ORGALIME

Position Paper

Brussels, 12 June 2017

Strengthening Trust and Transparency in IoT

Executive Summary:
The European Engineering Industries which Orgalime represents as a whole, attach considerable importance to achieving a secure cyberspace: as an industry, mainly capital goods industry, supplying technology and systems to all other industries and economic sectors. Orgalime's members are more and more called upon to provide solutions incorporating systems and technology increasingly reliant on digital technologies. Given the wide coverage of Orgalime's industry, it is inevitable that a sectoral approach will need to be considered as a one-size-fits-all approach will not be appropriate.

We therefore thank the European Commission for its focus on the issue and wish to provide hereafter our first input. We feel that cybersecurity is a core policy issue, best dealt with through a wide consultation of and open, coordinated conversation with all interested stakeholders.

Cybersecurity is not only a crucial prerequisite for digitisation of industry. It will also be embedded in industrial value chains and business models. Orgalime therefore requests policy makers to take a comprehensive industrial policy view and abstain from hasty regulatory measures. In particular, it is of utmost importance to firstly define the requirements against which any future scheme could be tested before debating different conformity assessment methods. The cart should not be put before the horse.

The industry which Orgalime represents is regulated under the New Legislative Framework (NLF). The NLF defines essential requirements and then leaves it up to companies to carry out the required risk analysis, establish technical files and perform compliance based on manufacturers' declarations (conformity assessment module A of Decision 768/2008/EC).

Internet of Things (IoT) devices and solutions will be used in multiple environments with different security requirements. In addition, cybersecurity is a moving target and any assessment can become obsolete overnight. We therefore find that in this fast-moving and heterogeneous area any rigid approach based on mandatory third party certification or labelling is inappropriate. However, Orgalime recognises the importance of EU wide transparent and comparable security product information for customers and users, especially in B2C markets. In order to increase transparency and trust, we suggest to follow two approaches:

- prioritise the definition of the requirements
- increase transparency of product capabilities

In this context, the use of international standards, such as IEC 62443 for general purposes and ISO/AWI 21434 for road vehicles, is a promising approach to improve cyber security for engineering products.

Orgalime, the European Engineering Industries Association, speaks for 40 trade federations representing the mechanical, electrical, electronic, metalworking & metal articles industries of 23 European countries. The industry employs some 10.9 million people in the EU and in 2015 accounted for more than €1,900 billion of annual output. The industry accounts for over a quarter of manufacturing output and a third of the manufactured exports of the European Union.

1. Introduction: Industrial Cybersecurity

Cybersecurity is not an isolated policy area or an end in itself. Firstly, it is an enabler to ensure resilience, privacy, reliability, availability and safety. Secondly, it implies substantial cost and effort for companies. Thirdly, it is embedded in value chains, business cases and innovation processes. Therefore, policy measures must be seen in this context and be purposeful, adequate, affordable and innovation-friendly.

Developments such as Industry 4.0 and the Internet of Things are characterised by high market dynamics, a huge variety of business cases and multiple actors. Future business cases are mostly unknown. As with all issues which are cross-cutting, so too cybersecurity requirements will vary with the use cases and along lifecycles.

In a B2B environment, cybersecurity is dealt with in the context of business relations and is part of products and services. Market dynamics and industry-driven standards will already ensure a substantial level of security and in most cases in a flexible way. Any intervention of policy makers should be restricted to areas where markets fail and where public interest is at stake – for example, in the area of critical infrastructures.

Cybersecurity is a cross-cutting core enabler of a future digitised European industry and will have implications for every company. Therefore, it is of the utmost importance that all industrial users are involved in the debate and that a broad range of interests is taken into account. The debate must take place in representative industry-led platforms, such as the standardisation bodies which ensure broad involvement and acceptance.

2. Don’t put the cart before the horse: define requirements first

As a principle, before moving into a debate on conformity assessment, the scope and the needs have to be defined. Moving towards a European certification scheme before having evidence of the needed scope and without having established the requirements against which a conformity assessment method can be tested is taking the second step before the first. In particular, it is essential to avoid that complex schemes such as the “Common Criteria” are applied in areas for which they are not created and where they are, as a consequence, too rigid and inefficient.

3. Cybersecurity is dynamic

While cybersecurity is a key element to make the IoT a reality, in industrial applications, cyber-attack vectors are evolving constantly and therefore cybersecurity will always be dynamic. Security management requires reactive and proactive security measures. Indeed, the security environment can change literally overnight and safety concepts can become obsolete within minutes. In order to avoid that a “certified” product would be already outdated minutes after its cybersecurity certification, it is important to focus on a dynamic approach which static schemes do not necessarily offer.

4. Keeping pace with future technologies – Allowing Innovation

Technical progress has a huge impact on protective measures. For example, the requirements regarding the length of electronic keys have increased over the years. Any scheme must be open to radically new technological solutions and innovation.

In the area of cybersecurity – especially for machinery and complex systems - niche applications are relatively common and are usually custom-made for a particular product. We believe that, especially in this field, any regime should provide sufficient flexibility.

Additionally, any framework should define requirements based on a risk assessment instead of specific implementation measures: ingenuity and innovation have characterised manufacturing companies. It is their core competence to meet technological challenges with new solutions. This is the basis for ensuring healthy competition among companies to the benefit of customers.

5. Possible solutions: The way forward

It is clear, given the complexity of the engineering industry and its great variety of technologies, that a one size-fits-all approach is too simplistic and that a tailored approach per sector, subsector, product or system will often be necessary in order to satisfy the rightful expectations of customers and market needs. Accepting this as a starting point will therefore facilitate the development of rational and pragmatic approaches in an area where technology moves fast.

With this in mind, Orgalime believes that industry will put more efforts into creating and transferring security standards on product and system level in multiple sectors. The promotion and sharing of best practices will help to move into this direction. Orgalime would welcome that the Commission support such industry-led initiatives, through test-beds for example. In addition, efforts should be made to improve transparency about the capabilities and specifications of IoT devices in terms of cybersecurity. Based upon these efforts and, if considered necessary, minimum legal requirements might be discussed based on the New Legislative Framework and an appropriate conformity assessment system developed in this context.

Orgalime's members are committed to provide suggestions through best practice examples, benchmarking, expertise and through industry-driven standardisation.

In conclusion, Orgalime believes that the complex area of cyber security is and will remain a core issue which will need to be discussed throughout the wider engineering and B2B community by regulators, manufacturers, standardisation bodies and users.

*   *   *

Responsible Adviser: Christoph Riedmann (first_name.last_name@orgalime.org)