

S₁ E₁ C₃ U₁ R₁ I₁ T₁ Y₄
E₁ C₃ O₁ N₁ O₁ M₃ I₁ C₃ S₁
A₁ N₁ D₂ T₁ H₄ E₁
I₁ N₁ T₁ E₁ R₁ N₁ A₁ L₁
M₃ A₁ R₁ K₅ E₁ T₁

Evaluation of Stakeholders' Replies to the Study on the overall subject matter of "Barriers and Incentives for Network and Information Security (NIS) in the Internal Market for e-Communication." commissioned by the European Network and Information Security Agency (ENISA) in 2007



Table of Contents

Introduction	3
Analysis of Received Responses	5
General Comments.....	5
Recommendation 1: Security Breach Notification	5
Recommendation 2: Electronic Crime Statistics	6
Recommendation 3: Bad Traffic Statistics	7
Recommendation 4: Removal of Compromised Machines.....	7
Recommendation 5: Secure Equipment by Default	8
Recommendation 6: Responsible Disclosure and Fast Patching	9
Recommendation 7: Security Patches	11
Recommendation 8: Electronic Payment Dispute Resolution	12
Recommendation 9: Sanction Abusive Online Marketers	13
Recommendation 10: Consumer Protection Law.....	13
Recommendation 11: Logical Market Diversity	14
Recommendation 12: Study IXP Failures	14
Recommendation 13: Ratification of Council of Europe Cybercrime Convention	15
Recommendation 14: EU-wide Co-operation on Cyber Crime	16
Open Question: Incentives for Lifting Barriers.....	17
Summary of Findings	17
Bibliography	18
ANNEX: LIST OF STAKEHOLDERS THAT REPLIED.....	18
About ENISA	19
Contact details.....	19
Legal notice	19

Introduction

As an input to its activities on economics of network and information security (NIS), ENISA in September 2007 commissioned a study identifying barriers and incentives for NIS. The overarching aim of the report is to analyse the economic impact of NIS, to assess added value and contribution to the smooth functioning of the Internal Market for e-communication.

In December 2007, ENISA held a consultation workshop in Brussels (Belgium) on the same subject matter. The half-day workshop aimed at launching a discussion among relevant stakeholders ensuring their input to the report tendered out by ENISA. It brought together representatives from all relevant stakeholder groups, i.e. EU and national decision-makers, industry and consumer representatives, academia and think tanks, as well as international organisations.

In February 2008, the final report entitled "*Security Economics and the Internal Market*" by Prof. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore was submitted to ENISA (Anderson, et al. 2008).

Based on the Report "*Security Economics and the Internal Market*" and its recommendations, ENISA invited stakeholders to comment on the report and its findings by means of a series of guiding questions on the Internal Market for e-Communication and incentives for removing remaining barriers to address NIS related issues as set out in an online questionnaire.

The Agency received responses from a wide range of sources on those questions that are of concern to them. The non-confidential stakeholder replies and comments on the report and its recommendations have been published on the ENISA website in June 2008. The results of the stakeholder replies can be summarised as follows:

73% of contributions received (cf. Figure 1) were sent by industry, i.e. by both international and European umbrella associations responding on behalf of their members as well as by individual companies. From EU Member States, both governmental departments and public authorities sent comments. Contributions from this group account for 27% of total replies received. No responses were received from other stakeholder groups such as consumer organisations and/ or academia.

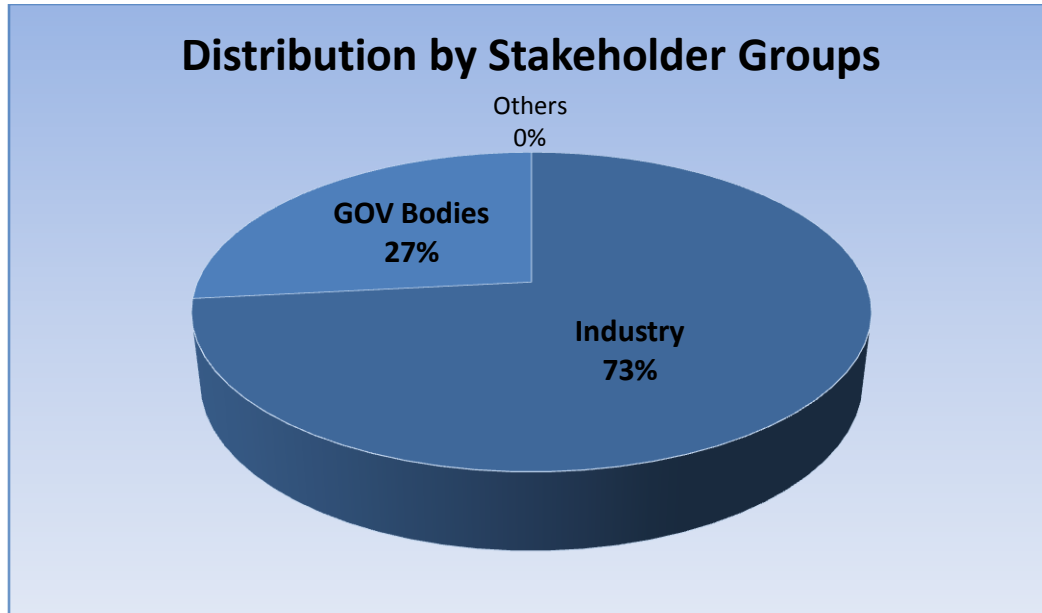


Figure 1: Distribution of Contributions received by Stakeholder Groups.

Responses were received from stakeholders originating from 8 EU Member States plus the USA. Category “Others” comprises international and European umbrella organisations.

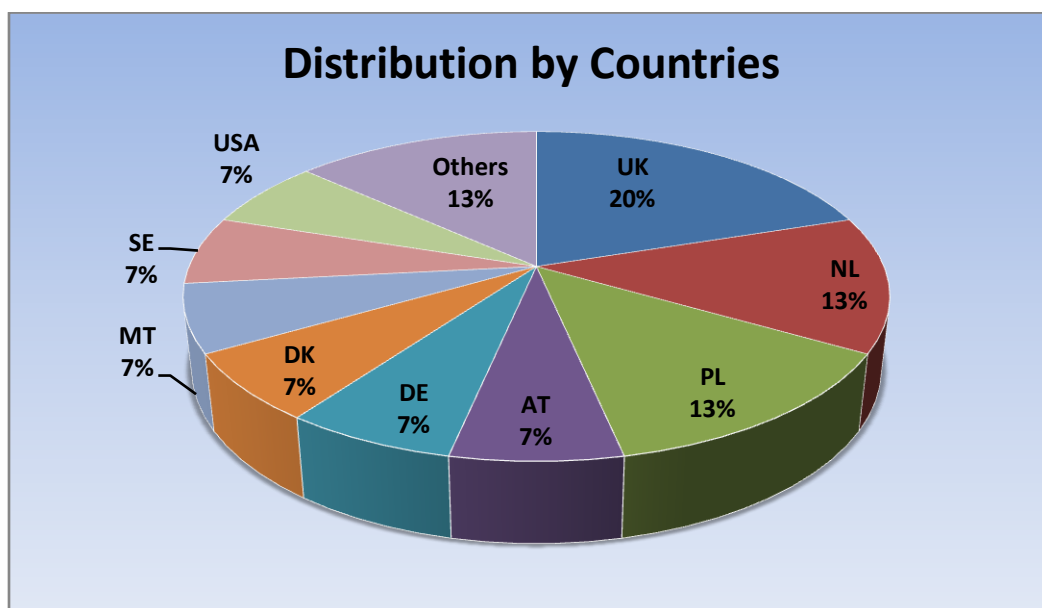


Figure 2: Distribution of Contributions received by Countries (EU and non-EU).

Analysis of Received Responses

General Comments

The report “Security Economics and the Internal Market” prepared by Prof. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore was generally well appreciated by government/ public authorities and industry stakeholders alike. Most respondents – notably industry representatives – welcomed the report as of excellent quality regarding analysis and incentives related to statistical measuring and metrics in particular. Many stakeholders endorsed the recommendations in principle whilst at the same time commenting in greater detail on those questions that are of concern to them.

Two industry stakeholder organisations – notably European IXPs and a SIG on product security vulnerabilities within major ICT companies – expressed concern about insufficient information on specific issues and hence non-comprehensive analysis of today’s business realities. Occasionally, respondents called for additional research to be undertaken in order to eliminate the perceived deficiency.

In addition to aforementioned general observations on the report, more specific and detailed comments on individual recommendations were received from all industry and government/ public authority representatives.

Recommendation 1: Security Breach Notification

The report states the point of security breach notification is to provide incentives for improving the protection of personal data without setting out in detail how data should be protected and hence imposing the burden of a strict liability regime across the whole economy.

A majority of stakeholders answered in the affirmative to the question regarding the need for a security-breach notification law in the EU. Some respondents, however, whilst generally supportive called upon decision-makers to be careful regarding the specific means to achieve the overall objective of enhanced transparency which such an initiative should bring about.

With few exceptions all respondents named self-regulation or a combination of self- and co-regulation the most appropriate and/or preferred policy instrument. Other “soft law” instruments (e.g. recommendations) were favoured by industry stakeholders whereas some Member State authorities opted for an “EU law”.

All respondents answering the question on the scope for such a security breach notification favoured a broad scope covering all service providers. Member State and public authority representatives advised

to include also government agencies, companies and non-profit organisations. Industry respondents would like to see all sectors covered but argued against a one-size-fits-all approach. Sector-specific mandates should be applied to (e.g.) telecom and ISP as well as the banking sector.

While no respondents denied the overall positive effect of the US – and in particular the Californian – privacy breach notification law for information security, most wanted to see further research carried out on both the actual impact achieved and other good practice examples from EU Member States. Concerns raised by stakeholders included the following issues: information on triggering event, entities covered, information covered, penalties and enforcement imposed.

Recommendation 2: Electronic Crime Statistics

As fraud statistics are already collected by police and/or other entities, the report recommends that regulatory action should aim at harmonisation of definitions, metrics and release cycles across EU Member States.

Many respondents indicated their support for the introduction of new EU regulation in order to ensure the publication of loss statistics for electronic crime as this would lead to an increase of transparency and rise of awareness among consumers. Nevertheless, a significant number of respondents expressed concern about imposing new regulation on ISPs and industry in general. Occasionally, respondents judged that a higher investment on technology and law enforcement resources would be more effective to battle cyber crime.

There was explicit consent on the question to include electronic crime statistics in the planned framework currently developed by 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”. Furthermore, it was suggested that an evaluation study should be conducted to establish whether current available sources of data would be sufficient.

As to mandatory reporting on particular indicators, respondents sounded a note of caution. Depending on both the nature of indicators and costs of compiling data a phased approach could be envisaged.

Member State and public authority comments agreed that all stakeholders (i.e. EU Members States, national regulators, industry associations and ISPs alike) should be encouraged to make electronic crime statistics available. No comments were received from industry on this particular question.

Recommendation 3: Bad Traffic Statistics

The report states that it would be in the public interest for quantitative data on ISPs' security performance to be available to the public. Furthermore, as for the information that should be published by and about Internet Service Providers (ISPs), this might include metrics such as number of spam messages sent from an ISP's customer, number of outgoing spam messages blocked by an ISP, number and source of incoming spam messages received by an ISP etc.

With regard to making quantitative data on ISPs' security performance available to the public, most respondents were very sceptical as to the benefits of such information to a general, non-expert community. Only if based on a homogenous model for data collection and interpretation, and if authentic and true such information would provide useful guidance to the wider public.

Explicit consent was received from all stakeholders replying to the question of whether ENISA should collect and publish data about the quantity of spam and other bad traffic emitted through European ISPs. Most respondents welcomed the increase of transparency provided by such an activity. By collecting data directly from the source burden on ISPs would be eased.

There is much diverse thinking on useful metrics to measure bad traffic. Comments range from proposals for specific metrics (e.g. volume of information in bytes rejected automatically and volume of traffic accepted) to the statement that the term "bad traffic" is to be defined first. Some industry stakeholders judged that whilst basic research should be done by both academia and industry, specific metrics should be defined by industry associations.

In addition, it was suggested that an evaluation of Information Sharing and Analysis Centres (ISACs) within the EU might be of value as it could disclose differences in implementation compared to US practice and in conclusion provide the basis for more effective information sharing approach in the EU.

Recommendation 4: Removal of Compromised Machines

Users may leave infected machines attached to the network, so that those machines can send spam, host phishing websites and distribute illegal content. According to the report the options available to fight the pollution of the digital environment are broadly similar to those with which governments fight environmental pollution (i.e. tax on "digital pollution", cap-and-trade system, fixed penalty scheme or private action). Rather than a heavyweight central scheme, the report suggests that civil liability might be tried first.

On the question of whether the EU should introduce a statutory scale of non-prompt response to requests about removing compromised machines all stakeholders unanimously agreed that it is important since a) it creates awareness, and b) adds a price to running a network.

Some respondents went even further to comment on the challenges and ways to implement such a scheme. All agreed that it is necessary to combine it with transparency measures, such as adding a “central portal” for publishing compliance and performance information. Stakeholders pointed out the importance of strong collaboration of providers with other stakeholders such as CERTs and hotlines that fight spam.

According to respondents, the major challenge regarding the implementation of this measure (removal of compromised machines) is that it needs a large scale (near) real-time monitoring which makes it costly. It was suggested that a cost-benefit analysis of societal added value versus implementation costs should be conducted prior to any enforcement. Outsourcing to specialised third party organisations was considered one means to reduce monitoring costs for compromised machines.

Respondents favoured an implementation scheme for this measure to include providers posting a bond (i.e. pre-paid fines) proportional to their size, from which fines could be deducted quickly. That way, long investigation or litigation processes would be sped up or even totally avoided.

Alternative means of dealing with compromised machines included a combination of statutory penalties with private bonding, third party detection and authentications, limit regulatory investigations and litigation only to extreme cases, traffic filtering, etc.

Recommendation 5: Secure Equipment by Default

Software liability is an important and at the same time highly sensitive issue due to the large and ever growing variety of goods and services in which software plays a critical role. The report favours a strategy whereby the European Commission should take a patient and staged approach. It is argued that other than stand-alone embedded products, which are subject to regulations on safety, product liability and consumer rights, networked systems can cause harm to others. The report suggests as a good starting point requiring vendors to certify that their products are secure by default. Furthermore, a “secure-by-default” practice should include requiring vendors to build in their products the capability for automated patching.

Responses received indicate that is a highly controversial matter especially for the software industry. Industry respondents pointed to stifling effects that a potential (re)allocation of liability may have, especially to open source and small vendors. They sent a very sound note of caution about the

potential complexities and side-effects that a shifting of liability might have as regards stifling innovation, increasing costs, decreasing competitiveness, etc.

Instead of shifting liability to vendors industry stakeholders suggested moving towards using best-practices on an on-going basis. In addition to “secure-by-default” these may include practices such as Secure Software Development Lifecycle, Security Capability Maturity Model, etc.

In general, public authority respondents had a more positive attitude agreeing that some form of liability is needed. They do share though some of the industry stakeholders’ concerns, especially regarding the impact on innovation power of smaller companies. In order to overcome some of the problems and achieve a wider commitment governmental respondents suggest to carefully study the potential impacts, to conduct a full evaluation, to follow an evolutionary process, and to negotiate/agree with the relevant stakeholders.

On the question regarding the development and enforcement of best practices for “secure-by-default” networked equipment, all respondents agreed that it is a laudable goal while at the same time pointing out some issues to be considered. It was felt that there is no one-solution-fits-all standard for secure-by-default since business users have different requirements; that research and education is needed on what constitutes a “secure-by-default” profile; that enforcing standards might be difficult and in some case undesirable, customer awareness might be a better option; and that standards need to be defined by industry and validated by third party auditors.

Positive reaction to self-certification was given only by governmental institutions, whereas some stakeholders suggested that quick and inexpensive testing might be a better option such as the CESG Claims Tested Mark (CCTM)¹ model in the UK.

Recommendation 6: Responsible Disclosure and Fast Patching

There has been some controversy about vulnerability disclosure and patching. Recent research has shown that the responsible disclosure approach gets better results than non-disclosure or open disclosure. However, some companies still take a long time to issue patches for vulnerabilities. The

¹ The CESG Claims Tested Mark (CCTM) scheme provides a government quality mark for the public and private sectors based on accredited independent testing, designed to prove the validity of security functionality claims made by vendors. In more colloquial terms, the CCTM is designed to assure public bodies that a product or service does ‘what it says on the box’. More information can be found at: <http://www.cctmark.gov.uk/>

report suggests that liability can be considered an incentive for cutting down on response time by companies.

Almost all respondents – with the exception of one industry association – agreed that a combination of early responsible vulnerability disclosure and vendor liability for not providing patches timely would increase transparency and therefore bring benefit to the quality of the security of software. Disclosure of vulnerabilities should be on a “*need to know*” basis. The regulation covering these two measures should be applicable only as last resort. They should be accompanied by regulatory support for third-party risk rating and other incentive instruments (i.e. insurance, contingent payments, bounties).

Those not in agreement with the recommendation call for responsible vulnerability disclosure to be reinvestigated to take into account the user’s operational model, i.e. defining it as disclosure from the vendor towards the customer (level of exposure and fix), rather than as it is defined now which is towards the vendor. Furthermore, they argue vendor liability for timely providing security patches is not feasible as the timeline for this process cannot be set in advance - not even defined within a framework - without affecting the quality of the security fix.

In general, respondents argue that responsible vulnerability disclosure can and should improve the partnership relations among stakeholders, including vendors, customers, and third parties, especially when it comes to sharing and analysing cyber risk information similar to what exists in the financial credit markets. However, some point that one should also look into whether this will also have a negative impact and tension between some groups of stakeholders. It is suggested that before proceeding with such solutions ways to avoid the negative impact and tension should be investigated.

Some respondents consider the main factor for delaying patching of vulnerable software is not the time it takes the vendor to produce the fix, but rather the time it takes the customer to apply it. The former tends to become shorter (close to absolute minimum needed) due to competition between vendors. The latter tends to be long since it is governed by users. Respondents conclude that automated patching and appropriate patch management methods would help a lot to speed up the process and thus to make information systems more secure.

Additional proposals for speeding up the time to secure the vulnerable systems include self-regulation, disclosure of other types of cyber risks, publication of threats and True Downtime Costs (TDC), as well as market forces. Stakeholders called for more research and innovation to be carried out in this field naming the work on incentive-based cyber trust (Thomas and Amon 2007) as a good starting point.

Recommendation 7: Security Patches

The report states that vendors also dissuade people from patching by bundling patches with upgrades and with disfeatures such as digital rights management (DRM). Therefore, it recommends that security patches be offered for free, and that patches be kept separate from feature updates. Furthermore, it argues that making end-users liable for infections caused by turning off automated patching or otherwise undermining the secure defaults provided by vendors might enhance the overall level of security. The report uses the following analogy: “It’s the car maker’s responsibility to provide seat belts, and the motorist’s responsibility to use them.”

Almost all respondents agreed that security patches only should be offered for free because it is the vendor’s responsibility to ensure that the security of their software/hardware products is not compromised as new vulnerabilities are discovered or new threats appear. A public authority representative suggested complementing such offering with a “central portal” that publishes *compliance* and *performance* information in order to improve transparency. One industry respondent argued that a clear quantitative definition of what constitutes a security vulnerability is lacking. With the current business model – it was stated – vendors do not release patches but issue new (improved) software versions. This model usually comprises a support contract with the customer to absorb the costs of new software releases.

All respondents – with the exception of one industry representative – agreed on the separation of security patches from new feature updates. Industry stated that at times such a separation might not be logistically or technically feasible, while producing free updates intrudes into some vendors’ business models. A business model might be that vendors sell their products at a very low price, or even give them away for free, but charge for continuous support. In such a model the separation proposed by the report would not be clear cut according to the respondent.

The issue of end-users being held liable for infections in case they turn off automated patching or security defaults is controversial. Some replies, mainly coming from the public sector, agreed that this would be an acceptable measure only if (1) it can be proven that the user intentionally turned the auto-security mechanisms off and (2) it is coupled with extensive awareness to educate users in order to avoid unintentional mistakes (analogy is given with driving licence).

On the other hand some, mainly industry responders reasoned that such liability may not be desirable since there are many users, especially business users, who intentionally turn off automated patching in order to verify, select and approve patches ensuring in this way robustness and minimum disruption of their information systems.

One public body pointed to the trend that exploits appearing after patches are out more and more rapidly. This shifts the risk of instability from the risk of instability due to bad quality patch towards the risk of instability due to exploitation. The respondent suggested fast patching unless there are serious suspicions about the instability brought in by the security patch. The latter could be minimised as long as there are incentives for vendors to follow best practices even when developing patches.

As an alternative or even complementary measure to end-user liability one respondent suggested to use other incentive instruments. According to the reply received, end-customers and end-users need real-time feedback on their cyber risk, how that cyber risk will increase or decrease based on actions (e.g. turning off automated patches), and subsequently how that change in risk will affect costs. This is considered much more flexible, adaptable, and compelling than the rather harsh penalty instrument of legal liability.

Recommendation 8: Electronic Payment Dispute Resolution

The handling of questions concerning liability for fraud, security failures and dispute resolution procedures varies significantly across EU Member States. Hence, the report concludes that the European Union should address the issue by harmonising procedures for the resolution of disputes between customers and payment service providers over electronic transactions.

A majority of respondents agreed that the EU should harmonise procedures for the resolution of disputes between customers and payment service providers over electronic transactions. Few comments advocated effective dispute resolution procedures but advised against harmonisation. Alternative proposals included a “central portal” for publishing performance/ compliance information.

With one exception, no respondent expressed an opinion on amending the Payment Services Directive by tackling the issue of varying fraud liability and dispute resolution procedures among EU Member States.

Comments on other, more appropriate legal instruments to address this problem must be considered inconclusive. While industry representatives referred to legislation and regulation to require reporting on fraud cases, consumer complaints, and disputes (frequency, payment/ settlement), public authority representatives referred to self-regulation as sufficiently effective.

Recommendation 9: Sanction Abusive Online Marketers

Directive 2002/58/EC concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (ePrivacy Directive) prohibits sending any unsolicited messages to individuals, requiring their prior consent but leaves it up to EU Member States to decide on whether to allow unsolicited communications to business. According to the report, the business exemption undermines the protection for consumers and hence should be abandoned.

All respondents agreed unanimously that the European Commission should take action by preparing a proposal for a directive establishing a coherent regime of proportionate and effective sanctions against abusive online marketers.

Likewise, all respondents accepted the recommendation for the existing Directive on Privacy and Electronic Communications (2002/58/EC) to be revised in the light of abandoning the business exemption for spam or “malicious activity” as one respondent put it.

In addition, some public authority comments related to using advanced technologies (such as database systems) for collecting and analysing spam for penalise spam campaign originators, and to extending base-line rules beyond the European Union in order to be truly effective.

Recommendation 10: Consumer Protection Law

Although consumer protection legislation is technologically neutral, extensive development of new information and communication technologies (ICT) necessitates specific guidance on how to apply the protection principles in practice. Technology enables information to circulate rapidly around the world and at the same time enables better protection of consumers where required. The report calls for further research to be conducted to study what changes are needed to consumer protection legislation as commerce moves online.

Whilst many industry representatives did not respond to this recommendation and related guiding questions, the majority of those who did were unanimous in seeking the European Commission/ ENISA to conduct research to study what changes are needed to consumer protection law as commerce moves online.

Furthermore, respondents felt ENISA should consider becoming involved in the wider European Commission policy process, considering security aspects of policy along with consumer protection questions. Respondents pointed to ENISA’s role as providing studies and information to EU Member States rather than concerning itself directly with consumer protection issues.

There was no strong support by respondents for the European Commission to address the issue of right to Internet connectivity. Some comments pointed to laws already in force such as equal employment, avoidance of discrimination, free speech etc.

Recommendation 11: Logical Market Diversity

The report argues that market forces have helped to mitigate the lack of diversity of products and that regulators need to be aware of security threats that follow from lack of diversity. In conclusion, the report recommends that ENISA should advise competition authorities providing technical expertise on issues at stake.

All stakeholders commenting on logical market diversity advised against ENISA seeking to advise Competition Authorities whenever diversity has security implications. Some comments suggested ENISA might use its social networks and contacts to advise EU Member States on how to improve prospects for market diversity.

Whilst acknowledging the lack of diversity and potential effects on consumer choices, a vast majority of respondents was opposed to ENISA taking an active role in providing expertise to decision-makers with regard to security threats that follow from a lack of market diversity.

Many respondents – mainly government and public authorities – judged that ENISA should 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.

Recommendation 12: Study IXP Failures

As for critical national infrastructure, one particular problem according to the report is the lack of appropriate incentives to provide resilience in competitive network markets. The report recommends that ENISA should sponsor research to better understand the effects of Internet Exchange Point (IXP) failures. Moreover, ENISA should work with telecommunication regulators to insist on best practice in IXP peering resilience.

This recommendation was commented on by seven IXPs and one IXP association. There was no feedback from other related stakeholders such as Internet Service Providers (ISPs), telecommunication services operators or regulators.

All respondents unanimously stated that no further regulation is needed in order to increase the resilience of IXPs. It is argued that there has not been any proper cost-benefit analysis to support the contention that regulatory intervention would produce superior outcomes compared to the current situation. Thus, the level implication to network resilience is without an appropriate foundation. On the contrary, it is argued that market forces must be considered the best way to determine the appropriate level in security and resilience, particularly when it comes to IXPs. Also, IXP customers already interconnect in multiple locations including private peering which increases resilience. According to respondents, the latter is a fact which the report is not clear enough on.

Even though respondents argued (cf. above) that there is not enough knowledge and study of the implications and cost-benefit of regulatory incentives to increase the investment of IXPs and hence their resilience, all were opposed to ENISA enhancing their engagement in research to better understand the effects of IXP failures. Respondents claim that National Regulatory Authorities (NRAs) already have measures in place which are effective and take local peculiarities in mind. Furthermore, best practices are shared openly between European IXPs since there is already a forum (i.e. the umbrella association Euro-IX) to discuss and resolve all issues.

All respondents disagreed with the report's conclusion regarding national monopolisation of the IXP market, and judged the "winner-takes-it-all" as inaccurate. While all agreed that small IXPs are important in order to provide diversity for small network operators within a local market, it was argued that additional regulation may put some unnecessary burden to these small IXPs. This may disproportionately increase their costs and lead to reduced competition.

IXP respondents pointed to a distinction to be made in relation to the Access and Interconnection Directive (EU Directive 2002/58/EC 2002). Using IXPs is not the only way that network providers are interconnecting. They decide how and when to peer, for example in different countries, using private peering, establishing transit agreements, etc. Therefore respondents considered the report's assumption about the role of IXPs in peering and resilience misleading. According to respondents, network providers are the decision makers when it comes to where and with whom to peer, i.e. regarding decisions on redundancy and resilience of their interconnections whereas IXPs are involved only in the internal redundancy of the peering network.

Recommendation 13: Ratification of Council of Europe Cybercrime Convention

According to the report, the cross-jurisdictional nature of cyberspace requires the harmonisation of national law within a consistent international framework. The 2001 Council of Europe Convention on

Cybercrime provides such a framework. The report calls for the harmonisation process within this framework to be speeded up if it is to bear fruits and fragmentation of legislation is to be overcome.

All respondents to the guiding questions supported continued political pressure by the European Commission on those EU Member States that have yet to ratify the Council of Europe Convention on Cybercrime.

In following up on the European Commission Communication on Cyber Crime, government bodies and public authorities commenting would also envisage new regulation including mandatory blocking of websites with particular content and controls on search engines whilst advocating cost/benefit analysis before launching any proposal. No industry comments were received on this recommendation and related guiding questions.

Ask about new EU regulation/ initiatives on any other issue, government bodies and public authorities mentioned *inter alia* the following: roadmap for ICT security development including a step-by-step guide on developing a higher level of security in electronic markets; educational programme regarding threats in IT systems starting as early as primary school age; and strategic forward thinking on future growth of the cyber territory whilst simultaneously retaining innovation, creativity, and child safety.

Recommendation 14: EU-wide Co-operation on Cyber Crime

The report states that the fragmentation of law enforcement combined with the international nature of cyber-crime makes successful joint operations across jurisdictions cumbersome and expensive. Furthermore, it argues that NATO as a model is one option for cyber-security co-operation.

Most respondents did not see any added value in charging an EU-wide body with facilitating international co-operation on cyber crime, using e.g. Europol and/or NATO as a model. Comments provided by both industry and public authority representatives recommended advanced (academic and industry) research and prototyping on how best to address the issue. Some identified the need to define “co-operation interfaces”, rules and procedures, among organisations currently charged with network and information security, cyber crime, terrorism etc.

Moreover, respondents mentioned global CSIRT co-operation and Basel II financial risk management standards and methods as other good practice examples of cross-jurisdictional co-operation models in the international framework.

Open Question: Incentives for Lifting Barriers

Some respondents reiterate their call for a co-ordinated action plan bringing together all stakeholders in e-communication including software and hardware vendors, telecom operators and electronic service providers, consumer organisations, home users, research and development experts, independent ICT security experts as well as international organisations, national governments and law enforcement agencies. It was argued, they all should join forces to raise the overall level of network and information security by addressing issues such as enhanced co-operation and co-ordination among all stakeholders; exchange of information on threats, vulnerabilities, and security incidents; methodology for developing secure architectures and protocols; security standards; product liability and security; target group specific education and awareness programmes etc.

Summary of Findings

ENISA received responses from a wide range of sources, both verifying and falsifying recommendations given by the report "*Security Economics and the Internal Market*". Feedback was sought from all ENISA stakeholder groups and all those interested in economics of network and information security. Regrettably, consumer representatives did not provide written comments.

In general, comments received and arguments expressed followed traditional stakeholder cleavage lines. With few exceptions on selective issues, industry respondents named self-regulation or a combination of self- and co-regulation the most appropriate and/or preferred policy instrument whereas public authorities often opted for stronger instruments such as an "EU law" considering "soft law" as not sufficiently effective. With regard to the more complex and at times sensitive issues stakeholders called upon decisions-makers in general and ENISA in particular to carry out and/or commission further research into the various aspects at stake prior to any follow-up activities or initiatives.

In a follow-up document, ENISA will now draw conclusions based on the report "*Security Economics and the Internal Market*" by Prof. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore, on replies received by stakeholders commenting on the report and its recommendations, and on the evaluation of the latter.

In deciding on potential follow-up activities and perhaps initiatives, ENISA might be able to single out some issues/recommendations which were identified by stakeholders as "important" and/or "desirable" to be addressed at EU level in order to remove still existing barriers and to further specify incentives for network and information security.

Consultation of and input by all ENISA stakeholder groups has been – and will continue to be – of utmost importance throughout the whole process.

Bibliography

Anderson, Ross, Rainer Boehme, Richard Clayton, and Tyler Moore. *Security Economics and the Internal Market*. ENISA, 2008.

Directive 2002/58/EC. *Directive 2002/58/EC of the European Parliament and of the Council of 7 March 2002 on Access to and Interconnection of Electronic Communication Networks and Associated Facilities*. Access Directive, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:HTML>: European Union, 2002.

Thomas, Russell C., and Patrick D. Amon. *Incentive-based Cyber Trust – A Call to Action*. White Paper, <http://meritology.com/resources/>, Meritology, 2007.

ANNEX: LIST OF STAKEHOLDERS THAT REPLIED

Amsterdam Internet Exchange (amsix)
German Internet Exchange (DE-CIX)
European Association for the Operators of Internet Exchange Points (EURO-IX)
FIRST Vendor SIG
London Access Point (LONAP)
London Internet Exchange (LINIX)
Logica Danmark
Malta Communications Authority
Meritology
Polish Ministry of Foreign Affairs
NASK
GOVCERT Netherlands
Netnod Internet Exchange
Vizuri Ltd
Vienna Internet eXchange

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For general enquiries on Economics of NIS, the study “Security Economics and the Internal Market” and evaluation of stakeholder replies in particular, please use the following details:

Mathea FAMMELS – Expert Relations with Industry, International Organisations and Third Countries —

Email: mathea.fammels@enisa.europa.eu

Internet: <http://www.enisa.europa.eu/>

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2008



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu