

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. YES, I do consent.

Organisation / Name:

Ministry of Foreign Affairs, Poland /

Piotr STRUTYNSKI

Contact Details:

ps_cdn@wp.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?

Notification is important but not crucial. I'd rather see it as a recommendation not a law enforcement.

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

Various complementary instruments should be used stressing the importance of self-regulation. The problem itself is too complex to summarise it in few sentences.

<p>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?</p> <p><i>The scope should be possibly widest.</i></p>
<p>Are there lessons to be learned from experiences in some US states? What are good practice examples?</p> <p><i>All lessons should be taken into account not USA experiences only.</i></p>
<p>2. RECOMMENDATION: Electronic Crime Statistics [p. 44-45]</p>
<p>Should the EU introduce new regulation in order to ensure the publication of loss statistics for electronic crime?</p> <p><i>To avoid surplus regulations I suggest to look through existing regulations thoroughly instead of imposing new ones.</i></p>
<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>Yes.</p>
<p>Should reporting on particular indicators be made mandatory?</p>

It is to discuss. The question is not very clear.

Should EU Member States, national regulators, industry associations and ISPs be encouraged to make such statistics available?

Yes. It can be helpful.

3. RECOMMENDATION: Bad Traffic Statistics

[p. 45-46]

Should quantitative data on ISPs' security performance be made available to the public?

It should rather be available for experts. I am not convinced media could make a good use of such an information.

Should ENISA collect and publish data about the quantity of spam and other bad traffic emitted through European ISPs?

Some general statistics should be published by ENISA.

What would be useful metrics to measure bad traffic?

Companies / corporate (volunteers) could report ENISA the volume (in bytes) of information rejected automatically by their servers monthly, as well as the volume of the traffic accepted.

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?

Certain clear regulation should be developed to combat with malicious activity in Internet. Co-operation between providers and organisations like ENISA is highly recommended.

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

It is very restrictive idea.

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

It seems to me there are some regulations protecting "ordinary users" against malicious activity. At least a brief look through national regulations should be done. Some solutions could be implemented into EU law if necessary.

5. RECOMMENDATION: Secure Equipment by Default

[p. 59-61]

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

It is to discuss. The idea seems be good but very general.

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

To define such standards should not be difficult, but to implement and enforce them could be a nightmare.

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

Yes (as a recommendation for them).

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?	
<i>Incentives for vendors to improve their products should bring some positive results.</i>	
Would responsible vulnerability disclosure be more efficient in the long-run as it creates a constructive relationship among stakeholders?	
<i>Yes, responsible vulnerability disclosure can create partnership relations among stakeholders.</i>	
What would speed up the process and hence make information systems more secure?	
<i>Contradictory vendors and consumers goals will influence the process. I am not convinced a substantial speed up would be possible.</i>	
7. RECOMMENDATION: Security Patches	[p. 64-65]
Should security patches be offered for free?	
<i>Absolutely.</i>	
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?

There are various possibilities to avoid infection. Automated patches is one of them. In case of malicious activity we may talk of "liability" only.

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?

It seems we can rely on existing law regulations.

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.

<p>Should the existing Directive on Privacy and Electronic Communications (2002/58/EC) be revised in the light of abandoning the business exemption for spam?</p> <p><i>Yes. In my opinion we should rather talk about “malicious activity” in general, than “spam” only.</i></p>
<p>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?</p>
<p>10. RECOMMENDATION: Consumer Protection Law [p. 68-70]</p>
<p>Should the European Commission / ENISA conduct research to study what changes are needed to consumer protection law as commerce moves online?</p> <p><i>Yes.</i></p>
<p>Should ENISA consider becoming involved in the wider European Commission policy process, considering security aspects of policy along with consumer protection questions?</p> <p><i>Yes.</i></p>
<p>Should the European Commission address the issue of right to Internet connectivity?</p> <p><i>To discuss.</i></p>

11. RECOMMENDATION: Logical Market Diversity	[p. 71-73]
<p>Should ENISA seek to advice Competition Authorities whenever diversity has security implications?</p> <p><i>No.</i></p>	
<p>Should ENISA take an active role in providing expertise to decision-makers with regard to security threats that follow from a lack of diversity?</p> <p><i>No.</i></p>	
<p>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?</p> <p><i>Yes.</i></p>	
12. RECOMMENDATION: Study IXP Failures	[p. 73-77]
<p>Should ENISA engage in research to better understand the effects of Internet exchange point (IXP) failures?</p> <p><i>Yes, but I would not devote too much time to it.</i></p>	
<p>Should telecom regulators be involved to insist on good practice in IXP peering resilience?</p> <p><i>Exchanging experience and any information of good practice is helpful.</i></p>	
<p>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?</p>	

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?

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?

Undoubtedly.

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?

It is growing problem and regulations are necessary. Blocking website should be one of recommended measures.

Would you envisage new EU regulation on any other issue?

I would like to stress the necessity of people education regarding the threats in ITC systems. Starting from the very beginning in primary schools during computer science lessons. Just like as we teach children how to cross a street. During the education we should not forget about the ethic aspect of hostile activity against ITC systems. If we teach young people to take advantage of common sense it can bring better effects than administrative regulations.

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?

Rather not. Charging them with international co-operation in cyber crime will cause additional costs bringing no effect.

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

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?

Few remarks regarding government level:

- *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 especially in terms of culture of security among young users,*
- *support programs and actions 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*