Cyber security within EBA CLEARING

Regional Seminar on Cyber Preparedness

Vienna, 18th May 2015

Andre Vink, CRO
The changing landscape of cyber threats: *Deal with “Financial Crime 2.0”*

The funding, organization and capability of “criminals” carrying out cyber attacks is increasing at an astonishing speed. Attacks are more sophisticated than ever, and it’s not “just go and get the money” anymore — today we need to deal with a new generation of Financial Crime threat, covering the full spectrum of business operations (from IT to payments to market manipulation to data).
Overview

Introducing the EBA group

Outsourced service EURO1/STEP2

EBA CLEARING Company operations
Operator of EURO1/STEP1 and STEP2
- Operates the pan-European payment systems EURO1, STEP1 and STEP2
- Founded in 1998
- 62 Shareholders
- Around 200 direct participants

The pan-European payment network
- Discussion forum for payment practitioners
- Developer of European payment initiatives
- Founded in 1985
- Over 200 members

E-authorisation solution
- Offers real-time access to accounts all over Europe
- Based on a four-corner model
- Services cover: SCT, SDD and E-identity
- Owned by Preta S.A.S, a wholly owned subsidiary of EBA CLEARING
1997-98: Development of the EURO1 large-value payment system (technical operator: SWIFT)

1998: Creation of EBA CLEARING Company in 1998 by 52 major banks to act as business administrator of the EURO1 system

2001: Launch of the STEP1 Service providing access to the EURO1 platform to the broader community of medium-sized and smaller banks

2003: Launch of the STEP2 Pan-European ACH platform (technical operator: SIA)

2008: Start of SEPA Credit Transfer processing

2009: Start of SEPA Direct Debit processing

2013: Launch of MyBank

2014: SEPA Migration End-Date

2015: Launch of SEPA Card Clearing Service
An automated integrated payment platform for:

Introducing EBA CLEARING Services

Settlement:
- direct TGT2
- indirect
- direct TGT2

Processing:
- single payments, same-day, STP & non-STP, credit & debit
- Payment files, full STP: SCT, SDD Core & B2B
Absolute volume peak day: 1st July 2014 with 125 m
Overview

Introducing the EBA Group

Outsourced services EURO1/STEP2

EBA CLEARING Company operations
Services outsourced

• EBA Clearing operates two SIPS services under ECB oversight,
• EBA Clearing is not an IT Company.

Traditionally, critical services are outsourced to external providers:

• **SWIFT**: EURO1, STEP1, MNM, SWIFTNet
• **SIA**: STEP2, SIANet
• **BBP**: Service bureau’s for SWIFTNet connectivity

Settlement services:
• **ECB**: TARGET2

(Settlement services are backed-up by manual procedures and tested regularly)

Oversight questionnaires:
• 2014: CPSS WG on Cyber Security
• 2015: ECB FMI Cyber Resilience
As a double SIPS operator, EBA CLEARING fully is aware that its payment infrastructure services are critical to a large number of banks in Europe and as a consequence to their capability to provide effective payment services to their customers.

This criticality commands that EBA CLEARING devotes the highest level of attention towards ensuring the robustness and reliability of its services, including an adequate protection of the system platforms that are used to deliver its services including cyber security risks.

EBA CLEARING has outsourced its main services to strategic providers (mainly SIA and SWIFT), that have a strong and long standing reputation in managing mission critical infrastructures.

These ‘Critical Service Providers’ (CSP’s) to FMI’s fall under local Central Bank oversight.
2013 Enterprise Risk Management Framework

Risk Identification

Risk Assessment

Risk Tolerance

Risk Treatment Plan

Red Flags

- Risk Mitigating
- Risk Avoidance
- Risk Transfer
- Risk Acceptance

• ERMF includes cyber security.
Risk Tolerance Methodology

- **Averse:** Avoidance of risk and uncertainty is a key organizational objective;

- **Minimalist:** Preference for ultra-safe business delivery options that have a low degree of inherent risk;

- **Cautious:** Preference for safe delivery options that have a low degree of residual risk;

- **Open:** Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of exposure to risk.
Critical Service Providers (CSP’s)
A resilient and experienced operator

(Among others, SIA provides card processing services in 11 countries, runs the Norwegian and Swedish RTGS platforms and is the preferred provider of the London Stock Exchange Group for fixed income trading and post trading)

- **ISO 9001**
  - Certified Quality Management System

- **ISO / IEC 27001**
  - Certified Information Security Mgt System

- **BS25999**
  - Certified Business Continuity Mgt System

- **Payment Card Industry**
  - Fulfils Data Security Standard re. card processing
Introducing the EBA Group

Outsourced services EURO1/STEP2

EBA CLEARING Company operations
EBA Clearing Business Administrator of EURO1 and STEP2:

- Spider in the web,
- 1st Line support to participants,
- OPC’s front offices,
- 3 geographical locations,
- Completely isolated from the Internet.

EBA CLEARING’s has established operational centres (OPC’s) front office environments which are isolated from any public network.

The strict segregation between the front- and back office operational network environments provides EBA CLEARING with a robust ‘defence in depth’ control on its mission critical applications in a highly secure manner.
EBA CLEARING adopted the ISO 27001 ISMS standard in 2011

- Formally certified since 2012;
- Continuous ‘Plan-Do-Check-Act’ circles;
- Continuously seeking alignment with industry best practices;
- Maintain pro-activeness e.g. internal and external Attack & Penetration Testing;
- Mandatory Information Security awareness sessions;
- Information Security Officers in each unit;

- So much more than ‘a certificate’ on the wall!
Cyber Security – sample of best practices

- 10 essential best practices:

Security Program Lifecycle

1. Build a risk aware culture and management system
2. Manage security incidents with greater intelligence
3. Defend the mobile and social workplace
4. Security-rich services, by design
5. Automate security “hygiene”
6. Control network access and assure resilience
7. Address new complexities of cloud and virtualization
8. Manage third-party security compliance
9. Secure data and protect privacy
10. Manage the identity lifecycle

Conclusion: There is no single ‘silver bullet’.
Regarding detection and monitoring, CSP’s have implemented state-of-the-art infrastructures and matured a long experience on this matter;

Monitoring capability is focused on technical security events and threats on internet network, and on threats at business and application layer;

Detection and monitoring at business layer require significant activities by EBA CL, CSP’s and the participants.
Cyber scenario’s: Internal next steps

- EBA CLEARING is considering the introduction of a separate ‘cyber-resilience framework’, which would enable us to create a specific cyber threat model, assess the current level of cyber resilience of all relevant stakeholders –including CSP’s- and report on the outcomes in a standardized visual manner.

- At current, its appropriateness to the organization is being investigated and outcomes are expected by July 2015…

![Figure 1: Framework Core Structure](image)
Cyber scenario’s: External next steps

Cyber incident response is more than a technical problem with a technical solution

Significant cyber events will require an entire cyber crisis management solution across the cyber incident response lifecycle, from react, to response, to resolve

1. React
   - Identify the issue
   - Perform triage to determine severity

2. Respond
   - Contain the problem to minimize the impact
   - Perform forensic analysis to understand the full impact of the incident
   - Engage third-party support (if needed)
   - Notify third-parties (if needed)

3. Resolve
   - Determine and repair control deficiencies
   - Return to normal business operations
   - Conduct lessons learned

EBA CLEARING is in the process of establishing specific points of contact (Focal Points) that will play a key role in the coordination between EBA CL and its CSP’s in case of cyber event, as follows:

- Contacts and escalation list
- Roles and Responsibilities
- Participants involvement (depending on the event)

So that all relevant parties are made aware of the problem and can activate the technical and organizational procedures, previously defined, to manage the predicted events.