Reporting On Cyber Risk Resilience With One Single Indicator

Jan Nys
GM Cyber Security

Fri. September 9th 2016
2:30PM - 3:00PM
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
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
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
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
Search For Support

• Get heavyweight sponsorship within the company
  – Chief Risk Officer for IT & 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
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.
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

- Basic network protection
- Cyber attack simulation
- Criminal hacker surveillance
- Automated discovery & forensics
Cyber Threat Assessment

Phase 1: On-boarding
- Define Business Services

Phase 2: Cyber Threat Assessment
- Define Interfaces for each Business Service
- Define Characteristics of Business Services and Interfaces

Phase 3: Cyber Capabilities
- Define Vulnerability of each Interface per Threat

Phase 4: Cyber Implementation
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
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 Cyber Resilience with One Indicator

“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

<table>
<thead>
<tr>
<th>Actions yet to be taken</th>
<th>Remaining Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 10% remaining</td>
<td></td>
</tr>
<tr>
<td>11% to 25% remaining</td>
<td></td>
</tr>
<tr>
<td>26% to 40% remaining</td>
<td></td>
</tr>
<tr>
<td>More than 40% remaining</td>
<td></td>
</tr>
</tbody>
</table>
Roadmap Evolution & Simulations: Example

Business Unit – Entity x

Now

EOY 2NNN

EOY 2NNN

Green is not necessarily equal to 100% OK

<table>
<thead>
<tr>
<th>Actions yet to be taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 10% remaining</td>
</tr>
<tr>
<td>11% to 25% remaining</td>
</tr>
<tr>
<td>26% to 40% remaining</td>
</tr>
<tr>
<td>More than 40% remaining</td>
</tr>
</tbody>
</table>

Europe 2016
Threat Landscape: Vulnerability Levels

- Phishing towards persons external to the organisation
- Phishing towards employees
- Generic malware towards customers and employees
- Targeted malware against customers
- Targeted malware against employees
- External network-level attack towards publicly accessible server
- External application-level attack towards publicly accessible server
- Network-level attack from trusted third parties
Spider Diagram: Example

Per capability:
- Blue: current maturity
- Red: intermediate target
- Yellow: required maturity

Per: - country - business service - interface
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
Provide Supporting Services to Group Members

- Cyber Intelligence
- Cyber Surveillance
- Breach Investigation
- Crisis Management
- Training & Awareness
- Resilience & Readiness testing
Cyber Intelligence – Sharing The Information Highway...

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
- Summary
- Weekly Incident Summary
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
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/crisis at the same time
- Crisis gets out of control
- Global Cyber crisis
Provide Supporting Services to Group Members

- Cyber Intelligence
- Cyber Surveillance
- Breach Investigation
- Crisis Management
- Training & Awareness
- Resilience & Readiness testing
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
Reporting To Board level

- Status on Resilience level with only one quantitative indicator
- Quarterly
- Input from ISOs in all entities and the cert.kbc
- Qualitative summary what happens in all entities
- Structure: guided by the wheel
  - Key take away messages
  - Most important incidents in KBC and around us
  - Per capability: Key messages + actions taken
Reporting to Top Level: Dashboard

KBC Group Dashboard
Information Security

Reporting period Q2 2015

Go! Take control

Note: Resilience results are based on the Cyber TNG maturity assessment dd. 15/07/2015

BORDERLESS
CYBER

Europe 2016
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