"Energy & Cyber Security in EU"

Poslanecká sněmovna Parlamentu ČR

Sněmovní 1, Praha 1, Sál 205

6. listopadu 2014

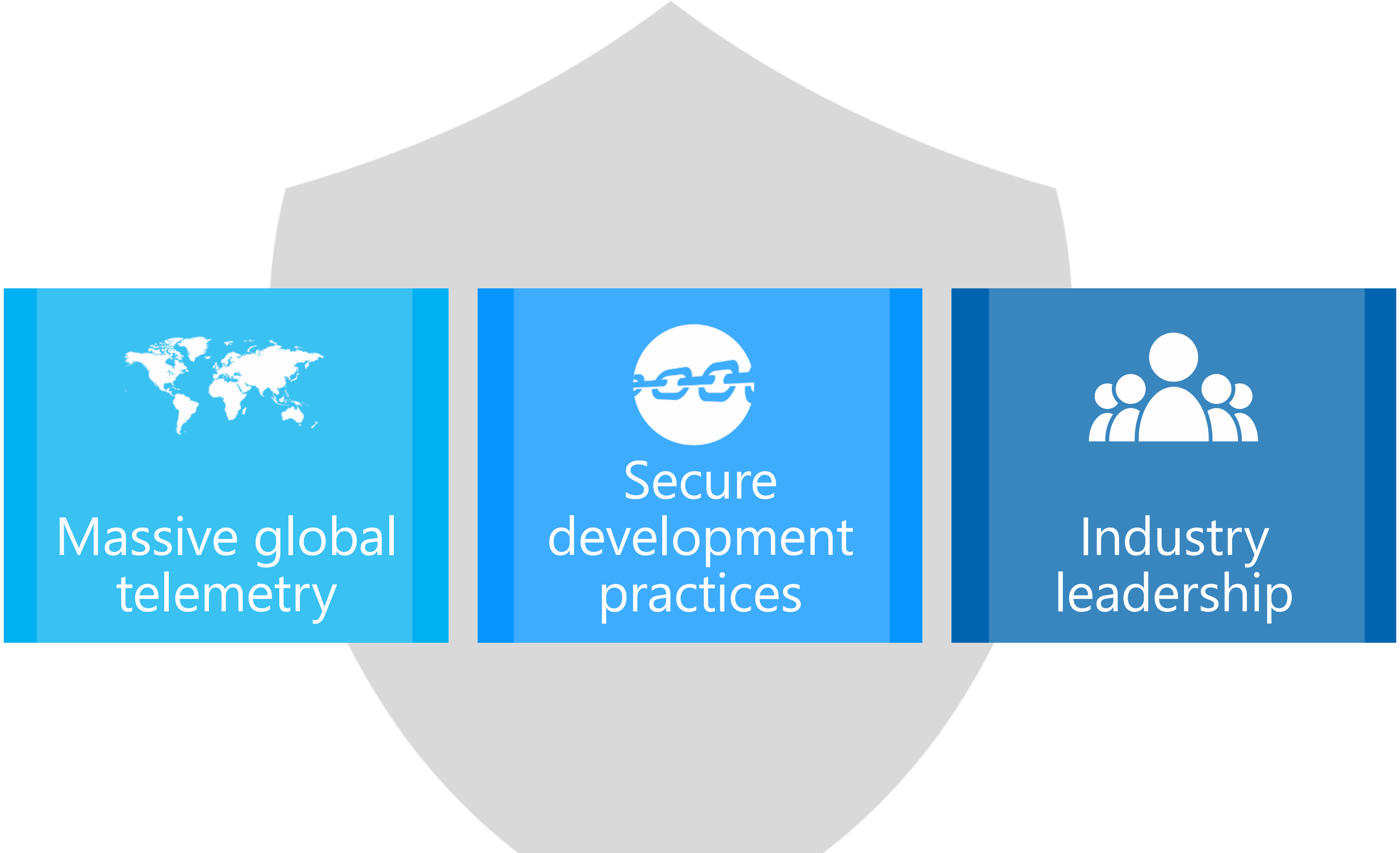
Microsoft

Cybersecurity Policy in the EU: The Network and Information Security Directive -

Security for the data in the cloud

Microsoft Commitment to Cybersecurity

Security at the heart of our products and services



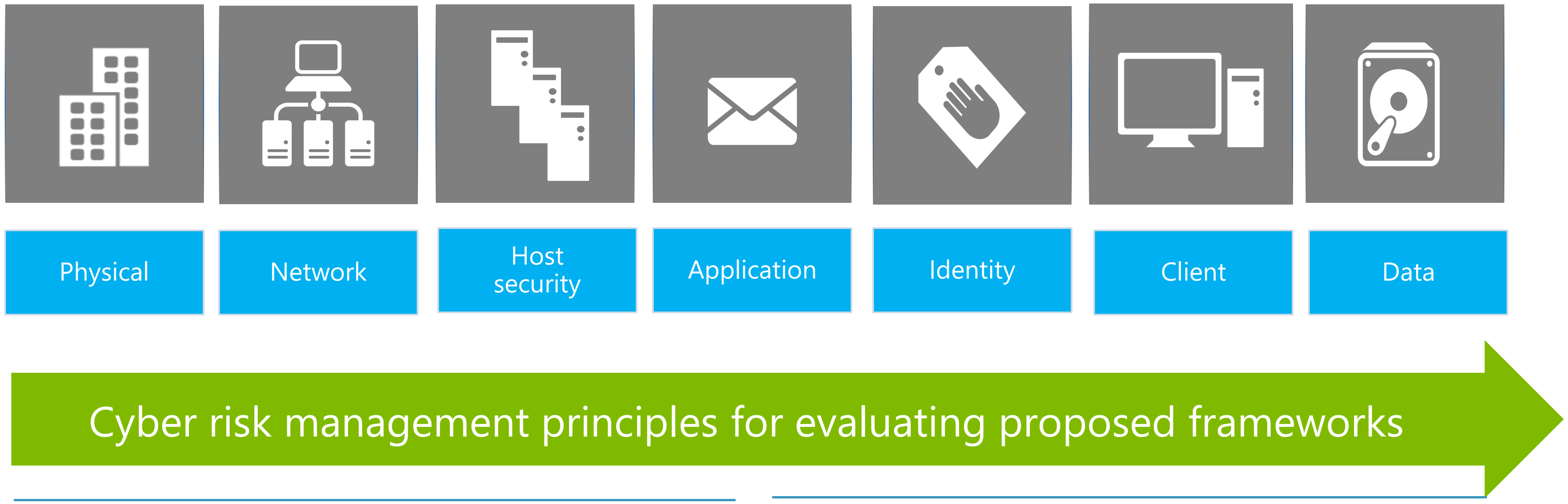
Massive global telemetry

Secure development practices

Industry leadership

Developing Cybersecurity Policy Framework

Core principles driving our approach


Physical
Network
Host security
Application
Identity
Client
Data
Cyber risk management principles for evaluating proposed frameworks

- Risk-based
- Outcome-focused
- Prioritized
- Practicable
- Privacy-respecting
- Globally relevant

Timeline of adoption

Estimated in October 2014

NIS Directive Published

February 2013

Parliament Position Adopted

March 2014

Council Negotiations

30 October 2014

COREPER Mandate

7 November 2014

Second Trialogue

11 November 2014

Telecom Council

27 November 2014

Final Agreement Accepted for Q1 2015

24 Months for Implementation

Member States are at different levels and expected to adopt the Directive at different speeds

Network and Information Security Directive

Significant improvements put forward by the Parliament

Microsoft believes regulation plays a critical role in the realm of cybersecurity & welcomes the Commission initiative.

Open discussion with industry

Focus on risk management

Focus on critical infrastructure (reduction of scope)

Introduction of single point of contact

Removal of Delegated Acts

Focus on risk management & prioritization central to the success of the Directive.

Questions remained:

- Are public administrations included?
- How will Member States cooperate?
- How to preserve voluntary exchange of information?
- How to best make use of international standards?
- How to ensure maximum harmonization across the EU, globally and with other legislative proposals?

Microsoft

Key Issues Still Under Negotiation

Based on our understanding of the Council discussions in October 2014

Operator

- A public or private entity referred to in Annex II, which provides an essential service in the fields of digital Internet infrastructure and service platforms, energy, transport, banking, stock exchanges, health, and water supply.
- Fulfils the criteria of: depends heavily on NIS; an incident to the NIS of the service having serious disruptive effects on the provision of that essential service or on public safety; service platforms shall also fulfil the criterion that a large number of market participants rely on the entity for their trading/ economic activities; each MS shall identify their own.

Incident Reporting

- Member States shall provide for a reporting scheme pursuant to which operators shall notify without undue delay to the competent authority incidents having a significant impact on the continuity of the essential services they provide.
- Focus of the discussion definitions: “significant”, “undue delay, “essential”.

Cooperation

- Split between those wanting stronger operational cooperation and those pushing for informal cooperation (rely on existing CERT-CERT exchanges)

Standardization

- To promote convergent implementation of Article 14(1) and 14(1a) Member States shall, without prejudice to technological neutrality, encourage the use of European or internationally accepted standards and/or specifications relevant to networks and information security.

Core Requirements for Technology Providers

Based on our understanding of the Council discussions in October 2014

Incident Reporting

- Only "*significant*" incidents reportable. Definition includes: number of users affected by the disruption of the essential service; Duration of the incident; geographical spread with regard to the area affected by the incident.

Public Warning

- "After consultation between the competent authority and the operator concerned, the single point of contact *may inform the public, or require the operators to do so, about individual incidents*, where public awareness is necessary to prevent an incident or deal with an ongoing incident".

Security Baseline

- Operator required to take *appropriate and proportionate, sector-specific technical and organisational measures to manage the risks posed to networks and information security of systems* which they control and use in their operations.

Audits

- NCAs have "*necessary means to assess operators' compliance*"
- Operators to "*provide information needed to assess security of their NIS, including security policies*"**;**
- Operators to "*undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.*"

Sanctions

- Member States to determine sanctions that are "*effective, proportionate and dissuasive*"

Potential Challenges with Current Direction

Making the perfect be the enemy of the good

Broad regulatory scope + minimum harmonization = uneven cybersecurity patchwork for Europe

Broad regulatory scope + limited security resources = less security.

Broad regulatory scope + incident reporting = data protection concerns

What does it mean for European cybersecurity

Microsoft

Harmonization will be critical

Opportunity Lost: Lowest Common Denominator

Rising Baselines: stronger risk management, analysis, readiness, response, and cross-border collaboration

Common Operational Understanding: Building on baselines to include sharing of strategic assessments and enhanced public-private cooperation.

Optimum scenario: EU cybersecurity shield

THANK YOU

Severin Loffler
Director Legal & Corporate Affairs
Microsoft Central and Eastern Europe