Cybersecurity Strategy for the European Union

An Open, Safe and Secure Cyberspace[1]

Remarks from CECUA

Cyber-incidents and Cyber-insurance

In previous remarks CECUA welcomed the alignment of on-line and off-line. Alignment of off-line and on-line and same values, same laws and the jurisdiction lies with off-line. This is a good start.

But the alignment should go further and make use of well-established off-line processes and procedures also for on-line where ever at all possible. There is no need at all to reinvent the wheel.

One of those off-line procedures and processes is incident reporting such as break-ins and fires. Why can we not use same procedure and processes for on-line incidents/attacks? An attack is an attack, it is a break-in into the network/computers of the company involved. It causes financial damage, reputation damage, value damage to the company owners.

In case of a break- in a company reports the incident to the police and its insurance company. Why should there not be the same/similar procedure for on-line incidents/attacks? Why not report the on-line break in incident/attacks to the police and the insurance company? Why should on-line break ins/attacks be kept secret while off-lines are treated as public information and reported in the media?

Both kinds of incidents cause financial loss to the companies involved and are a tarn on their reputation and reduce the value for the owners. The only real argument is that the police are presently not equipped to deal with on-line break-ins. All along off-line incidents have been the police domain. Now they have to add the on-line incidents. And the police are not equipped to deal with the on-line incidents/attacks. The CECUA computer network was attacked. The incident was reported to the police. They did not see it necessary to visit the CECUA office but advised CECUA to buy a virus protection software. If the CECUA office had been broken into, the window panes broken or the door had been forced open the police would have been on site looking for finger prints or other evidence. Nothing like this happened. Instead an elementary advice over the phone? Nothing came out of it. Now the Commission wants to step in. The Commission wants companies to report on-line incidents just like off-line ones. That calls for establishing competent police units to receive the reports and investigate them. First reaction is that this is a member state issue. UK is moving ahead preempting the Commission. But only

during office-hours. But it is not so simple. In many/most cases cross border issues are involved, the perpetrator, the one committing the on-line crime is not residing in the same country as the company being violated. This makes the investigation and prosecution a complex and complicated issue. The commission has created a new on-line police unit attached to Europol. This unit will have the role to coordinate cross border crimes and bring the perpetrator to justice. But in many cases it is not an EU cross border issues, it is an international border issue. But the EU Europol unit can only do so much. Here only an Interpol unit will help. That calls for an international agreement on cyber incidents/attacks follow up investigations and prosecution. The Europol is a good first step. But more is needed.

Cyber-incidents and Cyber-insurance

What about the insurance side? CECUA research has found little data about the EU situation but the more about the USA situation [2,3,4,5]

"Any high-value organization has been or will be attacked soon — that is almost certain in today's world,"[2] William Stewart, the leader of Booz Allen Hamilton's Cyber Technologies Center of Excellence is quoted to say. This statement surely applies not only to USA but also to Europe. Fear of a Cyber-attack tops the list of major business risks that CEOs are most concerned about, according to a recent study sponsored by American International Group[2].

Cyber-insurance is the term for insurance against cyber- incidents/attacks. How many companies carry on-line incident Cyber-insurance? The Cyber-insurance has been available for some time but has only recently been catching on. In USA Cyber-insurance is growing fast with 30% of all large companies carrying such an insurance. The estimated total insurance premium for Cyber-insurance was about USD 1 billion in the United States alone last year and is expected to grow to USD 1.2 billion this year. Europe lags far behind the USA with only 5% of companies having Cyber-insurance coverage. That is very low because the risk is similar in Europe as it is in the USA, the risk is a global issue. The strategy does not make any reference to this situation. It does not urge EU companies to buy Cyber-insurance coverage not to mention that here is a big opportunity for EU insurance companies. Only the EU Cyber-strategy urges insurance companies to let cyber-insurance buyers profit from investing in security measures when it comes to premium payments.

It is leaving out that also this is a big opportunity for insurance companies to extend their line of products to include cyber-insurance.

CECUA feels that the EU with its strategy has done a lot to clear the mysticism which has been surrounding the Internet and the Web. On-line and Off-line is easy to understand and getting rid of the mysticism around virtual world or virtual space

is an achievement indeed. Demystifying is good but action is better. Delivering action on this strategy will be a big challenge for the EU and its Member States.

Dr. Jon Thorhallsson

CECUA President

jon.thorhallsson@cecua.org

[1] http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

[2] http://www.cnbc.com/id/100512627

[3] http://www.microsoft.com/business/en-us/resources/finance/business-insurance/small-busines-cyber-insurance.aspx?fbid=KrDQ56egc-V

[4] http://abcnews.go.com/Technology/story?id=99343&page=1

[5] http://www.computerworlduk.com/advice/it-business/3312969/is-hacking-insurance-worth-it/