LSI SIN (14)01

Source: **Jozef Vyskoč**

Version for Publication
28.11.2014

CEPIS LSI SIN

Document for:

Decision	
Discussion	
Information	X
Publication	X

Supporting high-level decision making on cyber security and privacy protection with reliable data

CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among Informatics Professionals in recognition of the impact that Informatics has on employment, business and society. CEPIS – which represents 35 Member Societies in 32 countries across Europe – has agreed on the following statement:

1. Background

There is no doubt that both privacy protection and cyber security (i.e. addressing the problem of security of cyberspace on a national or international level) have achieved some recognition from governments and international bodies. Subsequently, the need for various high-level decisions highlights the importance of proper fundamentals for such decision making.

2. Concerns

High-level decision making in other domains usually makes use of real data (e.g. economic, demographic, etc.) allowing reasoning about the key characteristics of the respective domain, the definition of goals to be achieved as well as the measuring of progress towards these goals. This is, however, not the case for privacy protection and cyber security. As of now, there is no systematic and thought-out framework providing reliable data that can be used to infer useful conclusions for these domains. Instead, various surveys are used, though they suffer from providing solely subjective opinions and no objective data.

We believe that the lack of objective data on the domain under regulation (privacy protection and cybersecurity) increases uncertainty about how much the decisions made reflect reality. Let us consider privacy regulation as an example. Clearly, in practice there are subjects who process only a handful of boring records, but there are also subjects dealing with very large databases containing attractive and sensitive personal data. However, no reliable data on the number of subjects of one or the other type are available. Enforcing a "one size fits all" approach then leads to gratuitous duties for some data controllers, as well as grossly insufficient duties for other data controllers. Taking into account important characteristics of the target group to be regulated (in this case data controllers and the databases they deal with) may help in developing better (tailored) approaches to regulation.

Also, one should not forget that the lack of objective data impedes on our ability to study the effects of invested effort and, more generally, to better understand causes and consequences. In what follows we give just a sample of legitimate questions which are hard to answer without proper data available:

- Which regions or sectors are more likely to be attacked in the near future by cyber criminals or by hacktivists?
- Where is the most dangerous concentration of personal data (i.e. the need for increased protection)?
- Is it possible to compare threat levels for distinct sectors or countries and their changes over time?
- How can the effectiveness of the work of specialized bodies (e.g. Data protection authorities or CERTs) be assessed?
- Are we able to recognize trends and perhaps to provide reasoned predictions for the future of privacy protection and/or cyber security?

Questions like those above were not on the routine programme of specialists engaged in privacy protection or information security as they usually view such issues within the framework of one organization. However, reasoning within national or international frameworks requires solid data to argue with decision-makers on the proper ways of handling problems. We believe that both the need and the time for more systematic research and understanding of the collection of data pertaining to privacy protection and cyber security have come.

3. Recommendations

We recommend the initiation of steps aimed at acquiring reliable data to allow the study of important characteristics of target groups to be regulated in the domains of privacy protection and cyber security. For a start, existing or planned systems could be utilised, namely:

1. By adding proper questions to regular surveys (existing within the framework of official statistics) basic data on data controllers, their number, structure, distribution in sectors, regions, size of databases under control, etc. can be obtained.
2. Mandatory reporting of security incidents (considered by '*the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data'* [1] as well as '*the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union'* [2]) might be used to not only learn about the number of incidents, but also to collect useful data, such as data concerning the character of the incident, its potential impact, the character of (personal) data involved as well as data characterizing the reporting party, like the sector it belongs to, its size, and services affected by the incident.

We also recommend that communities of cyber security/privacy protection researchers and professionals [3] consider discussion and research on what data are to be collected and what indicators based on them provide proper fundamentals for high-level decision making pertaining privacy protection and cyber security.

References

[1] see Amendments 43, 125 and 154 of European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading) http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN

[2] see Amendment 97 of European Parliament legislative resolution of 13 March 2014 on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)) (Ordinary legislative procedure: first reading) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//EN

[3] including the NIS Public-Private Platform https://resilience.enisa.europa.eu/nis-platform, especially its Working group WG2