RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CXO-F02

How to Steer Cyber Security with Only One KPI: The Cyber Risk Resilience

Jan Nys
Nys@Jankbc777

#RSAC

I Did Not Find It Either…

KBC at a Glance

- Geographical spread
  - Belgium, Czech Republic , Hungary, Slovakia, Bulgaria, Ireland, …
- Different business areas
  - Retail banks, Insurance, Lease, Securities, Asset Managers, …
  - Local accountability
- IT systems interconnected

~1,600 bank branches worldwide

~36,000 FTEs worldwide, 45% in Belgium, and 51% in Central and Eastern Europe

KBC

Challenge: How to Take Control Over This Risk Area

Back in time:

- **Attacks to KBC companies** were happening all the time
- **A high risk** of financial loss, negative publicity, and unavailability of online banking
- The protective measures were **no longer sufficient**
- We work in a very **diverse** Group geographically, and also in terms of business and available resources
- **KBC PEARL** mission

KBC

Cyber Risk : The Next Gear

Mission of the Program

- Get Cyber defense on acceptable level for all companies of KBC Group
- Report to the KBC GEXCO (*) the status and mitigating activities of Cyber risk for the different Business Entities in the Group
- **Embed business ownership of Information Security in all entities of the Group**

*GEXCO: Group Executive Committee

KBC

Group-wide Strategic Objectives

- Strengthen Cyber defense in KBC Group while respecting and stimulating the ***Pearl spirit***
- Implement ***proactive threat-based*** Cyber Risk Management
- Create an ***information highway*** to be able to respond appropriately to trends and incidents at all levels of the organization
- ***Check and track maturity*** on Cyber Risk Management: compare to internal peers per business unit and to external peers for KBC Group
- ***Enable*** to ***prevent*** and ***detect*** Cyber-attacks in KBC Group companies
- Prepare for ***response*** on Cyber-attacks and for crisis management
- ***Manage*** priorities in mitigation actions and guard balance between ***cost*** & ***risk appetite***
- Prepare for ***reporting*** on Cyber Risk

KBC

Search for Support

- Get heavyweight sponsorship within the company
  - Chief Risk Officer for IT+ IS (Information Security)
  - Chief Risk Officer for Group
- Get support from top managers
  - Country Teams (Belgium, Czech Republic, Slovakia, Ireland, Bulgaria)
  - Management Teams (Asset Management, Securities, …)
- Start a program under the auspice of top management
  - Group Executive Committee

Poll 1

How many levels exist between your CISO and your GEXCO/Board?

- 1 Level
- 2 Level
- More than 2 Levels

Model = Information Security Wheel

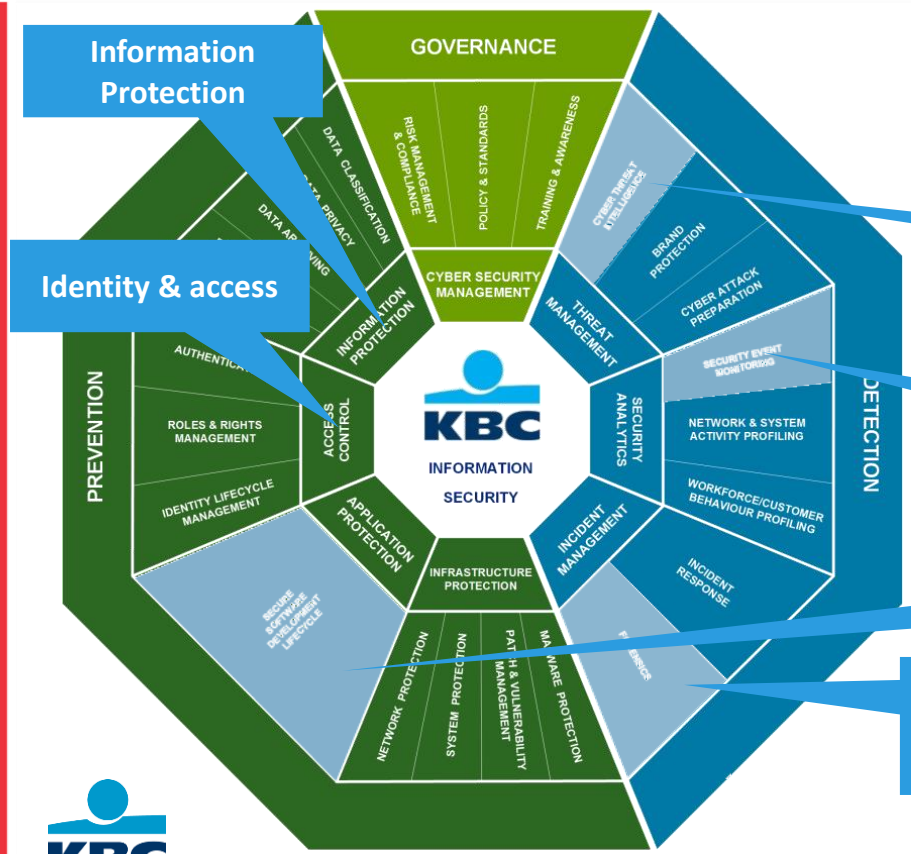


Chart all capabilities that have an influence on this risk

Some examples :

Cyber Threat Intelligence
Analysis of threats, incidents and trends

Security Event Monitoring
Correlation between events

Secure Software Development Life Cycle
Making software safe,
“from cradle to grave”

Forensic research
How did the attack happen? What’s the damage? Build a remediation plan.

KBC

The Concept of Maturity

Level 1
Initial

Ad hoc, Undocumented, uncontrolled

Level 2
Repeatable

Documented but discipline is unlikely to be rigorous

Level 3
Defined

Standards are established

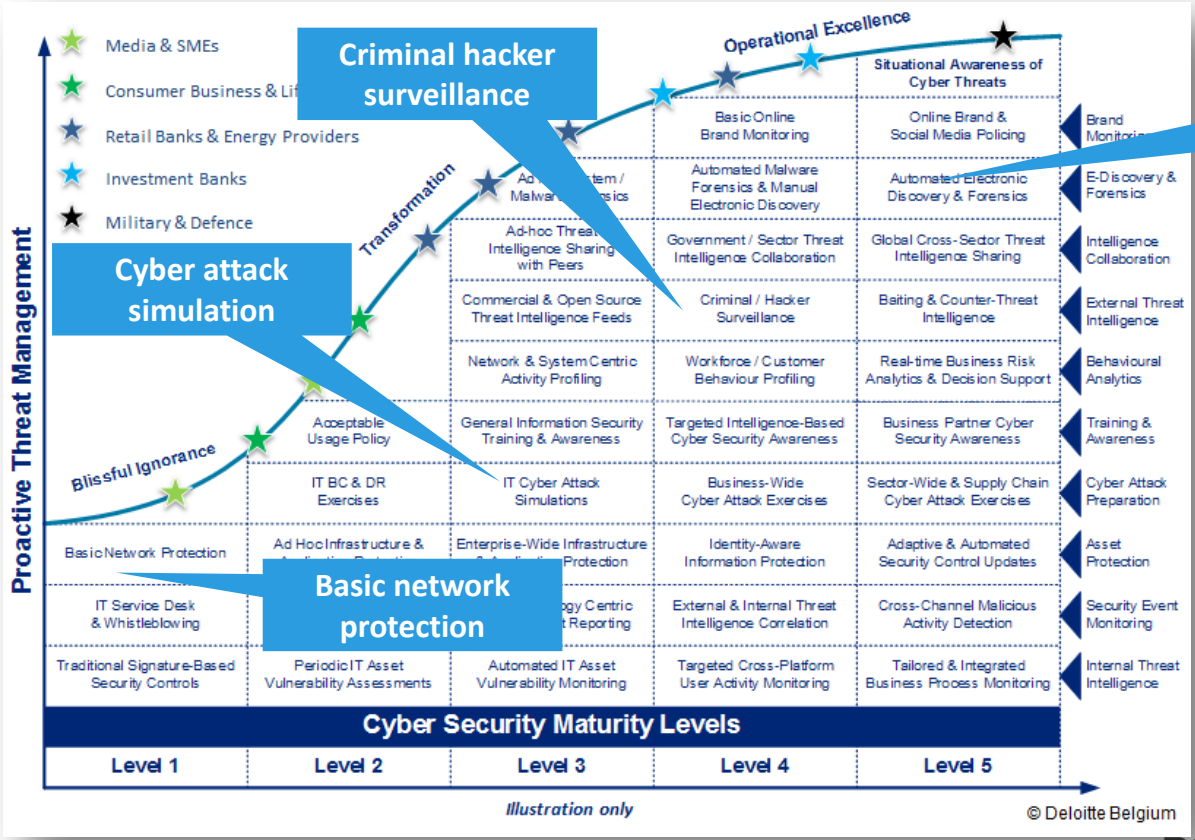
Level 4
Managed

Using process metrics, management can effectively steer & control

Level 5
Optimizing

Continuous improvement

The Concept of Required Maturity



Cyber Threat Assessment

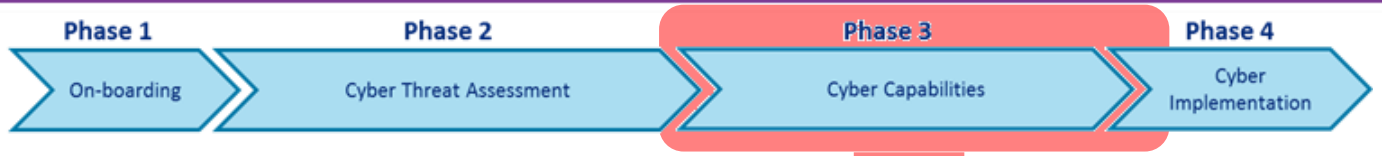
Define Business Services

Define Interfaces for each Business Service

Define Characteristics of Business Services and Interfaces

Define Vulnerability of each Interface per Threat

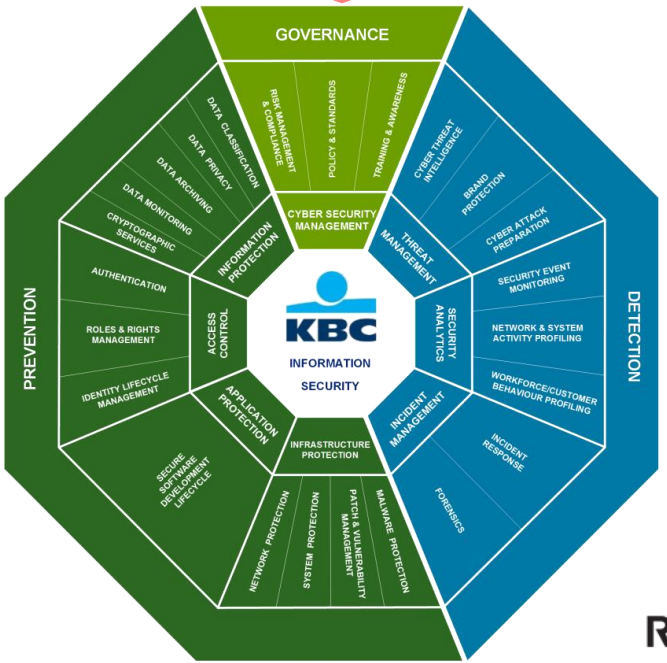
Capability Assessment



Required and current maturity level is defined for each of the 8 capabilities and 24 sub-capabilities

Required maturity
based on business services, interfaces and threat landscape

Current maturity
based on questionnaires & evidence
and Challenged



KBC

Methodology

Final result is a multi-year **roadmap** that will close the gap between Current and Required Maturity.

The yearly **security action plan** is the part of the roadmap that will be implemented within the next year.

Making the Risk Visible: How to Steer with One KPI – Cyber Resilience


“ WHAT GETS MEASURED, GETS MANAGED.”
PETER DRUCKER

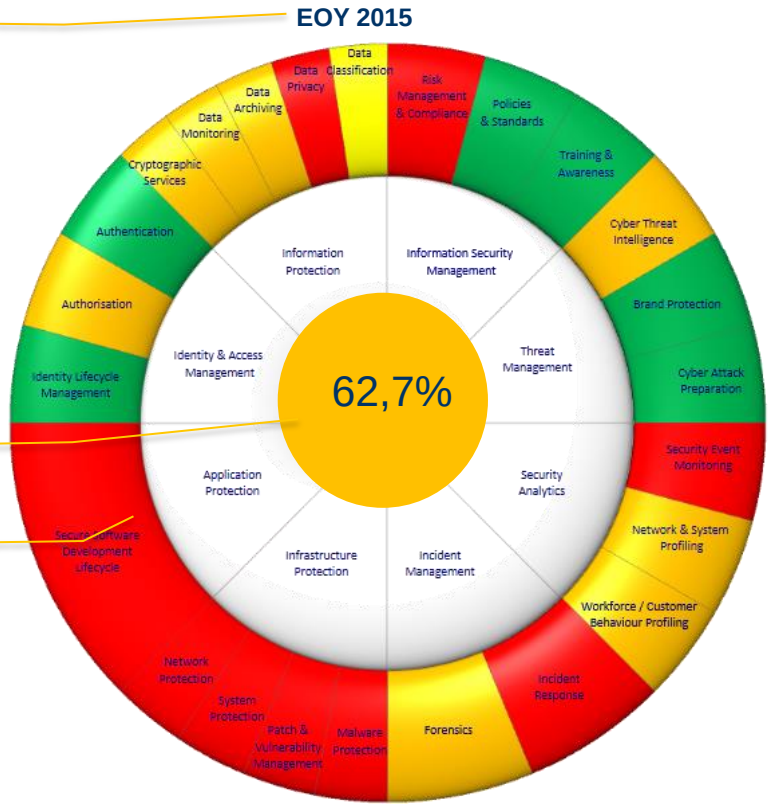
Cyber Resilience: Legend for Next Slides

This shows the moment in time for the presented values
… assuming technology doesn't change
… assuming the threat landscape doesn't shift
… assuming all planned projects can/will be implemented

The Cyber Resilience shows how close this organization is compared to the maturity that is required for its specific threat landscape

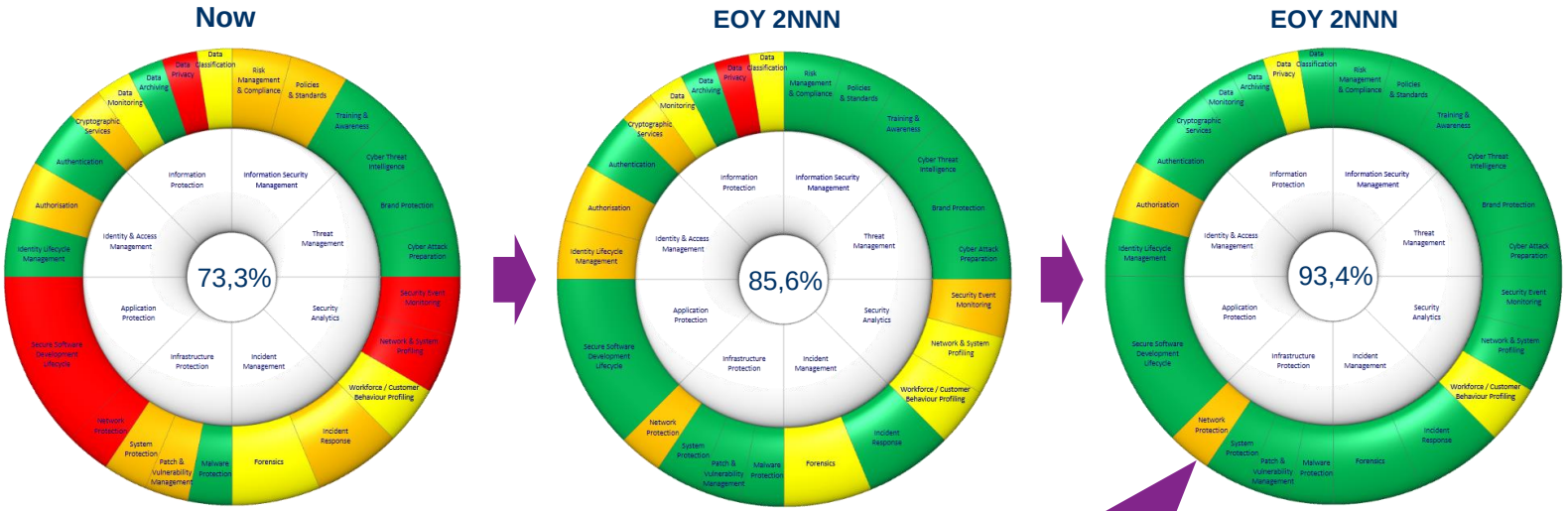
Color coding

Actions yet to be taken
Up to 10% remaining
11% to 25% remaining
26% to 40% remaining
More than 40% remaining



Roadmap Evolution & Simulations: Example

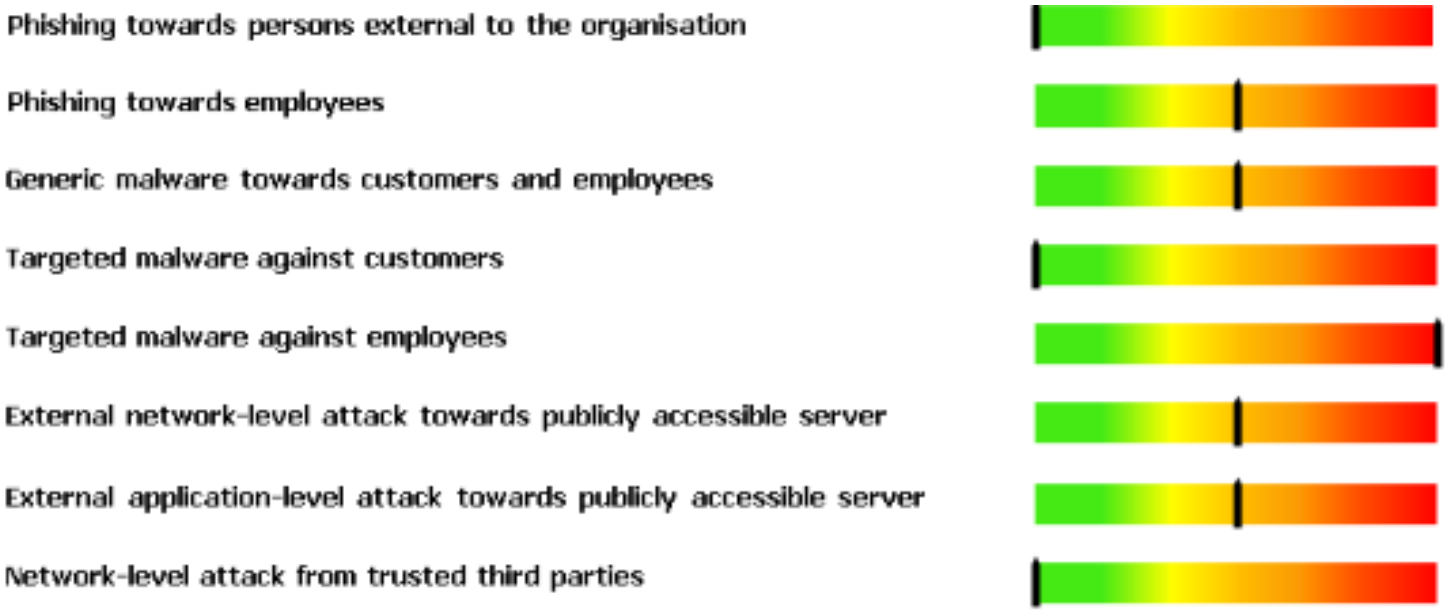
Business Unit – Entity x



Green is not necessarily equal to 100% OK

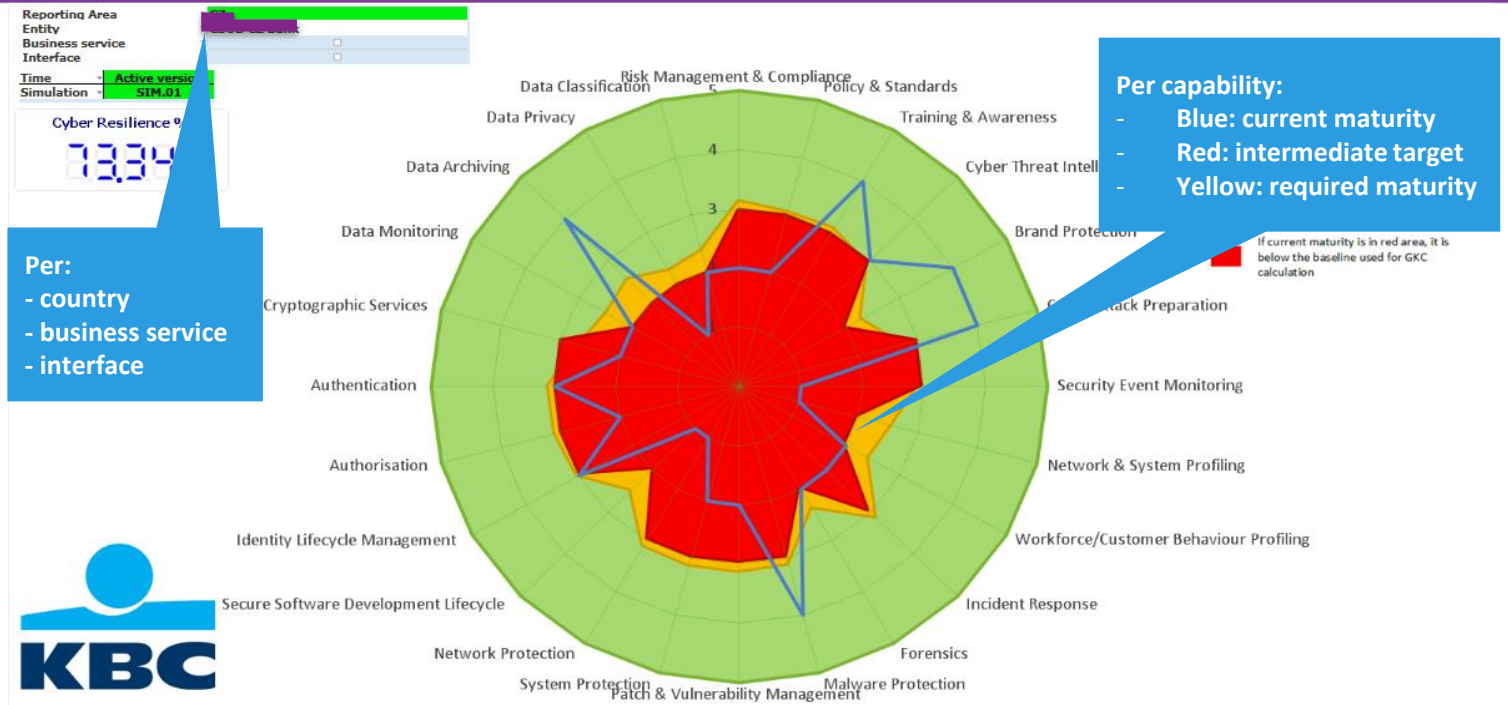
Actions yet to be taken
Up to 10% remaining
11% to 25% remaining
26% to 40% remaining
More than 40% remaining

Threat Landscape : Vulnerability Levels



KBC

Spider Diagram: Example



Group-wide Strategic Objectives

- Strengthen Cyber defense in KBC Group while respecting and stimulating the ***Pearl spirit***
- Implement ***proactive threat-based*** Cyber Risk Management
- Create an ***information highway*** to be able to respond appropriately to trends and incidents at all levels of the organization
- ***Check and track maturity*** on Cyber Risk Management: compare to internal peers per business unit and to external peers for KBC Group
- ***Enable*** to ***prevent*** and ***detect*** Cyber-attacks in KBC Group companies
- Prepare for ***response*** on Cyber-attacks and for crisis management
- ***Manage*** priorities in mitigation actions and guard balance between ***cost*** & ***risk appetite***
- Prepare for ***reporting*** on Cyber Risk

KBC

Cyber Risk Management on Group Level Services

Provide Supporting Services to Group Members

Cyber Intelligence

Cyber Surveillance

Breach Investigation

Crisis Management

Training & Awareness

Resilience & Readiness testing

KBC

Cyber Intelligence - Sharing

Publications

Cyber Threat Barometer

Newsbites

Notifications

Cyber Risk Early Warning

Cyber Alert

Cyber Threat Information

Sharing

Cyber Analyst call

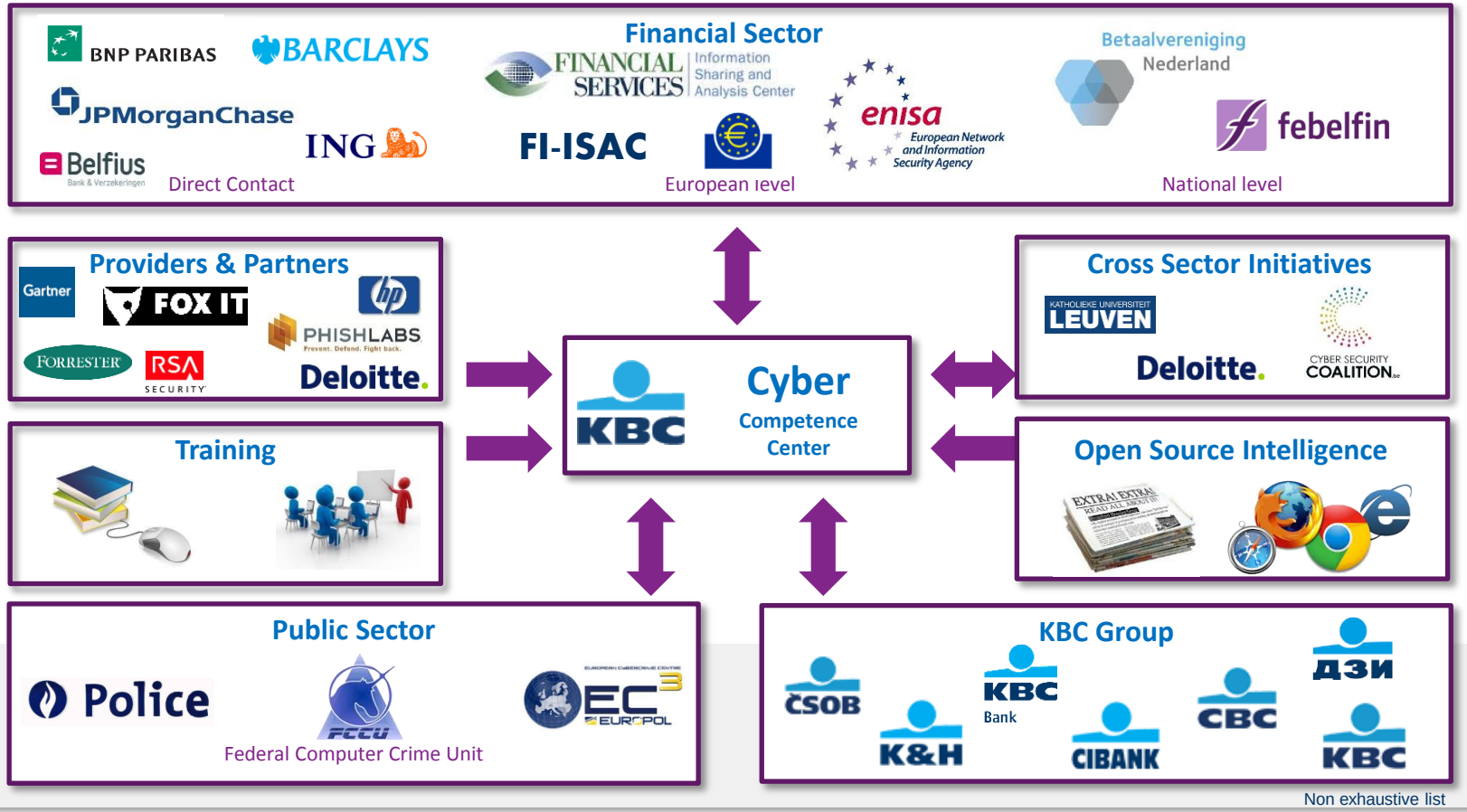
Round Table Meetings

Webcast

Management Reports

Weekly Incident Summary

Intelligence - Sources



Non exhaustive list

Provide Supporting Services to Group Members

Cyber Intelligence

Cyber Surveillance

Breach Investigation

Crisis Management

Training & Awareness

Resilience & Readiness testing

Cyber Surveillance

- Detection of **malware** targeting KBC companies and shutting down malicious servers (command & control servers)
- Detection of **phishing** activities and shutting down malicious websites
- Monitoring of mobile app stores for fake **mobile apps** of KBC Group companies
- Detection of customer/employee **credentials** on drop zones

Provide Supporting Services to Group Members

Cyber Intelligence

Cyber Surveillance

Breach Investigation

Crisis Management

Training & Awareness

Resilience & Readiness testing

Breach Investigation

- Forensic Investigation
- Malware Analysis

Provide Supporting Services to Group Members

Cyber Intelligence

Cyber Surveillance

Breach Investigation

Crisis Management

Training & Awareness

Resilience & Readiness testing

Crisis Management

Central team steps in when:

- Right profiles unavailable
- Too many incidents/crises at the same time
- Crisis gets out of control
- Global Cyber crisis

In 2016

KBC

Provide Supporting Services to Group Members

Cyber Intelligence

Cyber Surveillance

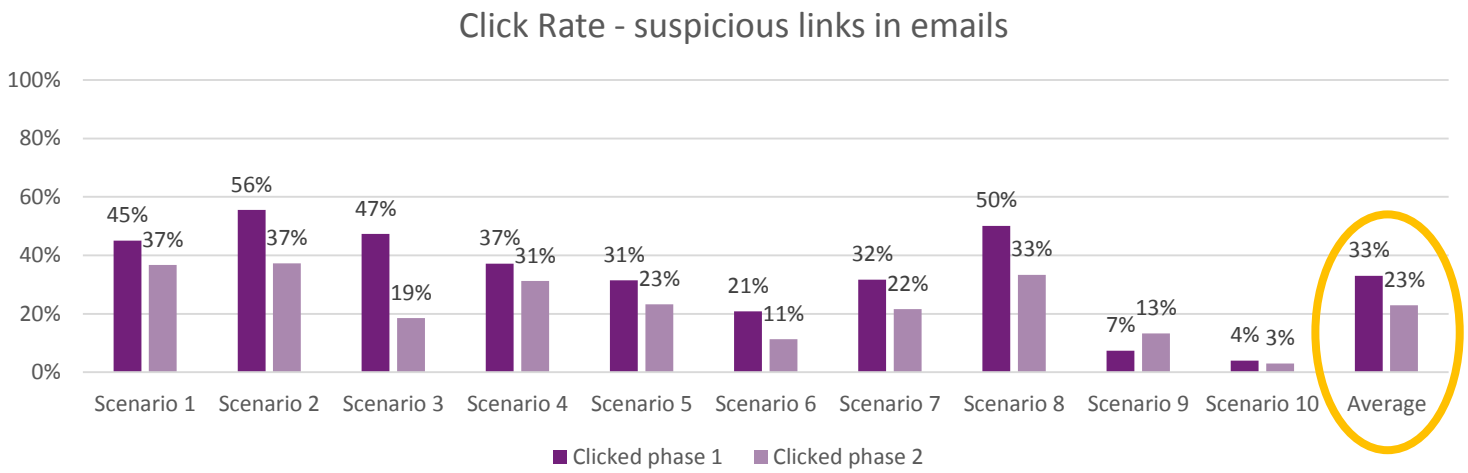
Breach Investigation

Crisis Management

Training & Awareness

Resilience & Readiness testing

Large Scale Phishing Campaign



Number of “clickers” dropped to 23% ➔ **Continue the efforts this year**

Provide Supporting Services to Group Members

Cyber Intelligence

Cyber Surveillance

Breach Investigation

Crisis Management

Training & Awareness

Resilience & Readiness testing

Cyber Resilience & Readiness Testing

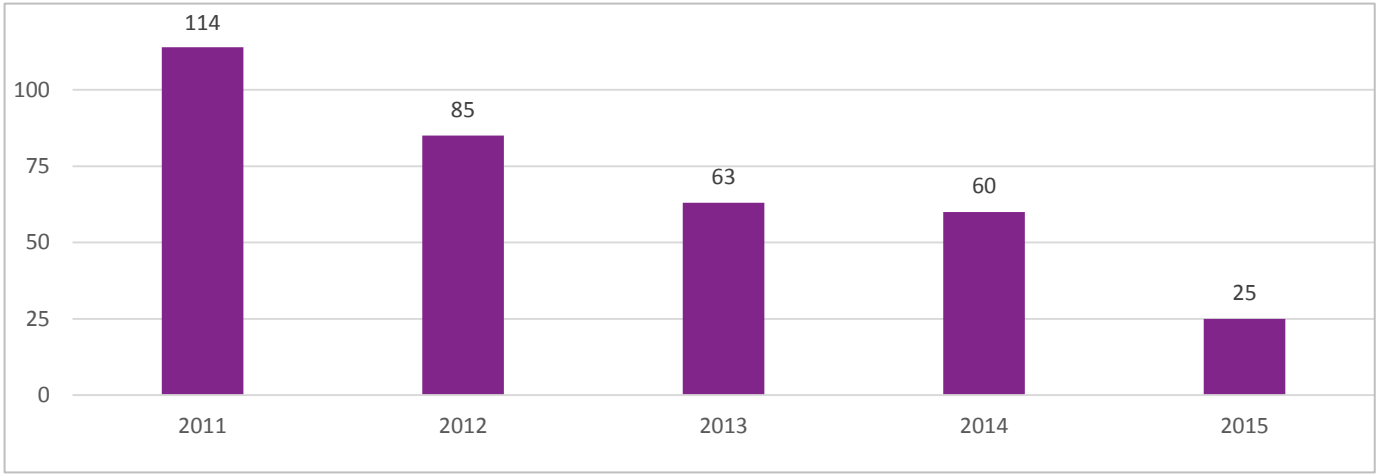
- Vulnerability scanning of all **websites** in KBC Group
- Vulnerability scanning of all **mobile apps** in KBC Group
- **Ethical Hacking** of our companies
- Vulnerability scanning on our **internal network**

Cyber Resilience & Readiness Testing

If you didn't start to scan your websites for vulnerabilities yet, **do it now** !

Positive impact of vulnerability scan

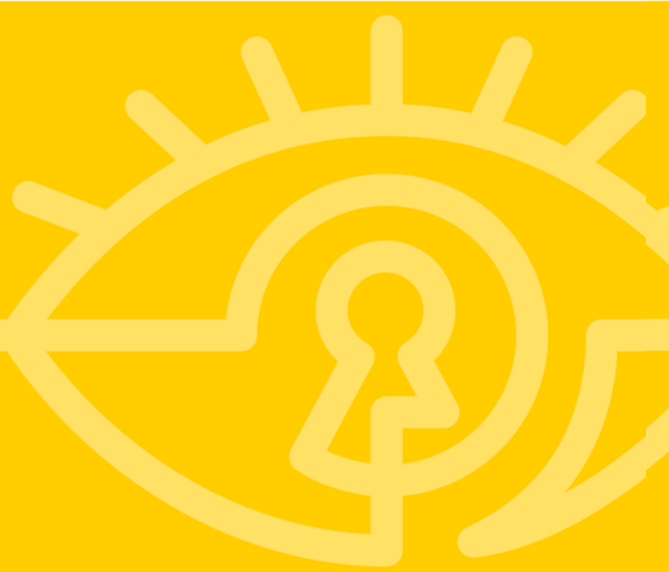
Number of severe Vulnerabilities (all websites)



Poll 2

Who has done an Ethical Hacking exercise?

- Never
- Yes
- I do not know what Ethical Hacking means



Reporting to Top Level: Dashboard


CONFIDENTIAL
KBC Group Dashboard
Information Security
Reporting period Q2 2015
IRM
We enable you to be safe
KBC
Pearl
Go! Take control
Note: Resilience results are based on
the Cyber TNG maturity assessment dd. 15/07/2015

Group-wide Strategic Objectives

- Strengthen Cyber defense in KBC Group while respecting and stimulating the ***Pearl spirit***
- Implement ***proactive threat-based*** Cyber Risk Management
- Create an ***information highway*** to be able to respond appropriately to trends and incidents at all levels of the organization
- ***Check and track maturity*** on Cyber Risk Management: compare to internal peers per business unit and to external peers for KBC Group
- ***Enable*** to ***prevent*** and ***detect*** Cyber-attacks in KBC Group companies
- Prepare for ***response*** on Cyber-attacks and for crisis management
- ***Manage*** priorities in mitigation actions and guard balance between ***cost*** & ***risk appetite***
- Prepare for ***reporting*** on Cyber Risk

KBC

Apply What You Have Learned Today

- Next week you should:
  - Not lose time in discussions about ‘the best’ Information Security Framework. Choose one!
  - Start getting your Top Level Buy-in
- In the first three months following this presentation you should:
  - Involve your Information Security Officers, get them to speak the same language based on your Framework
  - Define measurable target(s) for your risk appetite and approve them at the Board Level
- Within six months you should:
  - Define your program charter, get it decided at the Board Level and **go for it** !