Cybersecurity: EU's Network and Information Security (NIS) Directive - Consequences and implications for the financial sector

Copenhagen FinTech Week

Presentation June 20th 2018

By: John Michael Foley

Founder and CEO COPITS (advice ands consultations only)

Why is cybersecurity so important?

- Over the past years, digital technologies have become the backbone of our economy and are a critical resource all economic sectors rely on. They now underpin the complex systems which keep our economies running in, for example, finance, health, energy and transport.
- Many business models are built on the uninterrupted availability of the internet and the smooth functioning of information systems Cybersecurity incidents, be they intentional or accidental, could disrupt the supply of essential services we take for granted such as water or electricity. Threats can have different origins - including criminal, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The EU NIS Directive

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

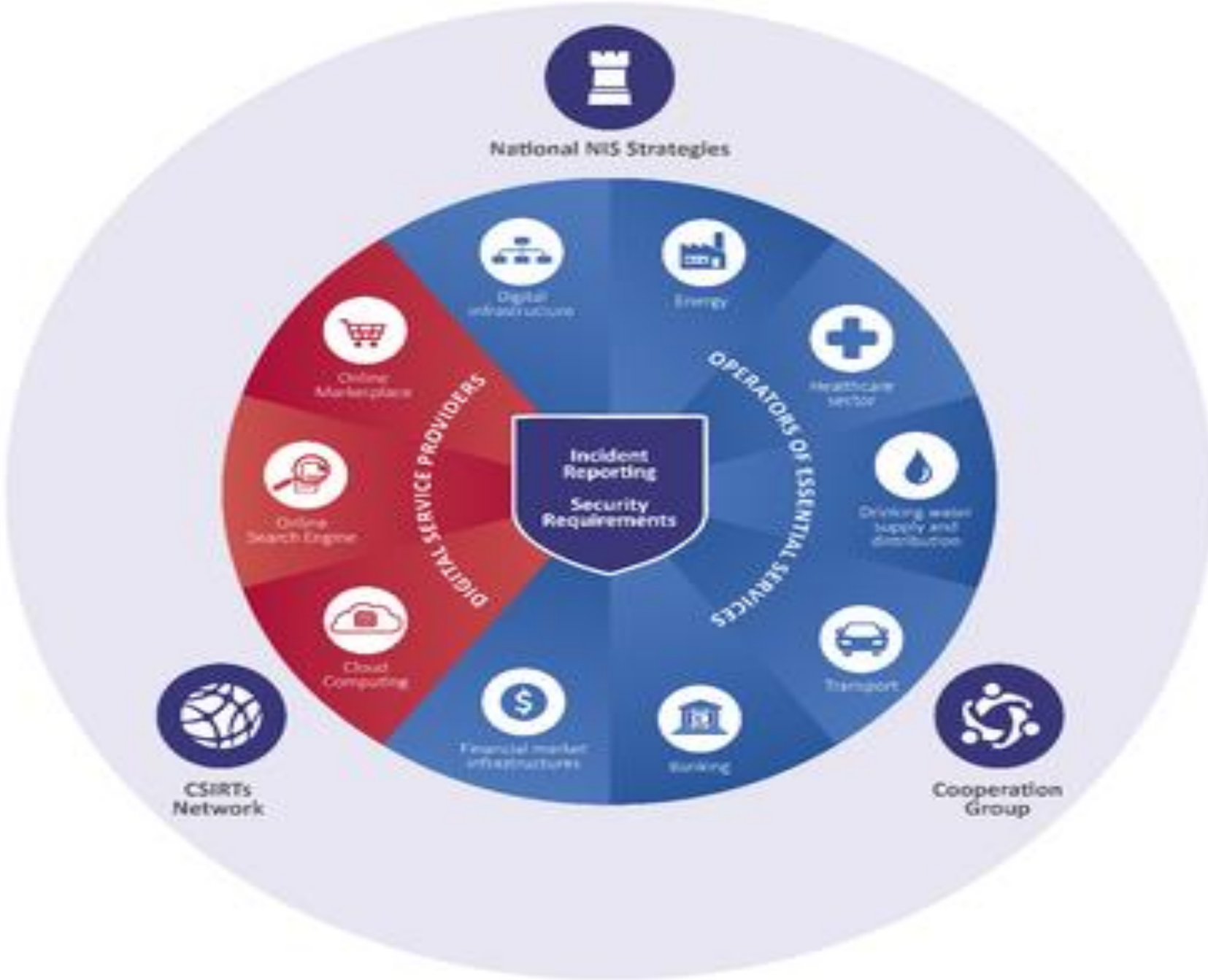
concerning measures for a high common level of security of network and information systems across the Union

The NIS Directive has three parts:

1. National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.

2. Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.

3. National supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: supervision in critical sectors (energy, transport, water, health, and finance sector), supervision for critical digital service providers (internet exchange points, domain name systems, etc).


National NIS Strategies
Digital infrastructure
Energy
Healthcare sector
Drinking water supply and distribution
Transport
Banking
Financial market infrastructures
OPERATORS OF ESSENTIAL SERVICES
DIGITAL SERVICE PROVIDERS
Online Marketplace
Online Search Engine
Cloud Computing
Incident Reporting
Security Requirements
CSIRTs Network
Cooperation Group

Transposition

Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 10 May 2018.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Milestones for each memberstate

- Before May 10 th 2018: Have national strategy for cybersecueity in place
- By November 10th 2018; have sectorspecific strategies in place covering
- By November 10 th 2018: Establish sectorspecific cybersecurity units in each of the identified society vital and critical infrastructures
- By November 10 th 2018: Have identified Operators of Essential Services
- By November 10 th 2018: Have identified Digital Service Providers

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES – Chapter 4, Article 14.

Security requirements and incident notification:

Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

Continued

Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

Continued

Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

Parameters

In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

- the number of users affected by the disruption of the essential service;
- the duration of the incident;
- the geographical spread with regard to the area affected by the incident.

Danish National Law – for the financial sector

- **LOV nr 436 af 08/05/2018 Gældende**
  (NIS-loven)
- Offentliggørelsesdato: 09-05-2018
- Ressortministerium: Erhvervsministeriet: Ministry of Economic and Business Affairs
- Finanstilsynet