Data on Security Incidents and Consumer Confidence

There is no reliable, neutral and European-wide data on information security. ENISA will find out how difficult it is to solve this problem.

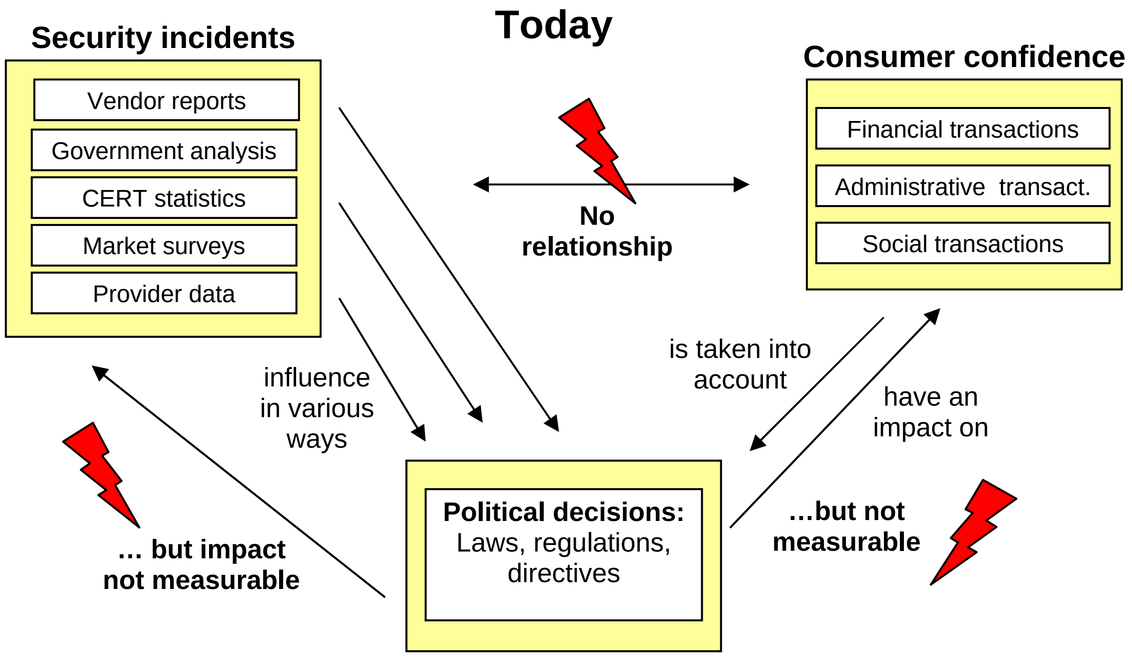
See http://www.enisa.europa.eu/pages/data_collection

Every solution must be appropriate for the size of the problem – information security should be no exception here. However, reliable information about online threats and security incidents is a scarce resource. Everybody would like to know more, but no one wants to share his own (often negative) experiences.

This is not only true for companies who implement security measures in response to an internal risk analysis, it is also true for policy makers – only that their portfolio of measures consists of laws, regulations and directives. However, when it comes to a risk analysis prior to the initiation of such measures, then policy makers often move on thin ice. So far there is hardly any analysis that is international and independent at the same time.

However, a sound legal framework is crucial to protect the citizen, not overburden the industry and maintain an efficient public administration. Legislators could make spam and spyware illegal, set a severe fine for hacking, force ISPs to manage the SMTP port or require them to report the security measures they have implemented, as it was suggested last year by an ENISA report. In any case, unilateral attempts are rarely effective; they have to be coordinated at least on the European level in order to be successful.

Judging the success of such regulatory measures is not only a question of a reduced amount of security incidents – however this is measured. It is more important that companies and citizens trust the Internet (again), which has to be proven by statistical data on financial, administrative or social online transactions.



Measuring these two parameters – security of the Internet and consumer's trust – is the goal of an initiative of the European Commission. However, considering that large parts of the network infrastructure are in private hands, both the main contributors as well as the main beneficiaries can be found in the private sector.

Ready to share?

The motivation for exchanging data is more important than the question what type of information is actually exchanged. Why should a Computer Emergency Response Team, a Managed Security Service Provider, a network operator, a vendor, or a public authority be willing to share information on security incidents with others, even if that exchange happens only once every year in aggregated form? "Give" and "take" are two sides of the same coin.

Every partner who is asked for contributions needs an incentive – be it material gain, political influence or a market advantage. Also, not every partner can contribute in the same way: some possess a wealth of data, others are willing to contribute human or IT resources, again others can offer logistical support.

In addition, the circumstances of the exchange are crucial. The first challenge is bringing everybody to the same table. Soon it will become apparent that there are far too many potential partners to reach an agreement in the short term, especially in a cross-border scenario. Moreover, some partners will have quite opposite interests. So the primary goal is to define a framework for information exchange that is both reasonable and practical.

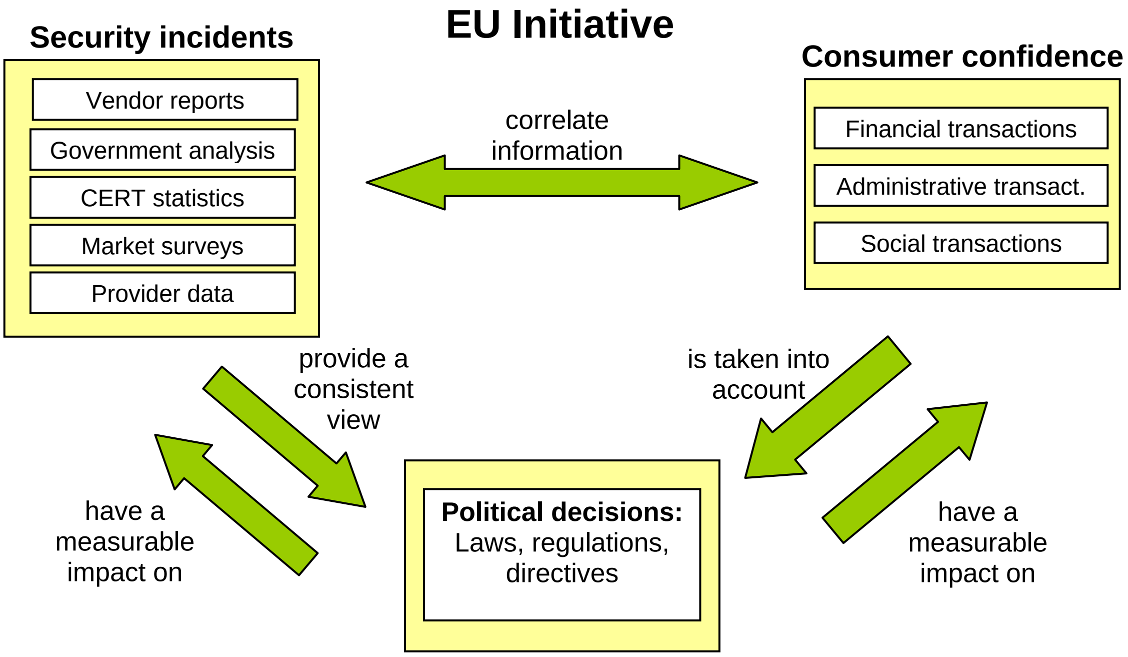
Mutual trust is the main prerequisite here. Even if data is aggregated and made anonymous - which would be more than sufficient for political decisions -, such data does represent a certain value, for example if it competes with established vendor reports. Others might fear that data can be traced to the source, despite the aggregation. Of course this depends on the way that data from different sources is assembled and by whom.

Another important aspect is that the framework guarantees a certain level of quality, but at the same time does not pose an unnecessary burden which could deter valuable partners. Ideally, there would be different levels of cooperation. On one extreme, a partner might contribute only information that is publicly available anyway, and so he just transforms the data into a different format. On the other extreme, a partner could participate in the definition of the exchange format, provide data with a high granularity, but also benefit from detailed evaluations and a high level of influence.

How can we exchange data?

It is common sense that technical, organizational, and legal measures have to go hand in hand in order to achieve an optimal solution. The private sector will only benefit if politicians rely not on expert's opinions alone, but can also base their decisions on up-to-date statistical data. On the other hand, such data would also be valuable for companies directly, for no one intends to keep the yearly reports confidential.

Sure, every company can consult the newest CSI/FBI report or DTI/PwC analysis. However, by and large these reports have a national focus, are created at different times and with different methods, and do not reflect the situation in all of Europe. Moreover, there are also reports from security vendors which describe the situation in a larger geographical context, but these are not free from vendor interests.



The aforementioned initiative is supposed to overcome these constraints: defining a framework for data collection that balances the interests of product vendors, service providers, and other private and public entities from all of Europe. The question remains whether such endeavor is realistic. ENISA will try to find an answer and would like to hear your opinion. How valuable would such a framework be for your public or private organization? Which prerequisites and potentials do you see?

ENISA has started to contact a number of potential partners individually. If you want to voice your opinion or if you feel that your organization has something to contribute to this framework, then please write an email to Carsten.Casper@enisa.europa.eu