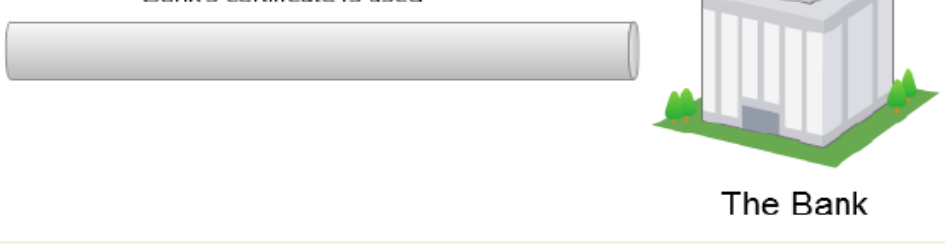
- #1 threat of online banking

(source: http://youtube.com/watch?v=4bPlAFZajuo https://www.youtube.com/watch?v=DUnZMwXCkyw)



New trends – threats and risks





- Client send a payment instruction, attacker dynamically change amount and beneficiary account in the background
- Data are encrypted in the transfer
- Possible indicators:
  - Extra request in the e-banking application to enter your credentials (on the places that were not asked previously)
  - Possible certificate error
- Payment orders generated on this way are valid and generated through the e-banking system are ready to be sent through payments system

Agenda

1	New trends, threats and risks
2	**Activity of the National bank**
3	Cyber-risk preparedness tool and Investigation

Activity of the National bank

- Activity of the National bank in the previous time were mainly focused on:
  - Analyzing new threats and attacks in cyberspace in global and regional level
  - Informing the banks for risks of using old, legacy information systems including continuous using of Microsoft XP on working stations and ATMs
  - Special focus in performing the onsite examinations on :
    - Security of part of the information system for internet banking and inclusion of the system in the part of audit trail and log management system; providing budget for diverse testing from independent source
    - Integrity of the audit trail system is pre-request for the implementation of relevant "credible" internal source of intelligence for cyber-risk
    - Strengthening the process of the way bank is managing incidents (loss event database)

Activity of the National bank

- Recommendation of Basel, World bank and other central banks to strengthen the controls in this segments:
  - **Cyber resilience in financial market infrastructures (Committee on Payments and Market Infrastructures, November 2014)**
  - Cybersecurity Framework NIST (February 2014)
  - World Economic Forum Partnering for Cyber Resilience (2014)
  - World Bank Group (Financial Sector Advisory Center FinSAC) - Regional Cyber Security Issues and Options (May 2015)
  - FFIEC Cyber Preparedness Framework (2015)

Activity of the National bank

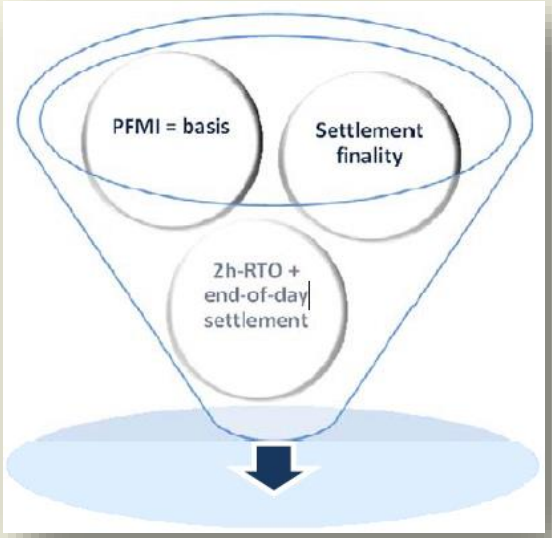
- **Key recommendations:**
  - National bank must ensure adequate, timely, and coordinated responses to prevent and recover quickly from such attacks. The financial services industry is one of the most targeted industries for malicious attacks, but cyber risks extend beyond the financial world and cyber threats cannot be addressed in isolation
  - Many governments and central banks (Bank of England, U.S, U.K.) and other fora of standard setters (BIS, International Organization of Securities Commissions (IOSCO), European Commission,), as well as industry groups (NASDAQ), and private companies (DTCC, Symantec), have flagged common sense measures
  - More sophisticated advice is being provided by some supervisors, specialized companies and industry groups, to enhance the protection of systemically important players and critical market infrastructure (ex., CBEST and the Bank of England, the ECB as well as the BIS)

Cyber resilience in FMIs

- BIS-CPMI report **"Cyber resilience in financial market infrastructures"** was issued in November 2014
  - Response to the more and more frequent, sophisticated and widespread cyber attacks against the financial system
  - FMIs should promote **stability and efficiency** in the financial system, nevertheless could address the risks to broader financial stability
  - Cyber risk falls within domain of **operational risk** (Principle 17) and **governance** (Principle 2)
  - FMIs consider a two-hour recovery time objective (**2h-RTO**), to recover operations quickly and settle activities by end-of-day even in extreme scenarios
  - FMIs support the **regulatory community** in the pursuit of effective solutions
  - Support of cyber resilience activities from **senior managers** at FMIs is very important!

Cyber resilience in FMIs

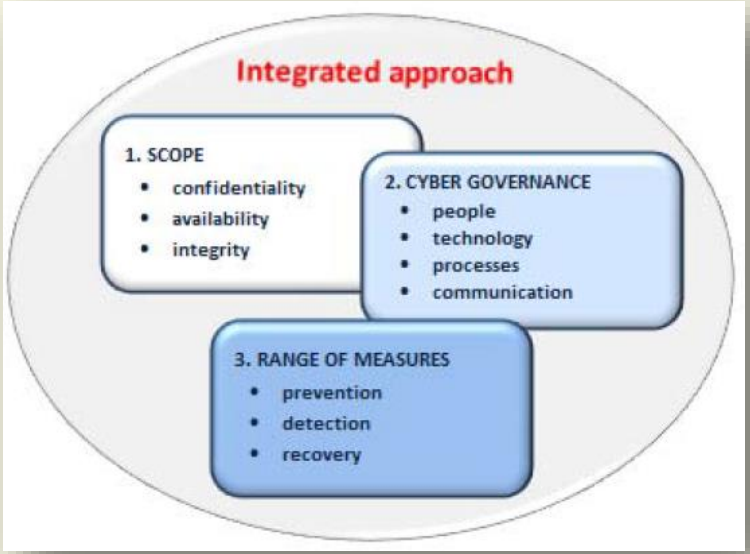
- **PFMIs are the basis** for the cyber-resilience, settlement finality has to be intact and the goal of 2h-RTO achieved
- **Attackers**: hacktivists, who seek merely to disrupt activity; cyber criminals motivated by financial gain; terrorists aiming to cause political and financial instability; and nation state-related actors attempting to interfere with or gain access to sensitive information, or to cause systemic instability
- Cyber resilience typically covers **three broad dimensions**:
  - **Scope**: confidentiality breach, an availability breach and an integrity breach
  - **Cyber governance**: covers FMI's IT infrastructure, people, processes and communication
  - **Range of measures**: (i) prevent (ii) detect an attempted or successful attack, and (iii) resume services



Cyber resilience in FMIs

- **Prevention**: identification, awareness, proper network and application security level, reduced access surface from outside/inside, malicious code prevention, access control and infrastructure control and development
- **Detection**: direct and heuristic monitoring and usage of checkpoints.
- **Recovery**: recover to normal or good-enough state, golden point, failing-backward, failing-forward, non-similar facility

– **Cooperative and/or coordinated** approach to cyber security is VERY important, in particular to share information on threat intelligence and forensics. **PFMI's Responsibility E** for authorities



Current practices and positions

- **Recent cyber-attacks in close region are identifying similar information security standards (natural persons are using OTP, legal persons are using digital certificates, similar practices and awareness)**
- **Clients are using old legacy information systems or they are not upgraded with the latest security patches and on such way they are on higher risk**
- Clients and employees in the banks are targets of social engineering and phishing attacks
- **Banks don't have systems for analyzing the behavior of the clients that are using information system to help prevent** fraud/attack from cyberspace
- **Banks do not have a protocol for exchange of the information with each other**
- Potential risks: financial, operational, legal and reputational. Costs may include forensic investigations, public relations campaigns, legal fees, consumer credit monitoring, and technology changes. ***In order to minimize this risk, National banks prepared comprehensive tool and performed a investigation in Q1 2016***

Agenda

1	New trends, threats and risks
2	Activity of the National bank
3	**Cyber-risk preparedness tool and Investigation**

Cyber-risk preparedness tool

- Main objective:
  - To help banks to identify their cyber-risks and determine maturity level in cybersecurity;
  - This tool can be used frequently in order to provide to the management: adequate metrics and repeatable process. This will make a process integrated in risk management process.
- Integrated in the tool:
  - Current standards for security of the information systems in our country
  - Best industry standards and practices in the field of cybersecurity
- Consist of two parts:
  1. **Assessment of inherent risk**
  2. **Choose adequate/preferable maturity level**

Assessment of Inherent Risk

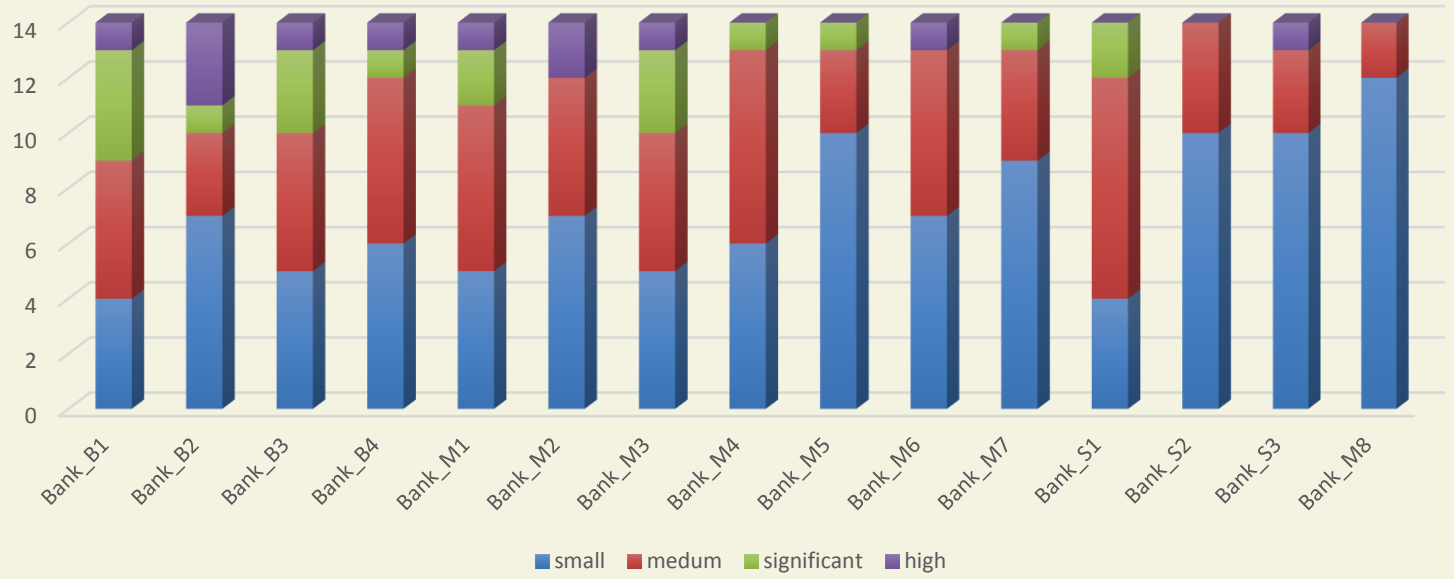
- Assessment of inherent risk in 5 Areas:
  - Technologies and Connection Types (applied information technology and connection types with external systems);
  - Alternative channels (open channels with clients to exchange information with clients, merchants and suppliers);
  - Products and technology services available on alternative channels (e-banking, m-banking, cards, etc.)
  - Organizational Characteristics and
  - External Threats.

- Assessment of inherent risk should take in consideration scope, complexity and products and activities which are performed in the bank. Consider the specific threats that are present in the environment.

- **Inherent risk does not include mitigating controls.**

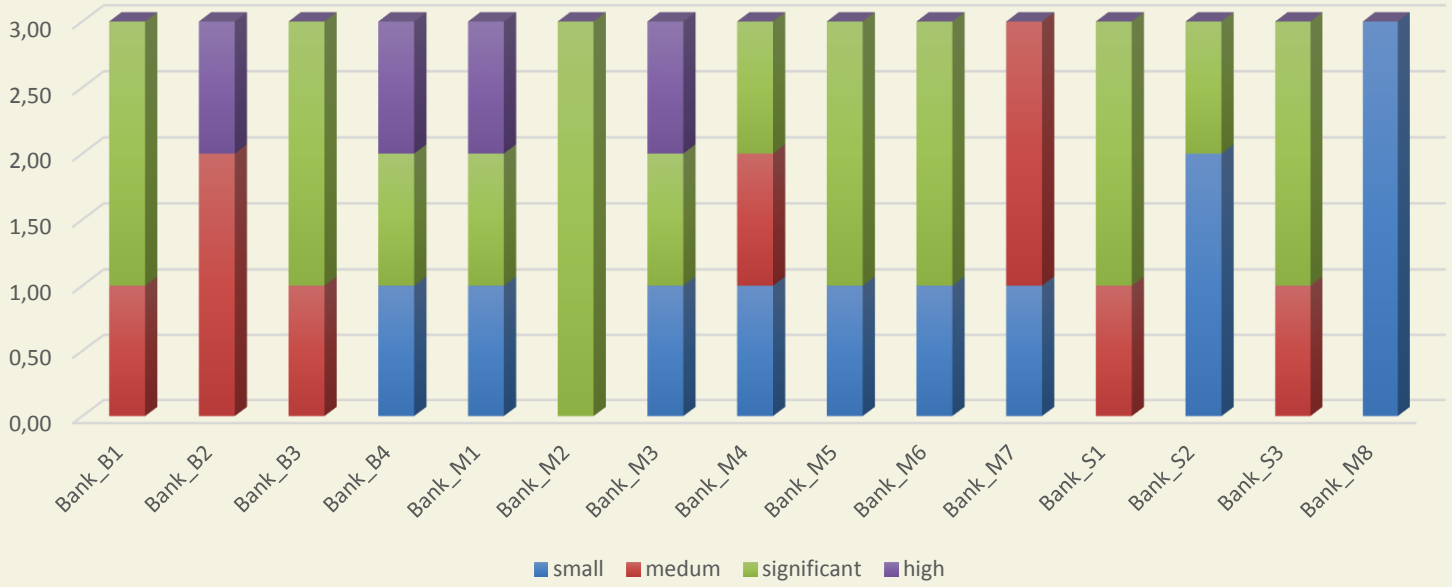
Cat.1: Technologies and Connection Types

- Complexity of IT system and interoperability and interconnections with other IT systems
- Identification of old legacy IT technologies, Wi-Fi devices and personal devices
- **General conclusions :**
  - **3 banks** are having higher risk than other banks in this category 1
  - **2 banks** are using old legacy Microsoft XP system in order to use their group core IT infrastructure
  - **1 bank** is also a processing center for card operation so they have a complex infrastructure



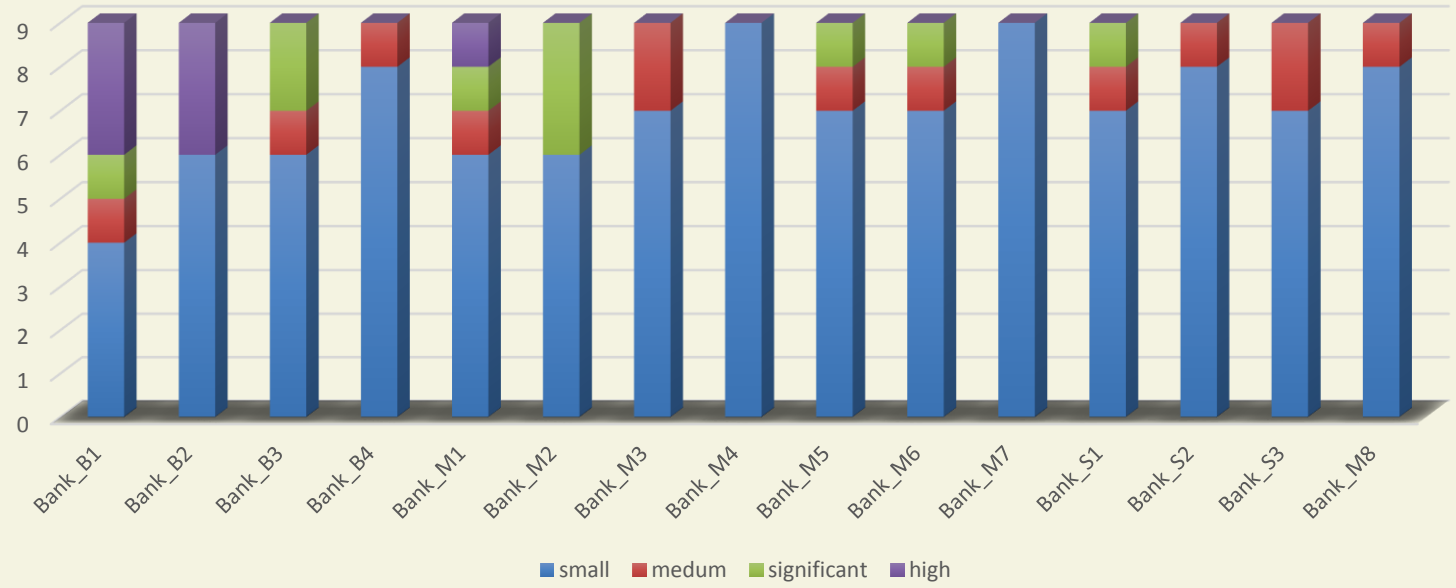
Cat.2: Alternative channels (exchange information with clients)

- Identify available alternative channels that financial activities can be processed
- e-banking, m-banking, advanced ATM application
- **General conclusions:**
  - **Majority of banks don't have limits and restrictions on payments through internet banking**
  - **6 banks** are using m-banking application for processing payments for physical persons limited on amount. Very well accepted by clients. Other banks will follow.
  - **National bank will closely follow risks associated with m-banking implementations** and eventually issue standards in this area



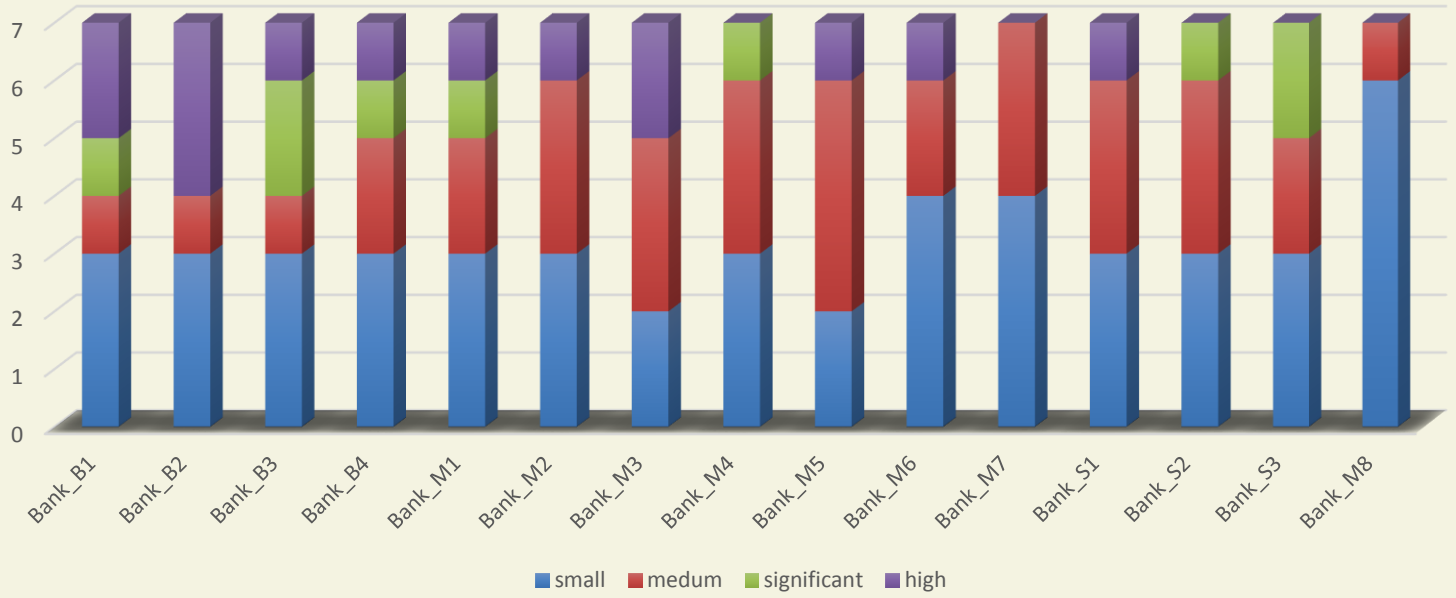
Cat.3: Products and technology services (quantity of payments through different platforms)

- Identification of portfolio of products that are available through alternative channels.
- **General conclusions:**
  - Systematically important banks are at higher risk in this category- large portfolio of products through different channels. Large numbers of accounts and wide network through POS systems in merchants
  - Different ways to transfer money from person to person and new innovative technology for transfer of funds



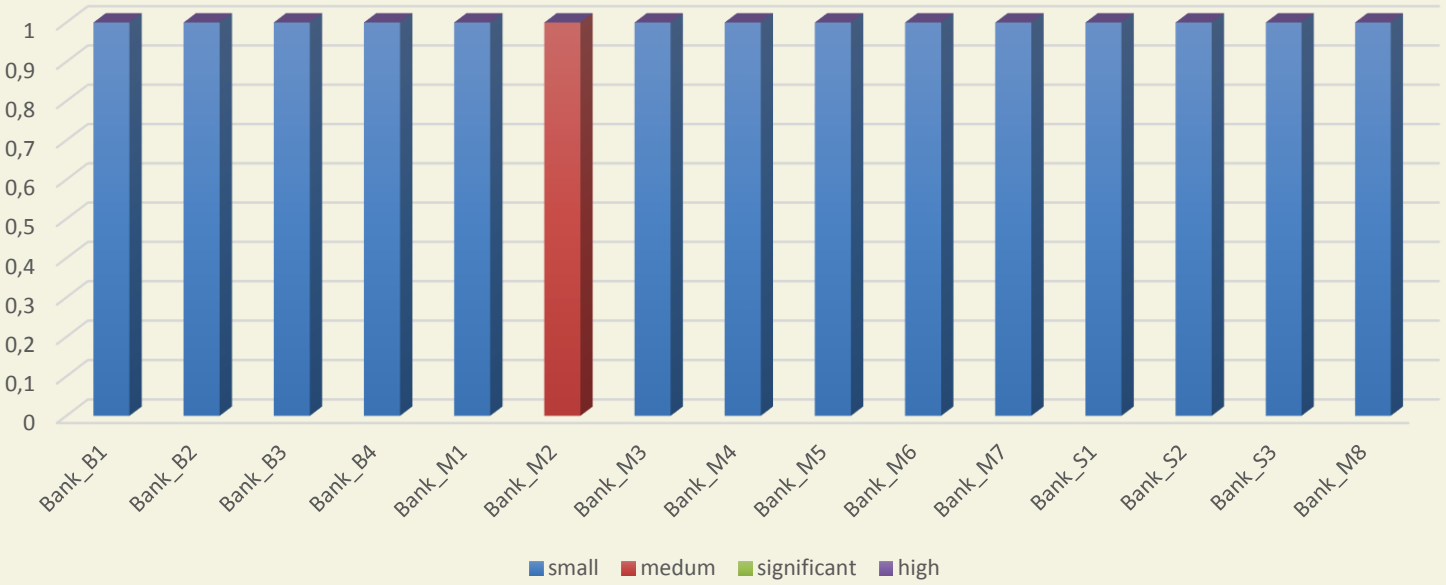
Cat.4: Organizational Characteristics

- Organization, complexity, frequency of changes in the infrastructure (hardware, software, key employees).
- **General conclusions:**
  - Systematically important banks are having complex organizational structure with large number of employees
  - IT systems are having frequent changes in their environment and regular updates from the manufacturer of the system
  - **In general banks are at medium risk in this category**
  - **Two banks are having biggest changes in their environment (evident transfer of professional personnel from one bank to another M3>M5)**



Cat.5: External Threats

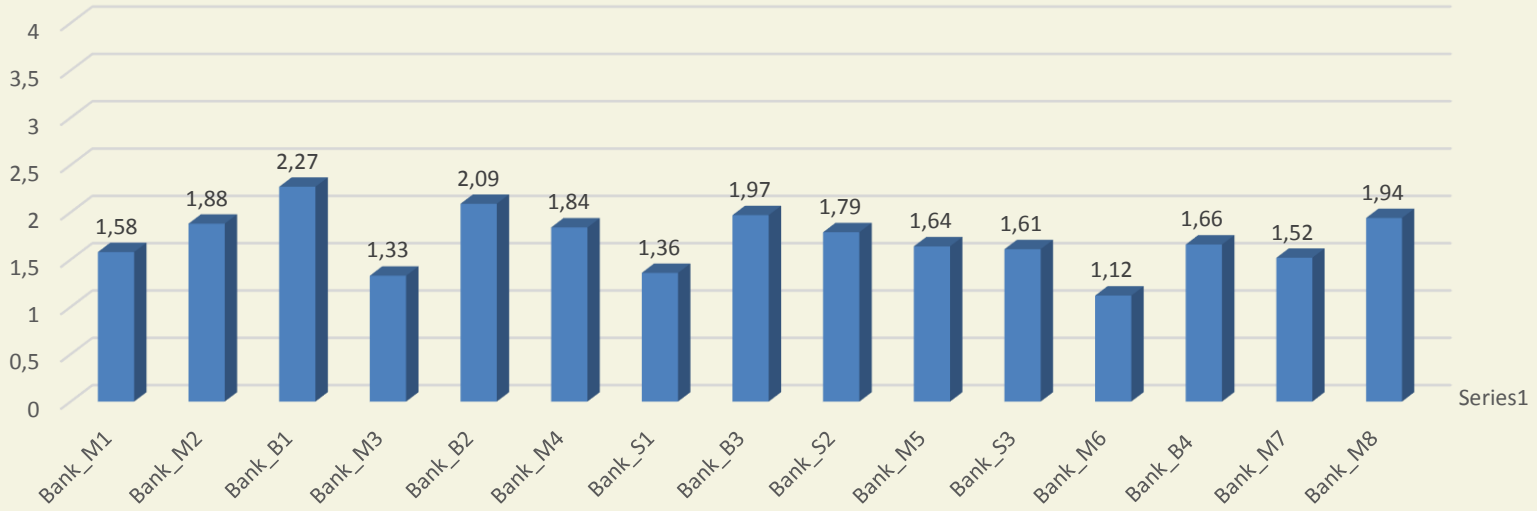
- Assessment of threats and attacks in the previous year. Is the bank attractive target?
- **General conclusions:**
  - Cyber attacks in the previous year were on very low scale. In general were phishing attacks on clients or employees
  - Only one bank is reporting higher level of attacks on monthly level more then 10 attacks and one major DDoS attack which interrupt IT system
  - **We are taking this answers with "reserve" because banks don't have external and internal threat intelligence for cyber incidents**
  - **Attack on clients side-changing instructions for beneficiary account on email (2014); ransomware (2015); etc**



Aggregate Inherent Risk

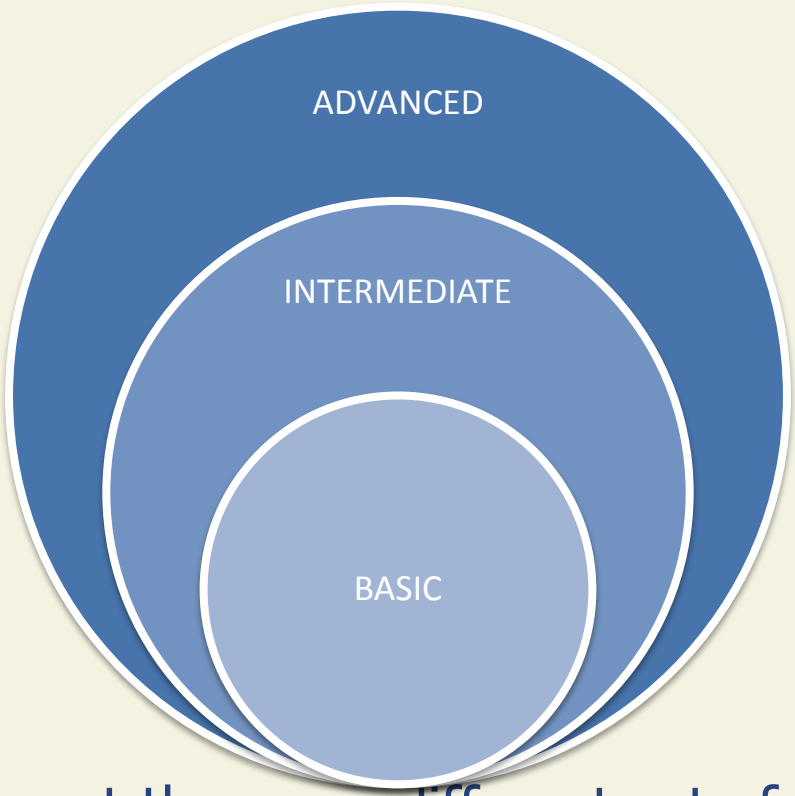
- **General conclusions:**
  - 3 banks are having **Low Inherent Risk** (score less then 1.5)
  - Other banks are having **Medium Inherent Risk** (score less then 2.5)

- **According to methodology:**
  - **3 banks will have to be BASIC cybersecurity maturity level**
  - **12 banks will have to choose BASIC or INTERMEDIATE level**



What is maturity model?

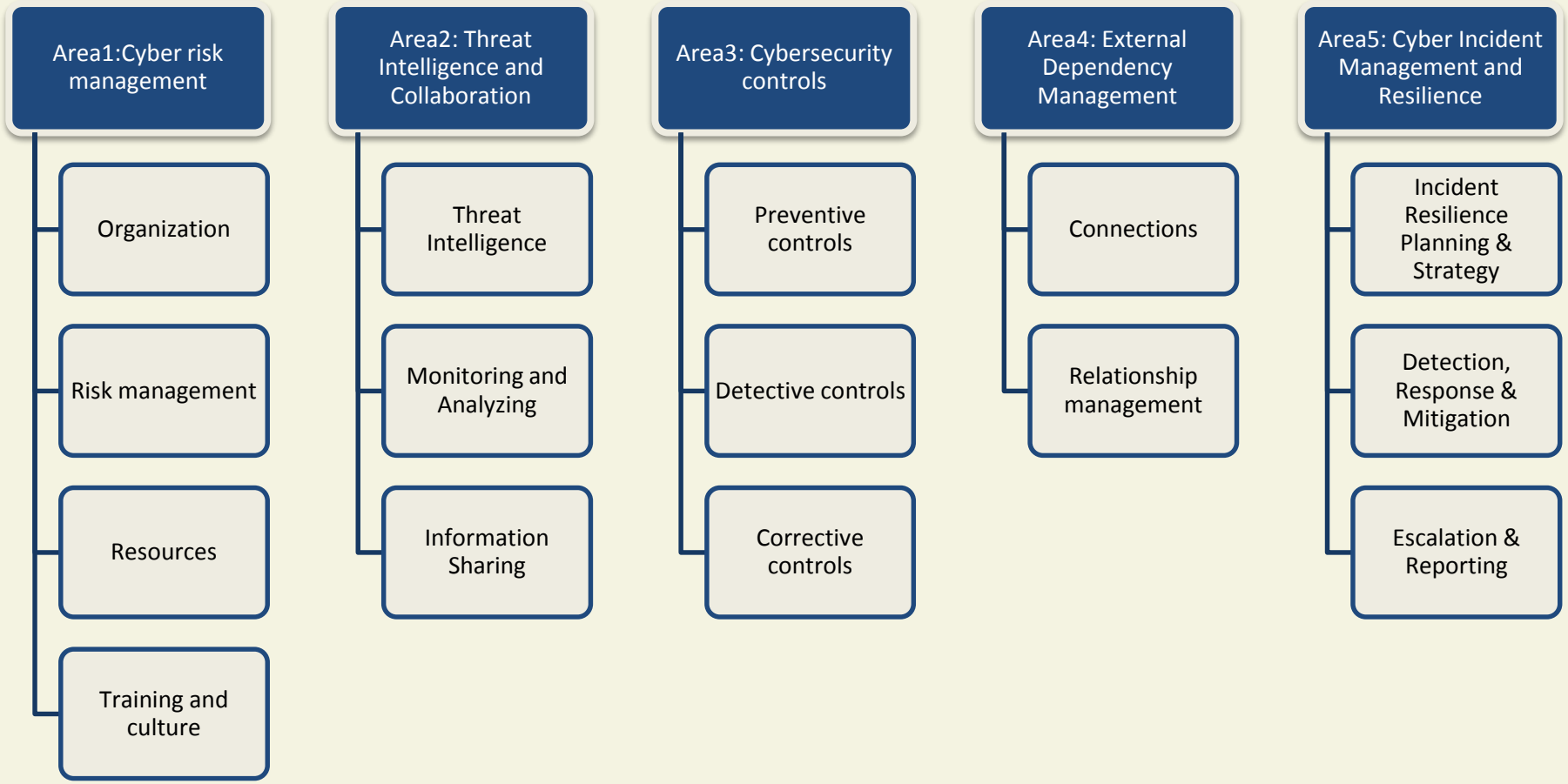
- Maturity level is categorized in three levels: basic, intermediate and advanced.



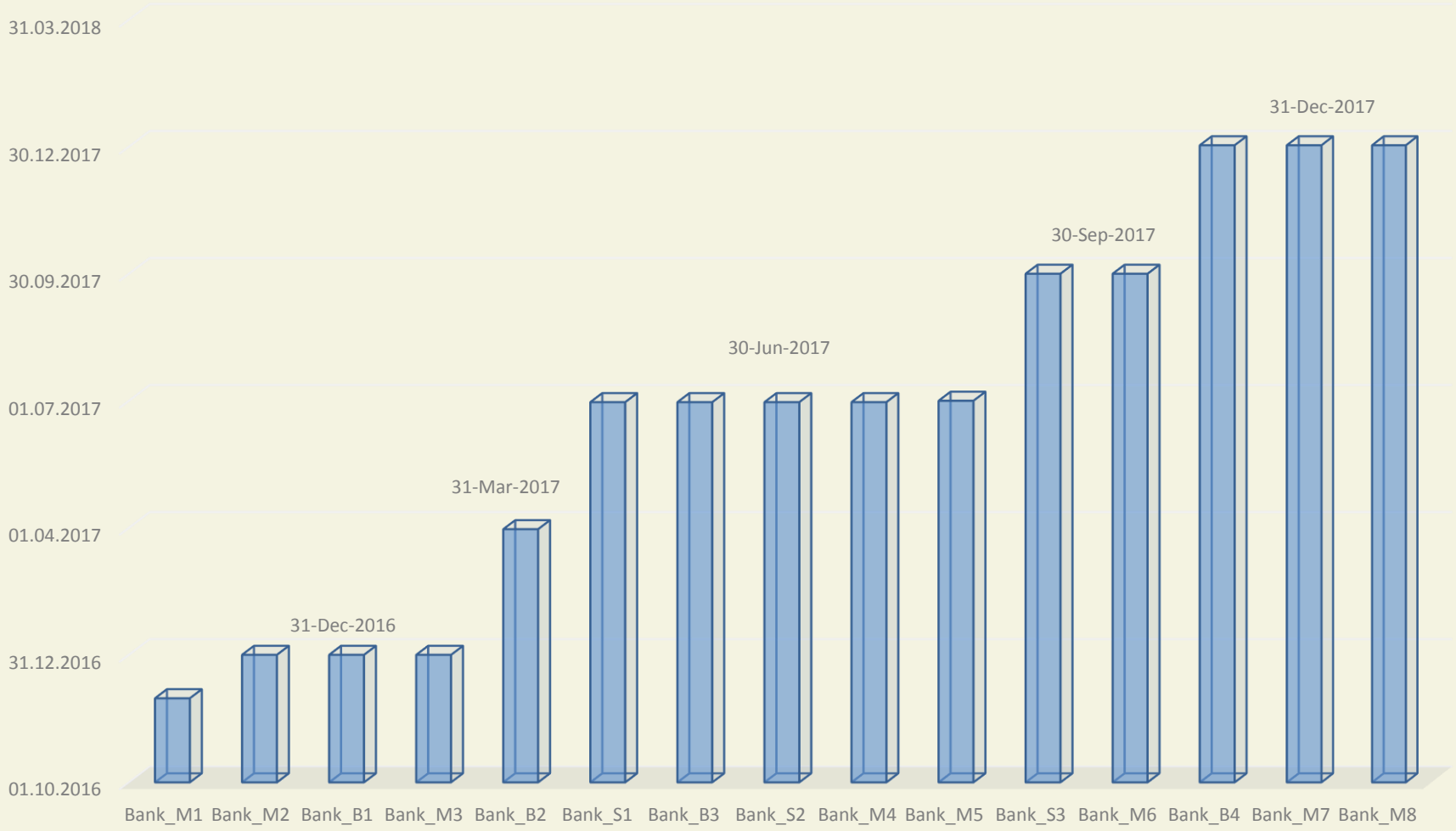
For each component there are different set of phrases developed for each maturity level. **That is customized by the central bank taking into account specifics in the financial system in the country.**

5 different areas to approach cyber security and measure the success

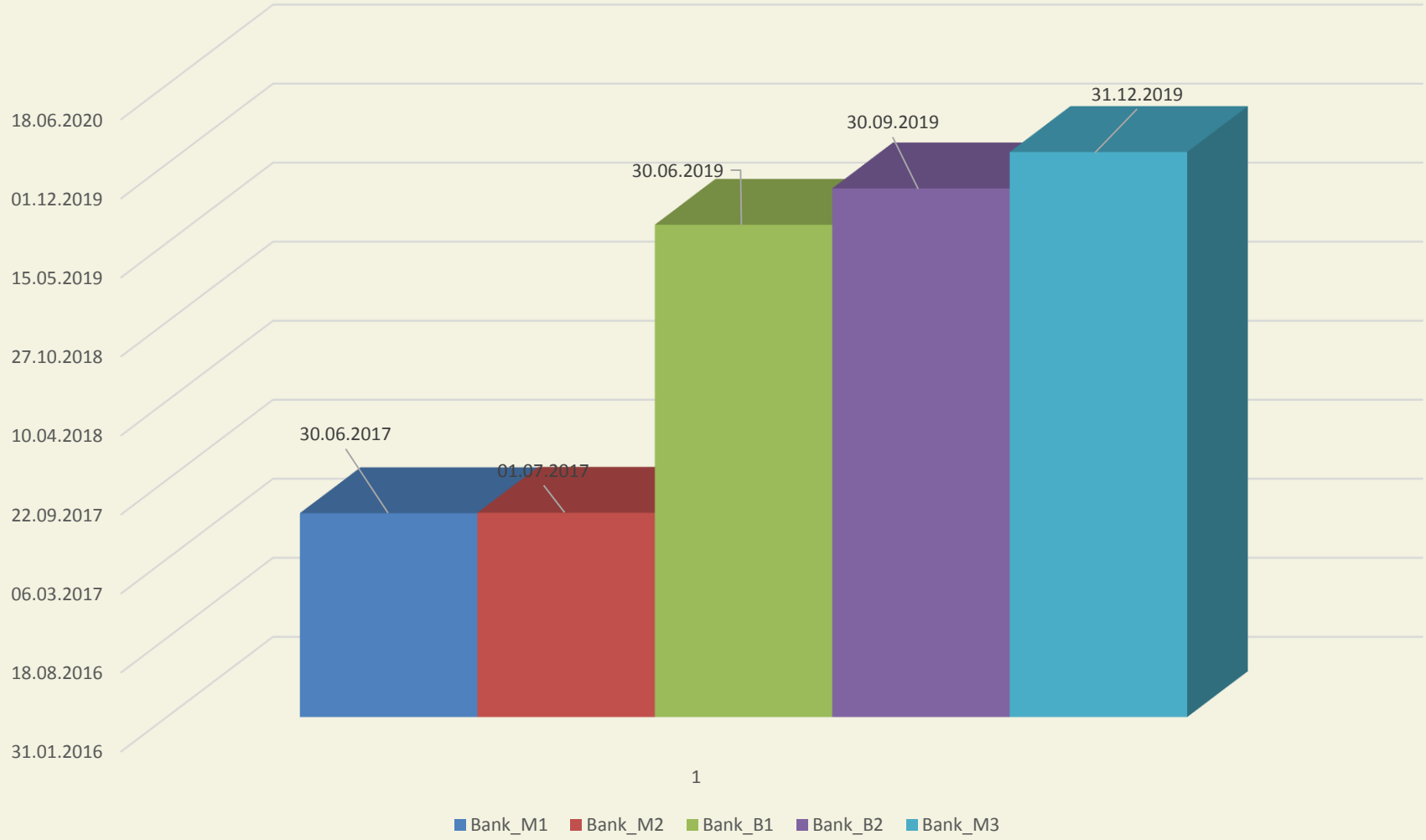
– Determine maturity level in five areas



Basic Level of Cybersecurity maturity timeframe



Intermediate Level of Cybersecurity maturity timeframe



Action plans are developed (1)

- Area 1 (Cyber Risk Management)
  - Strengthening the framework for risk management in the field of cybersecurity and integrating this process in the risk management process (policy, strategy, procedures, guidelines, training, awareness and corporate culture)
- Area 2 (Threat Intelligence and Information Sharing)
  - National CERT is established and the banks can apply for membership (central coordination of cyber incidents and response)
  - Special group under Banking Agency is established for sharing the security incidents and sharing of new threats and risks that are associated with cyber-risks
- Area 3 (Cybersecurity controls)
  - Encryption of the mobile platforms if there are confidential data (laptop, mobile devices etc.)
  - Periodical review of access controls on systems and applications (also firewall rules)
  - Secure Coding industry practices for programmers that need to be followed in development phase
  - Special systems for monitoring of ANOMALIES and unusual behavior of the clients and employees (fraud management system)
  - Special group under Banking Agency is established for sharing the security incidents and sharing of new threats and risks that are associated with cyber-risks

Action plans are developed (2)

- Area 4 (External Dependency Management)
  - Data Flow Diagrams to capture the flow of all kind of data to/from the external parties
- Area 5 (Cyber Incident Management and Resilience)
  - Strengthening the current practices of security management (clear responsibilities of the team members, more expertise needed)
  - Different Cyber Related SCENARIOS and reaction PLANS to be analyzed and established in advance in order to strengthen the bank RESILIENCE for this kind of attacks

Closing remarks

- **Our FINANCIAL SYSTEM will have BASIC cybersecurity maturity level by the end of 2017.**

- **Several banks will implement INTERMEDIATE Cybersecurity maturity level by the end of 2019**.

- Banks should be in a position to shift maturity level in certain time period, according to the threat level or recommendation.

- Current action plans are showing that banks will easily fulfill criteria for basic maturity levels, however **biggest challenges are in area 2, 3 and 5.**

- Estimations are for fulfilment of intermediate level banks should invest more then 600K Euro budget.

- Changes in the regulations and current standards in our financial system will be made if it is necessary.

Cyber Resilience Investigation

Goran Jankoski
Department of on-site supervision
IT and Operational risk
Q&A: jankoskig@nbrm.mk

Zoran Georgiev
Payment Systems Department
Oversight Unit
Q&A: georgievz@nbrm.mk