

## 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:**

**Malta Communications Authority**

**Contact Details:**

Steve Agius – [sagius@mca.org.mt](mailto:sagius@mca.org.mt)

## 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?

**Yes. The percentage of businesses serving customers across public communications networks, continues to grow, as does the need to adopt a harmonised data security breach notification mechanism.**

**Businesses need to be aware of their general obligation to safeguard against data security breaches, both by attempting to secure their own systems and by ensuring that their service providers do the same.**

**The most important variation on the California's Security Breach Information Act (SBIA) has been the introduction of a risk-based exception, allowing affected entities to avoid notification based on their own assessment that the risk of harm is less than a statutorily defined standard. This approach should be considered prior to any legislative provisions being adopted in the EU.**

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

**A specific law would be the most effective.**

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?

**The scope of the security breach notification should be directed towards organisations (controllers) that obtain and store personally identifiable information in computerised data files immaterial of scope and industry. This should include state government agencies as well as companies and non-profit organizations regardless of geographic location and size. However any regulations should take into account cost / benefit considerations as too onerous obligations could have a negative impact on businesses.**

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

**While most states follow some version of the California model, many significant and key differences appear throughout the landscape of these data security statutes. In some cases, a seemingly small difference in language from one state to another can have a large impact on what is considered an appropriate response.**

**In establishing a US Multistate Strategy, the following areas need to be considered: the triggering event, the entities covered, the information covered, and the penalties and enforcement imposed.**

***Source: U.S. Data Breach Notification Law: State by State By John P. Hutchins, Anne P Caiola,***

## **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?

**Yes and No. Some argue that this would place a huge reporting burden on ISPs and the industry. It is also argued that investment would be more effective if spent on technology and law enforcement resources to battle cyber crime rather than on data capturing and analysis mechanisms.**

**On the other side of the coin, the publication of loss statistics would raise awareness making any plan more effective and less bound to fail.**

**Having said this we feel that this proposal is somewhat unrealistic as major undertakings would strongly resist such a legislative measure. Perhaps such laws could be more effective if they only required provision of such data to competent entities under confidential cover.**

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?

**Crime statistics should be obtained from current available sources. An**

**evaluation study should be conducted to establish whether these sources of data would be sufficient.**

Should reporting on particular indicators be made mandatory?

**Mandatory quantitative data collection should be introduced in a phased approach. In any event this would depend on the nature of the indicator and the costs of compiling the data.**

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

**Yes, provided statistics are compiled and presented in a 'user-friendly' manner with minimal cost on all parties.**

### **3. RECOMMENDATION: Bad Traffic Statistics**

**[p. 45-46]**

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

**In practice, there is a big challenge to rationalise the diverse ways ISPs collect such data in a way that can be interpreted and compared by the general public. A homogeneous model would have to be established to ensure that data can be compared effectively. The complexities involved could therefore outweigh benefits.**

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

**The only way ENISA can achieve this is by employing its own probes and collect data directly from source. In this way, data could be rationalised and would not create extra burdens on the ISPs.**

What would be useful metrics to measure bad traffic?

**The term 'Bad Traffic' is to be defined and qualified. It is after this has been established that effective metrics can be established.**

### **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?

**In a real world, such measure would create the awareness and would put a price tag for not running a safe network. However, at any one time there are millions upon millions of compromised hosts on the Internet. Establishing real-time monitoring mechanisms to monitor this huge number of hosts is a real challenge. Such a proposal could also increase costs so as to have a negative impact on the information society so again costs / benefits would have to be very carefully weighed.**

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

**Same as the above – one has to establish the amount of supervision required to enforce such a measure.**

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

**ISP's in conjunction with involved undertakings and the security community can identify and filter traffic from compromised machines. This is already being done as far as spam and phishing is concerned.**

**5. RECOMMENDATION: Secure Equipment by Default**

**[p. 59-61]**

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

**This is an interesting concept that merits full evaluation.**

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

**Companies who take security seriously already do this. Although, security comes at a very high price, the market is the main driver and companies will have no option but to take security seriously in order to retain market share and increase competitive advantage.**

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

**One has to establish what is meant by 'secure by default.'  
Same reasons as previous question.**

**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?

**Very good recommendation, however, one has to establish whether this should be applied to all software/software vendors.**

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

**Yes, responsible vulnerability disclosure in most of the times improves the relationship between a vendor and its customers. However, one has to establish whether such vulnerability disclosure would create a negative impact and consequently tension between the stakeholders.**

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

**Market forces, publication of threats and True Downtime Costs (TDC) have made Information systems much more secure over the last decade.**

**7. RECOMMENDATION: Security Patches**

**[p. 64-65]**

<p>Should security patches be offered for free?</p> <p><b>Yes, it is the responsibility of the software vendor to ensure that the security of his software/appliance is not compromised as new threats come out.</b></p>
<p>Should they be kept separate from feature updates?</p> <p><b>Yes, this would make it possible for the software vendor to be able to charge separately for feature updates (added functionality).</b></p>
<p>Should end-users be made liable for infections if they turn off automated patches or otherwise undermine the secure defaults provided by vendors?</p> <p><b>Users should be held liable for their own actions if these are intentional.</b></p>
<p><b>8. RECOMMENDATION: Electronic Payment Dispute Resolution [p. 65-66]</b></p>
<p>Should the EU harmonise procedures for the resolution of disputes between customers and payment service providers over electronic transactions?</p> <p><b>Effective dispute resolution procedures should exist but harmonisation may be unwarranted.</b></p>
<p>Should the Payment Services Directive be amended by tackling the issue of varying fraud liability and dispute resolution procedures among EU Member States?</p>
<p>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?</p> <p><b>Self-regulation would appear to be sufficiently effective.</b></p>
<p><b>9. RECOMMENDATION: Sanction Abusive Online Marketers [p. 67-68]</b></p>
<p>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?</p> <p><b>This is an interesting proposition. One could even go as far as to suggest that ideally base-line rules should extend beyond the EU to be truly effective whilst not “penalising” European enterprise. Having said this, one has to be careful not to go beyond what currently applies in the physical world.</b></p>
<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><b>Yes.</b></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><b>See above.</b></p>

<b>10. RECOMMENDATION: Consumer Protection Law</b>	<b>[p. 68-70]</b>
<p>Should the European Commission / ENISA conduct research to study what changes are needed to consumer protection law as commerce moves online?</p> <p><b>Yes, however, such study should not propose more regulation that will hinder creativity, innovation and growth. Furthermore it would not appear to fall under the remit of ENISA.</b></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><b>ENISA should be more involved in research studies and make these studies available to MS in a timely fashion, it should not concern itself directly with consumer protection issues.</b></p>	
<p>Should the European Commission address the issue of right to Internet connectivity?</p> <p><b>The terms and conditions and ‘modus-operandi’ of ISPs should reflect and respect laws that are already in place. (equal employment, free speech, avoidance of discrimination, etc.)</b></p>	
<b>11. RECOMMENDATION: Logical Market Diversity</b>	<b>[p. 71-73]</b>
<p>Should ENISA seek to advice Competition Authorities whenever diversity has security implications?</p> <p><b>A diverse environment is more stable and much harder to attack. ENISA should use its social networks (contacts) and resources to advice MS on how they can improve the prospects for diversity.</b></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><b>Yes, in conjunction with other bodies.</b></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><b>Yes, but the level of interoperability should not hinder diversity.</b></p>	
<b>12. RECOMMENDATION: Study IXP Failures</b>	<b>[p. 73-77]</b>
<p>Should ENISA engage in research to better understand the effects of Internet exchange point (IXP) failures?</p> <p><b>Yes, research should also include recommendations and best-practices.</b></p>	
<p>Should telecom regulators be involved to insist on good practice in IXP peering resilience?</p>	

**Possibly, but one would have to assess the implications and the feasibility of such a proposal.**

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?

**The report seems to make a compelling case regarding practices by established players to erect barriers to entry for newer, smaller players.**

**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?

**This should be encouraged, but ultimately remains a matter for Member States.**

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?

**With the ever increasing number of websites, regulating content is a real challenge - very difficult and costly. One has to conduct a cost/benefit analysis before embarking on such a complex exercise.**

Would you envisage new EU regulation on any other issue?

**Cyber-space is both complex and continuously evolving. The EU should be always on the forefront and establish new ways on how the cyber-territory can grow whilst retaining innovation and creativity and yet be a safe place for our children.**

**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?

**We do not have the competence to respond on this issue.**

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?