

PRIVACY STATEMENT

Please be sure to **indicate** if you **do not consent** to the **publication** of your personal data with the publication of your response or if you require us to publish your contribution anonymously. By responding to this "Invitation for Comments" you automatically give permission to ENISA to publish your contribution on the website unless your opposition to publish your contribution is explicitly stated in your reply. ENISA is committed to user privacy. Details on the personal data protection policy can be accessed at:
<http://www.enisa.europa.eu/pages/disclaimer.htm>

NO, I do not consent to the publication of my personal data. xYES, I do consent.

Organisation / Name:

NASK, Poland/Krzysztof Silicki

Contact Details:

Krzysztof.Silicki@nask.pl

Report "Security Economics and the Internal Market"

by

Prof. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore

Guiding Questions for Stakeholder Comments on the Report and its Recommendations

1. RECOMMENDATION: Security Breach Notification

[p. 22-26]

Does the EU need a security-breach notification law?

This recommendation should not be treated as the most important factor for ICT security improvement. Further analysis is needed whether examples of security-breach notification regulation existing in some member states are really helpful. At least one example from one member state exists, where ISPs are obliged to deliver security incidents information to the regulator and they report near zero incidents (which is not likely to be real data) therefore it can lead to false conclusions about overall security level in the country.

What policy instrument would be most appropriate: legislation, (public/private) co-regulation, self-regulation etc.?

Self-regulation should always be treated as preferred policy instrument. On the

other hand it is probably the most difficult model to achieve. To gain from this instrument, stakeholders should have some incentives to adopt self-regulation approach. Unfortunately “Security Economics and the Internal Market” report is lacking of possible incentives analysis and ideas. Therefore this work should be continued to find possible positive incentives – not only penalisation threat for telecoms, ISPs, banks, or home users.

Should the scope of security breach notification go beyond the telecom and ISP sectors? Should all e-communication service providers and/or all service providers in general be included?

All those players should be included – but in sense that concrete incentives should be developed for them as they could adopt self-regulation model most easily. That approach would show real picture of ICT security in Europe.

Are there lessons to be learned from experiences in some US states? What are good practice examples?

Not only lessons from US should be taken into consideration but also some existing examples from EU member states. It requires further work on this issue.

2. RECOMMENDATION: Electronic Crime Statistics

[p. 44-45]

Should the EU introduce new regulation in order to ensure the publication of loss statistics for electronic crime?

The existence of real statistics is very important. To achieve this a common standard for collecting data and producing statistics should be adopted first. It is obvious that bad or inaccurate statistics are worse than no statistics at all because they could be misleading. We have examples in our country that computer crime statistics, when conducted without strict guidelines for respondents and special care in interpretation result in wrong conclusions.

What is more, harmonizing common standards among member states is an additional challenge. Before decision about new regulation an analysis of working examples in member states should be performed.

<p>Should the EU Expert Group set up by the European Commission following the Communication “Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: An EU Action Plan 2006-2010” include electronic crime statistics in the planned framework?</p> <p><i>Generally, yes.</i></p>
<p>Should reporting on particular indicators be made mandatory?</p>
<p>Should EU Member States, national regulators, industry associations and ISPs be encouraged to make such statistics available?</p> <p><i>Yes, those stakeholders should be encouraged to do this. As stated in previous section the collection of incentives should be developed to help this process to be developed.</i></p>
<p>3. RECOMMENDATION: Bad Traffic Statistics [p. 45-46]</p>
<p>Should quantitative data on ISPs’ security performance be made available to the public?</p> <p><i>There is unclear function of such data to be presented to the public. Especially media and competitive market will probably use it to cause a sensation or black PR. On the other hand such a data – if authentic and true – should be available to policy makers or independent expert organisations , like ENISA.</i></p>
<p>Should ENISA collect and publish data about the quantity of spam and other bad traffic emitted through European ISPs?</p>

ENISA as independent body could collect such a data and use it to characterize the phenomenon and publish aggregated data.

What would be useful metrics to measure bad traffic?

4. RECOMMENDATION: Removal of Compromised Machines [p. 49-54]

Should the EU introduce a statutory scale of damages against providers that do not respond promptly to requests for the removal of compromised machines?

Providers should co-operate with not only law enforcement but also with organisations combating illegal security incidents – like CERTs or Hotlines fighting with illegal content on the Internet. That requires either developing set of incentives for providers either clear regulations – ideally: both.

Existing European initiatives should be assessed to collect lessons about whether and how regulations applied on providers are turning out to be successful.

Should such a scale be coupled with a right for users to have disconnected machines reconnected if they assume full liability?

What would be alternative means for dealing with compromised machines which remain connected to the network?

It is not only about compromised machines but also hosts which contain: illegal or harmful content, malware and other dangerous stuff.

If the owner of the machine is not cooperating with his/her ISP – provider should have right to put this machine into quarantine. If ISP do not want to react to complaints from other users, incidents handled by CERTs or cases conducted by LEA there should be an “escalation mechanism” (penalty fine?) adopted in eg. telecommunication law.

5. RECOMMENDATION: Secure Equipment by Default

[p. 59-61]

Should the EU re-allocate slices of liability in response to specific market failures?

Some form of liability is needed from the market perspective. But it should be “negotiated” with stakeholders and treated as an evolutionary process (a roadmap) to achieve wider and wider commitment.

Should the EU develop and enforce standards for network-connected equipment to be secure by default?

Yes, developing and promoting standards to achieve security by default is really important issue. Nevertheless standards should not be enforced – better mechanism is to build user/buyer awareness who then will be choosing products with better embedded security.

Should vendors be required to (self-)certify that their products are secure by default?

Yes, it seems to be a good idea.

6. RECOMMENDATION: Responsible Disclosure and Fast Patching [p. 61-64]

Should the EU adopt a combination of early responsible vulnerability disclosure and vendor liability for unpatched software?

Liability for too long time of unpatched software is important. On the other hand vendors who are applying fast patching BUT their software is so vulnerable that they have to issue patches every week should not be treated as positive example. Vulnerability disclosure should be understand as “need to know” approach. It means that users which can suffer from particular vulnerability or threat more than others (e.g. government, banking sector, corporations) or can help others (e.g. CSIRTs/CERTs) should learn about this vulnerability or threat as quick as possible. After that broad disclosure can occur.

Would responsible vulnerability disclosure be more efficient in the long-run as it creates a constructive relationship among stakeholders?

Yes, responsible vulnerability disclosure can create partnership relations among stakeholders.

What would speed up the process and hence make information systems more secure?

It is crucial to understand different interests of different stakeholders. E.G. tough competition between vendors is shortening time to lead of the software and hardware products. This, quite often is related to poor level of the security of those products. On the other hand consumers more and more aware of security issues would press vendors in a mid term scale to deliver more secure products.

7. RECOMMENDATION: Security Patches

[p. 64-65]

Should security patches be offered for free?

Yes.

Should they be kept separate from feature updates?

Yes.

Should end-users be made liable for infections if they turn off automated patches or otherwise undermine the secure defaults provided by vendors?

Assuming that end-user is aware of what she/he is doing we can talk about liability. So when it is proved that user intentionally turned off security measures – he/she is liable.

On the other hand nobody should assume that user is an IT expert who should understand what it is firewall and how to configure it. Car user is not responsible for “configuring” or “enhancing” his car. He use it as it was sold by the car dealer. But the driver has manual (to learn how to use car properly) and driving license (he understands his liability for being dangerous to others)

8. RECOMMENDATION: Electronic Payment Dispute Resolution [p. 65-66]

Should the EU harmonise procedures for the resolution of disputes between customers and payment service providers over electronic transactions?

Should the Payment Services Directive be amended by tackling the issue of varying fraud liability and dispute resolution procedures among EU Member States?

Would any other legal instrument be more appropriate to address this problem? If yes, which form of legal instrument (e.g. public-private co-regulation, self-regulation) do you consider more beneficial?

9. RECOMMENDATION: Sanction Abusive Online Marketers [p. 67-68]

Should the European Commission take action by preparing a proposal for a directive establishing a coherent regime of proportionate and effective sanctions against abusive online marketers?

Yes, it is worth to put an effort to establish sanctions to those who are the sources of eg. spam campaigns.

Should the existing Directive on Privacy and Electronic Communications (2002/58/EC) be revised in the light of abandoning the business exemption for spam?

Would any other legal instrument be more appropriate to address the problem concerned? If yes, which form of legal instrument (e.g. public-private co-regulation, self-regulation) do you consider more beneficial?

The process of punishing spam campaigns originators should be supported by advanced technology (database systems) collecting and semi-automatically analyzing spam.

10. RECOMMENDATION: Consumer Protection Law [p. 68-70]

Should the European Commission / ENISA conduct research to study what changes are needed to consumer protection law as commerce moves online?

Yes, it is important task.

Should ENISA consider becoming involved in the wider European Commission policy process, considering security aspects of policy along with consumer protection questions?

Rather yes.

Should the European Commission address the issue of right to Internet connectivity?

11. RECOMMENDATION: Logical Market Diversity

[p. 71-73]

Should ENISA seek to advice Competition Authorities whenever diversity has security implications?

No.

Should ENISA take an active role in providing expertise to decision-makers with regard to security threats that follow from a lack of diversity?

No.

Should ENISA liaise with the European Commission's Interoperable Delivery of European e-Government Services to Public Administration, Businesses and Citizens (IDABC) in order not only to ensure interoperability and competition but also security?

Yes.

12. RECOMMENDATION: Study IXP Failures

[p. 73-77]

Should ENISA engage in research to better understand the effects of Internet exchange point (IXP) failures?

It is not directly connected to "core" problems of ICT security.

Should telecom regulators be involved to insist on good practice in IXP peering resilience?

Good to think about this issue. Good practise can help.

Would you agree with the report's observation that the Access and Interconnection Directive (2002/19/EC) has had limited impact on Internet transit provision?

As regards peering arrangements, would you agree with the report's observation that distortion of competition is taking place as smaller ISPs/ IXPs encounter disadvantages compared to large ISPs?

It is normal market effect, on the other hand smaller ISPs should have – to some extent – assistance in ISPs associations and law to avoid distortion of competition.

13. RECOMMENDATION: Ratification of Council of Europe Cybercrime Convention [p. 78-79]

Should the European Commission continue to put pressure on the EU Member States that have yet to ratify the Council of Europe Convention of Europe?

It is important , so EC pressure is needed.

In following up on the European Commission Communication on Cyber Crime, would you envisage new regulation including mandatory blocking of website with particular content and controls on search engines?

Yes, the problem of harmful content is growing, websites are fast moving from one country to another to avoid punishment and unwanted content is rarely blocked at all. I would prefer including mandatory blocking topic.

Would you envisage new EU regulation on any other issue?

Roadmap for ICT security development

To successfully plan future higher level of culture of security it is essential to create and adopt in Europe a roadmap for step by step process of developing substantially higher level of general security in electronic market.

With this goal in mind it is necessary to:

- *make description of the phenomenon by collecting the most important:*
 - *obstacles that restrain progress in ICT security*
 - *limitations and problems that are indicated by different stakeholders of electronic communication market*
 - *make a diagnosis of the problem taking into consideration different incentives, interests and goals of all stakeholders*
- *propose possible solutions in frame of which roles and responsibilities of all stakeholders:*
 - *governments*
 - *consumers*
 - *providers*
 - *vendors*
 - *international bodies*
 - *academia*

will be defined

- *establish a schedule of action items, milestones and checkpoints to monitor the progress of work*

It is very important to build the culture of security in a coordinated manner using all possible incentives, initiatives, programs and projects that are focused on ICT security

European Commission with substantial support from ENISA has the right power to initiate a roadmap for ICT security that can make breakthrough in this area and to create the strategy for the future.

14. RECOMMENDATION: EU-wide Co-operation on Cyber Crime [p. 79-81]

Should an EU-wide body be charged with facilitating international co-operation on cyber crime, using e.g. Europol and/or NATO as a model?

Not necessarily. It would be enough to define “cooperation interfaces” between all pillars of the security area. Now Europe is lacking of cooperation rules and practise between organisations dealing with NIS, cybercrime, terrorism, etc. Interfaces among those parties are not defined what is a fatal flaw since security is a horizontal problem.

Would you envisage any other good practice example of cross-jurisdictional co-operation in the international framework?

Global CSIRT cooperation.

15. Open Question: Incentives for Lifting Barriers

In which other areas do you see barriers for NIS in the Internal Market?

Which incentives (regulatory, non-regulatory, technical, educational, etc.) would you suggest for lifting barriers identified to cause distortion of the smooth functioning of the Internal Market for e-communication?

The need for coordinated action plan

Every party, every stakeholder of electronic communication market should perform a systematic action on their field:

- software and hardware vendors should take care of substantially higher quality of their products in terms of reliability and security –best incentives for vendors create users aware of security issues, other incentives should come from certification instruments,*
- research and development environment (both academia and industry) should examine critical obstacles of fast ICT security development as well as should create methodologies of developing secure architectures, protocols, information technology environment to accelerate adoption of security standards – incentives*

for this area should be created by R&D policy of EU

- *governments having a lot to do should probably:*
 - *introduce the incentives of applying proper standards and minimal security requirements as well as promoting best practices in ICT security,*
 - *take care of better education and awareness of information society especially in terms of culture of security among young users,*

 - *support concrete programmes and actions (e.g. using public private partnership) aiming in building immunity of SME and home users against Internet and new communication media threats,*

 - *support development of computer law and proper capabilities of law enforcement*

 - *define critical infrastructure of the country (private and public) and adopt optimal model of its protection*

- *telecom operators and electronic services providers should ensure high level of security for their services as well as inform users about threats and security incidents and cooperate with other parties to achieve higher level of coordination in reacting for incidents, threats and vulnerabilities – self-regulation incentives should be examined,*

- *consumer organizations should have power to defend users of electronic services facing products and services that not meet minimal standards of security or forcing them to become “security experts” when they want to operate in secure mode,*

- *home users should have knowledge how to use electronic, on-line tools in a secure manner and to cooperate with other stakeholders to raise the culture of security – governments together with providers should create incentives for awareness raising of home users,*

- *international institutions and organizations should adopt the roadmap for rapid and coordinated development of ICT security in collaboration with all stakeholders of electronic communication market,*

- *independent ICT security experts and organizations should cooperate to find effective methods of supporting: public administration, vendors, telcos and research institutions with state of the art knowledge about urgent directions needed to be addressed in ICT security; the voice of experts should become one of the most important element to achieve a positive breakthrough in this area.*