# On Economics of ICT Security

At the beginning of 2008 ENISA (the European Network and Information Security Agency) released a study by Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore entitled "Security Economics and the Internal Market" [1] which makes a very interesting 100+ pages reading for any professional of ICT Security. We suggest everybody to read it, at least the first few chapters, to think over some aspects of the ICT Security market which matter to all of us.
In this article we will not make a summary of the report, but we will take it as a starting point to consider how much economics interests influence the development and the current status of ICT Security.
We, as ICT Security professionals, tend to believe that the development of ICT is driven by innovation and quality. It is easy to be let to believe that an innovative product, either hardware and/or software, should be very successful and that high quality products should encounter the favours of the customers. In practice, looking at today market and to what has happened in the last 20 years, we can say that this has happened unfortunately very few times.
Of course there are exceptions, that is innovative and quality products which are successful. We just have to look at the history of Apple for one of such examples. But looking at the whole ICT market, these are just indeed, exceptions which, as it is said '*confirm the rule*.'
The real truth is that, as it happens in many other manufacturing sectors, ICT is driven by prices, costs and margins: no quality and no innovation! Actually among the most successful companies are those which are able to copy an innovative product of someone else and produce a cheaper clone at lower price. You start from an innovative, high quality and costly product, which risks to give low margins to the producer due also to the costs of development and research, and by imitating it (or cloning it) another company can realize with almost no research or development, a lower cost, much lower quality and with many less features product which has much higher margins.
If the ICT would be a mature market, high quality and innovative products will be expensive but also successful and would be profitable for the producer. There would be some customers who would prefer to spend more to get something which has higher quality and more features. At the same time there would be other customers with less requirements who would go for the cheaper versions knowing that the quality of the product is not the same as the one of the expensive product but deciding to buy the cheaper one based on price and lower requirements.
Here we touch what it is probably the fundamental problem of the ICT market: customer ignorance.

When buyers are not able to appreciate and evaluate the difference in quality and features between goods, the market is inherently biased. Indeed in this situation only few criteria remain to a customer to choose between competing products, and among these criteria the most relevant are:

1. the look
2. the brand name
3. the cost.

Notice that here we are not considering the consumer market, for which look, brand name (both related to the fashion of the moment) and/or price, can be reasonable choice criteria, but the company market, that is the market of ICT products for companies. In practice most of the times a company decides which ICT product to buy based almost exclusively on

1. how good the salesman presentation is
2. the brand name
3. the cost.

The features and quality of the competing ICT products are usually brushed through by giving a quick glance at the product website or brochure and inferred from the salesman presentation. In practice the customer does not know what he is buying, and does not do a through evaluation process neither of what are his needs nor of which are the characteristics of the products is going to buy and how much they satisfy the needs of the company. Besides having a biasing effect on the market, which we will soon describe, this is quite worrisome if, for example, ICT products for national critical infrastructures would be selected in this way.

In practice it is rare that before the selection of an ICT product by a company for buying, features and quality of the competing offers are really evaluated. This is because :

1. the buyer usually does not have in-house expertise to make the evaluation
2. it is often difficult to find external expertise to make an independent technical evaluation of the competing offers
3. the process of really technically evaluating a product takes time besides expertise, and usually the product should have been installed '*yesterday*'
4. evaluation of a product costs and this is often not perceived as an investment but only as a loss.

Since the buyer cannot evaluate what he is going to buy, he is in practice obliged to adopt the selecting criteria that he can use, that is mostly look, brand name and cost, as we said.

A market driven by price is usually dominated by the '*lemon effect*' introduced by George Akerlof in

his Nobel prize winning paper [2]. The main idea is that in a market where buyers cannot ascertain the difference in quality, features etc. of products, that is a market with asymmetric information where sellers know things that the buyers do not know, there is a inherent bias which privileges what the buyers know. In our case price is the first factor and brand name comes just next to it.
In this situation high quality and expensive products tend to disappear from the market, with the only exception of fashionable and '*cool'* products. The average quality of the products goes down together with the average price. Of course there is a bottom point in quality below which the products cannot go because if they just do not work or the number of bugs is really excessive, people will not buy them any more in any case and the final risk is a contraction of the market. In this case indeed, since buyers cannot ascertain quality, they will not look for a better product, but just stop using and buying any similar product!
Another effect of the use of these selection criteria, is the concentration of the market. If brand name is the second and often the first buyer's selection criteria, it becomes almost impossible for new and innovative companies to enter the market. At the same time marketing strategies more than products development become crucial for the survival of a company, and at the end big companies tend to become bigger either by killing or acquiring smaller companies. So the market tends to become a monopoly or a market controlled by just a few companies. In the case of ICT and ICT Security in particular, this happens also at the level of market sector or slice. Consider what has been the development for example of the market of firewalls or anti-viruses in the last years: the tendency is obviously to have just a few well known brand name products which are practically identical in functionality and quality. Some very innovative products have disappeared from the market either because acquired by bigger companies or because the companies did not manage to survive. Overall it is not clear at all if the quality of the ICT Security products is increasing with time, and our personal opinion is that the current quality level of the ICT Security products falls short of what were the expectations of a few years ago.
So in the situation of a market driven by price and brand name, the market tends to align itself to the bottom sustainable quality level, with the lowest prices for the buyers and the highest margins for the sellers. In this situation of the ICT market, Security as a quality component of each ICT product, is what suffers the most. We all know very well that Security costs very much and it is often an impediment to features and performance, so Security is the first also to be left out of a product, minimized as much as possible or introduced only if really strictly necessary.
As we said, if buyers do not ask or care for Security, why should the producers spend more money

in the development and offer more expensive but more secure products? Nobody would buy them. The sad status of ICT Security is that, except that for Security professionals, very few really care about it and Security is considered in the development of a ICT product only if it is absolutely necessary not to go below the bottom quality level, that is when the risk that the product would just not work is too high.

If this is the trend of the ICT market, what can we do to change it and make it an healthy market? The obvious answer would be to educate the customers. This of course must be done and it is ongoing, even if more efforts must be put in it. If most buyers would be competent buyers, able to judge the features of the products and willing to pay more for a more secure product or at least conscious that a less expensive product could be less secure or provide less features etc., then we would not see the ICT market aligning itself towards the bottom.

But ICT is a new thing for humans, and machines and men speak and think in different languages. It will take a long, very long time before we, men, get used and understand what it means and how to handle the pervasive irruption of ICT in our lives which has happened in the last few years. Moreover ICT is still changing itself and our lives at a tremendous and dazzling pace so that at the end we are every day using tools that mostly we do not understand.

But the risks we run into today by our dependency on ICT technologies are too large to allow us to wait for 10 or 20 years for a completely free ICT market to balance and cure itself.

The only way to go is to force the pace of this development by regulating the ICT market. By introducing laws, regulations and commercial standards which require widespread adoption of some procedures and technologies, it is possible to force the ICT market to develop and include Security features which otherwise would not even be considered.

The introduction of standards, regulations and laws is an opportunity for producers to innovate and develop new products, and for customers it is an opportunity to learn something new and understand better the possible consequences of the use of ICT tools. This is of course already ongoing process, consider for example the consequences on the ICT market of the introduction of SOX in the US and of the Privacy normative in the EU.

An analogy which is often done, and sometime is appropriate other times less, is between the ICT and the automotive or car market. The automotive market, at least in north america and europe, is regulated in the sense that producers can sell vehicles only if they satisfy some security features and pass various tests. The market is otherwise free, but the buyers are guaranteed by the state that whichever vehicle that they can buy has some minimum tested safety features. So buyers do not

need to have the expertise to evaluate the safety features of a vehicle, since they are guaranteed by the state that anything that they can buy has already been tested. Moreover car makers are also responsible for defects of their products and there is a well developed market of liabilities and insurances.

Of course, the automotive market is an old and by now well developed market, still is partially regulated and it will always be to guarantee that its minimum quality level is high enough for the customers.

So something similar should be introduced also in the ICT market to guarantee to all buyers that all security features which are deemed necessary are present and tested in any ICT product which they can buy. Even if stated like that it looks like a dream, as we said this process has already started, but still a long way has to be done.

In any case even this path it is not easy at all. First of all, those who write these laws, regulations or standards must really understand well not only the legal aspects of them but also all possible technological aspects. There are many examples of proposed laws which if enacted would have for example implied that internet would have become completely illegal in that nation just because those who wrote the law had a very vague and wrong idea of what ICT is and how it works. Introducing plainly inapplicable requirements or even just badly worded ones has the consequence of making people less sensitive to them and less willing to implement them, so practically voiding the effect we would like them to have!

ICT Security professionals must participate to the writing of these laws, regulations and standards and must dedicate time and efforts to educate those responsible for them to the intricacies and subtleness of ICT Security. This is probably not what most of us dream to do, but today it is a necessary part of our job.

Once laws, regulations and standards are in place, they must be enforced. To this end someone must verify that they are put in place. This again is not an easy task and requires the direct participation of ICT Security professionals. Today ICT Security audits are too often formal checks that papers are in order more than Security evaluations of the real ICT infrastructure. For an extreme example it has even happened that the check was on the buying of the firewall but that the fact that it was still in its box unpackaged did not matter too much.

The important message which ICT Security professionals should send to the companies is that ICT Security audits are not against their interests but actually are very useful to them. Companies should learn from very negative assessments since they can then understand where their biggest ICT

Security problems lie, how they can approach them and what they should ask their suppliers to give them. It is not good neither for the auditors nor for the companies to minimize the problems and make it look as if everything is ok when it is not. Even if it can feel self-absolving and auto-congratulating, at the end it is in nobody interest to minimize or overlook ICT Security problems. It is not even in the interest of the ICT market since only by knowing which are our risks and weaknesses we can force the development of the market towards a more safe and secure future ICT.

Andrea Pasquinucci
PhD CISA CISSP

http://www.ucci.it/

[1] The report can be downloaded from http://www.enisa.europa.eu/

[2] G. Akerlof, *The market for 'lemons': quality uncertainty and the market mechanism*, Quart.J.Economics, 84, 1970, 488