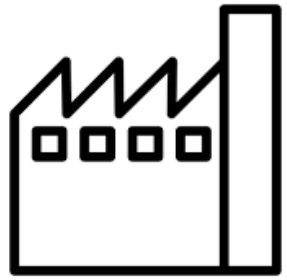
Panel 1: Cybersecurity and Radio Equipment Directive – setting up the scene and future work

Wim De Kesel
Group Vice-President Standardization
Legrand
Convenor of CEN/CLC BTWG10

We all have the same wish

Regional
National
State
Province
County
Township
City

Residential
Tertiary
Hospitality
Industrial



Chemicals
Construction
Electrotechnology
Energy and utilities
Food and agriculture
Healthcare
Machinery
transport

Water
Gas
Electricity
Steam
Hotwater

Security
Entertainment
Repair
Recycle
Design
Communication
Education

Cyberspace needs to be safe

Cyber security risks are not limited to a single application, therefore **a horizontal approach** (applicable to most situations) is essential

Cyber security risks are not stopped by country or continent borders, thus **an international approach** is essential

Stakeholders need sufficient time to introduce changes to their systems and products to ensure compliance – a **compliance deadline** far enough in time is essential

Standards will need to give presumption of conformity to minimize cost for society, **Citation in the OJEU** is essential

Cyber security is an overarching need

Tackling this on a product or application limited basis is not such a good idea in terms of coherence

Not on a regulatory level
And
Not on a standardization level

The point is that the RED is a vertical legislation, a product legislation.

We can do better.

Standardization shall do better.

Horizontal approach

Standardization should work on a **generic standard** to provide presumption of conformity with the cyber requirements of the RED.

The **generic standard** should also provide presumption of conformity with future legislation on cyber security for networkable products.

The verticals (products/applications) should then evaluate the **generic standard**, **based on the specific risks of that vertical,** if there are gaps to be filled.

Gaps should be covered by further improving the **generic standard** so that all verticals take benefit.

Gaps could be covered by product specific standards

Cyber threats do not know borders

Tackling this on a province, national or regional level, is not such a good idea

For standardization, there is an **international** level where all experts from around the world can join.

Generic standards should be established on an **international** level, involving experts from all stakeholders.

International approach

European **generic standards** shall be based on (if not identical to) **international generic standards**.

European standardization organizations need to further finetune the **international generic standards** to ensure compliance with the legal requirements related to the **citation in the OJEU**

Cyber security needs to be easily accessible to all stakeholders

The conformity assessment procedure for the cyber security requirements depends on the usage of **harmonized standards**

If no **harmonized standards** are used (e.g. due to non-availability of these standards), there is the obligation to involve notified bodies

If **harmonized standards** are used, a **manufacturer's declaration** is sufficient

This is a matter of
- Time to market
- Cost for society

Citation in the OJEU

Harmonized standards need to comply with legal requirements:
- Compliance with the standardization request
- Adequate coverage of the essential requirements
- Addition of the necessary annexes.

This calls for
- a standardization request giving sufficient liberty for standardization experts to do the job
- standardization deliverables
  - to cover adequately all requirements of the RED
  - to include the required annexes
- sufficient flexibility while assessing the compliance of the standard with the legal requirements
- timely **citation in the OJEU**

Cyber security needs to be easily accessible to all stakeholders

The conformity assessment procedure for the cyber security requirements depends on the usage of **harmonized standards**

If no **harmonized standards** are used (e.g. due to availability of these standards), there is the obligation to involve notified bodies

If **harmonized standards** are used, a **manufacturer's declaration** is sufficient

This is a matter of
- Time to market
- Cost for society

Compliance deadline

Networkable products in the scope of the RED need to comply with the delegate act at the **compliance deadline**.
Industry needs a reasonable period to ensure this compliance by using cited standards

The **compliance deadline** for the delegated act needs to be set taking into consideration
- the publication of the delegated act
- the **citation** of the standards **in the OJEU**
- time needed by industry to ensure compliance with the **harmonized standards**

Society needs
timely **generic harmonized** standards
identical to **international** standards
to ensure that **cyberspace is safe**

Thank you for your attention