



**THE POLISH  
BANK  
ASSOCIATION**

# **Banking Cybersecurity Center**

**Mieczysław Groszek, Ph.D.  
Executive Vice President  
Polish Bank Association**

Kruczkowskiego Street 8  
00-380 Warsaw  
tel. +48 22 48 68 180  
[www.zbp.pl](http://www.zbp.pl)



## Banking Cybersecurity Center has been created on the initiative of the Polish Bank Association and with participation of the banks

### Main reasons behind creation of Banking Cybersecurity Center

Considerable increase of amount and volume of cyberattacks against banks and its customers

Effective attack against one of the Polish banks

Information about planned cyberattack againsts Polish banking sector and banking sectors of other EU countries planned for October/ November 2015

### Other reasons

- Generation change
- Current formula of interbankk co-operation in the field is no longer sufficient
- The banks are in need of new information sources
- Current forms of customer education are not sufficient
- Expectaions of the Financial Supervision Commission re increased IT security within the banks



THE POLISH  
BANK  
ASSOCIATION



The National Cyber-Forensics & Training Alliance (NCFTA) is a non-profit corporation founded in 2002, focused on identifying, mitigating, and neutralizing cyber crime threats globally. The NCFTA operates by conducting real time information sharing and analysis with Subject Matter Experts (SME) in the public, private, and academic sectors.

### General Principles of NCFTA operation

- Mutual trust
- Solidarity based on mutual co-operation

### Specific principles of NCFTA operation

- All members are equals
- Every member is obliged to co-operate with remaining partners on prevention of cybercrime
- Members' representatives are delegated to work in the NCFTA and are positioned within one localisation.
- Every representative has broad competences allowing him to take immediate action on the part of his institution.
- Members' representatives remain employees of delegating institutions and are paid by them
- The organization's assets come from contributions in kind and financial donations from members.
- The management and maintenance costs are financed by yearly members' contributions.
- To join the organisation at least one recommendation from current member is necessary.

### Public sector members of NCFTA are *inter alia*:

- Australian Federal Police
- Customs & Border Protection
- Homeland Security Investigation
- Federalne Biuro Śledcze
- National Crime Agency
- US Postal Inspection Service
- US Secret Service

### Private sector members of NCFTA are *inter alia*:

- American Express
- Bank of America
- Bank of New York Mellon
- JP Morgan Chase
- PNC Bank
- Synchrony Financial
- USAA



## Recommendation of the Polish Bank Association of 29 September 2015 on Cybersecurity and DDoS attacks prevention

### Steering Committee

Indicates directions of actions and takes strategic decisions regarding banking & customer cybersecurity. Accepts procedures and schemes of action in day-to-day and emergency operations

### Banking Cybersecurity Management Group

Prepares procedures and recommends actions increasing protection in day-to-day operations. In emergency acts in close co-operation with Crisis Center and assures communication between all Groups.

### Operational Group e-Fraud Contact

Consists of persons acting in 24/7 mode who have the authority to execute operations within their institutions on the recommendation of the Crisis Center in areas of procedures and solutions prepared by the Banking Security Management Group.

## Members

### Steering Committee

- Commercial Banks
- Financial Supervision Commission Office
- Police HQ
- National Clearing Chamber S.A.
- Polish Bank Association

### Banking Cybersecurity Management Group

- Commercial Banks
- Financial Supervision Commission Office
- Police HQ
- National Clearing Chamber S.A.
- Polish Bank Association

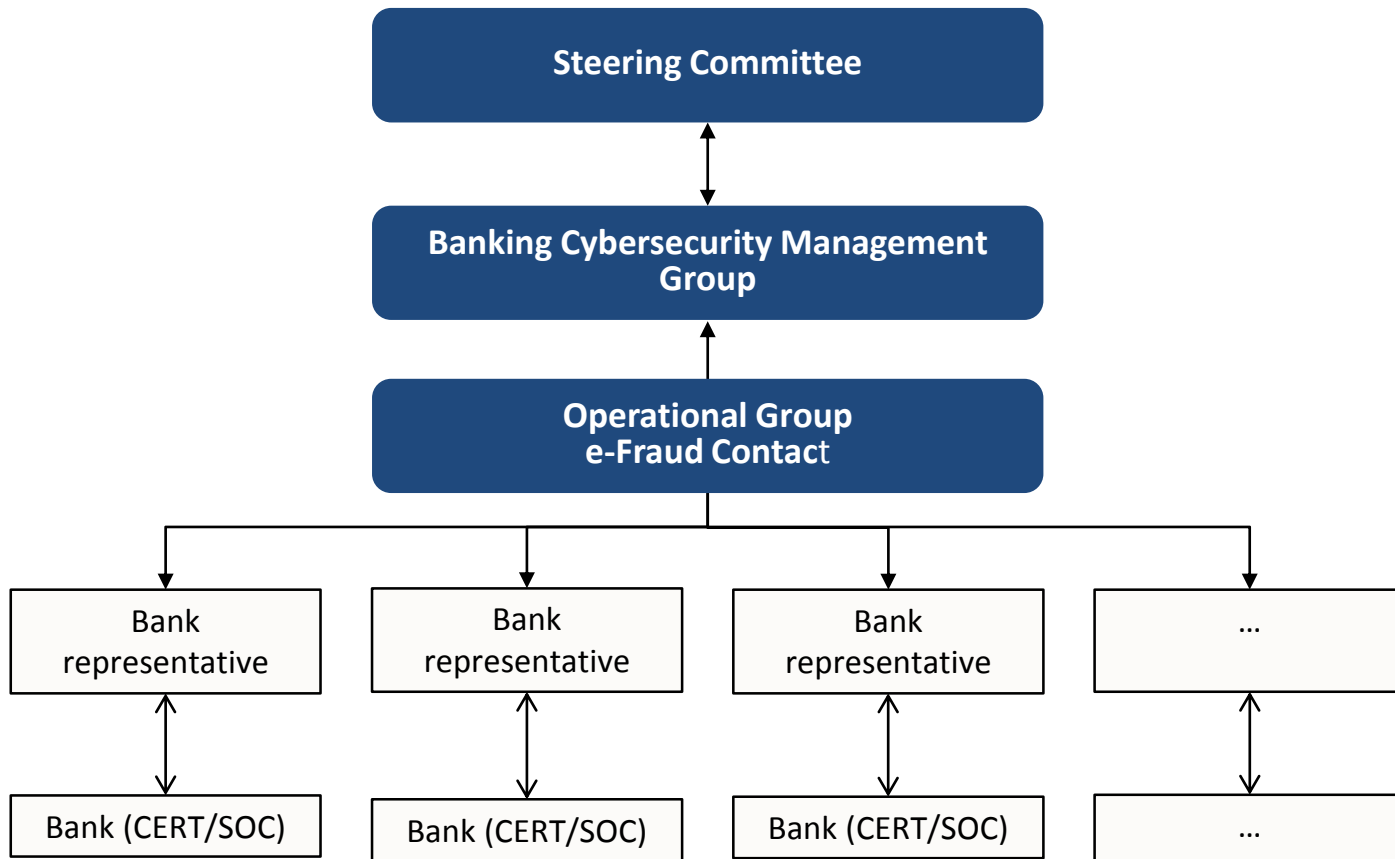
### Operational Group e-Fraud Contact

- Commercial Banks
- Co-operative banks
- Police HQ
- National Clearing Chamber S.A.
- Polish Bank Association



## Structure of the Banking Cybersecurity Center– target model

THE POLISH  
BANK  
ASSOCIATION





## Banking Cybersecurity Center-areas of operation

### Internal actions, within the banking community,

Collegial bodies with the PBA

- Electronic Transaction Security Forum
- Card Frauds Prevention Forum

Tools – the PBA IT systems: Threat Early Warning System, Banking Register of IT Security incidents, Restricted Documents, Access to Public databases – Wanted Notices, PESEL Registry oraz ID Card Registry

### External actions-cooperation with external institutions

International co-operation-exchange of data: Police->Europol, EBF, FBI, NCFTA ...

Co-operation with Ministries: Digitalization, Internal Affairs, Development, Prosecutor Office, FIU, Police - legislation: Blocking of Servers, eID, Account Registry, information exchange, good practices, training conferences

Co-operation with Polish Chamber of IT & Communications, Union of Polish Leasing, e-commerce, advisory companies, NASK...

### Education and Information

Customers' education (retail: children up to 13 y.o., teenagers, students, young professionals up to 30 y.o., customer aged 30 – 55, customers 55+ and corporates: users of web-services or accounting systems)

Informations about cyber attacks - *post factum*

Correct information channel for all target groups: schools, dedicated YouTube channel , dedicated information services www incl. [www.zbp.pl](http://www.zbp.pl), co-operation with www information portals , graphics to be used in kwejk.pl and demotywatory.pl portals, trainings, educational films, comics, subplots in TV series



## Co-operation of the Banking Sector with the Police

### Legal Framework

1994 – signing of agreement on crime prevention

### Co-operation in the field of cybersecurity and cyberfraud prevention

Permanent participation of the Police representatives in:

- Electronic Transaction Security Forum
- Card Frauds Prevention Forum
- Banking Cybersecurity Center (Steering Committee, Management Group, Operational Group)

Police has access to ZBP IT systems

- Restricted documents
- Amron”

The Police shares information on :

- „Wanted” notices,
- Bank account used for fraudulent transactions

Assistance in obtaining information on bank account of persons who are under investigation

Education

- Confernces in Szczytno Police School (banking crime prevention, Technical aspects of IT & Communication)
- Workshops on electronic crime prevention for judges, prosecutors, FIU and Police
- Szklarska Poręba Workshops
- Preparation of Good Practices for bankers and policemen



**THE POLISH  
BANK  
ASSOCIATION**

**The Banking Center of  
Cybersecurity**

**The National Center of  
Cybersecurity**

**Integration of national  
cybersecurity centers**





**THE POLISH  
BANK  
ASSOCIATION**

**Thank you for your attention**

