

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

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



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.

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, both verifying and falsifying recommendations given by the report "*Security Economics and the Internal Market*". The non-confidential stakeholder replies and comments on the report and its recommendations have been published on the [ENISA website](#) in June 2008.

With regard to the more complex and at times sensitive issues stakeholders called upon decision-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.

ENISA Conclusions on Follow-up Activities

ENISA is drawing 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 was 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.

1. Security Breach Notification: Report Findings, Recommendation, Stakeholders' Comments

The report states the point of security breach notification is to provide incentives for improving the protection of personal data and availability of provided services without setting out in detail how data should be protected nor how service availability could be enhanced and hence imposing the burden of a strict liability regime across the whole economy.

According to the report as well as ENISA's Multi-annual Thematic Programme (MTP) 1 stock taking on the resilience of public eCommunications networks, it is important that security breach notifications be as effective an incentive as possible, and lessons can be learnt from the US regarding this. In particular, US experience demonstrates the disadvantages of a patchwork of local laws. In particular some of the US state laws permit companies to assess the risk and they need not issue a notification if they believe there is 'no risk'. Some of the state laws require that their citizens be notified 'first' which is difficult for companies with a national presence. The variation between the laws has led to calls for a federal statute. Hence, the report recommends a security breach notification law to be brought forward at EU level, covering all sectors of economic activity.

Security breach notification legislation has been put forward as a part of the 2007 review of the framework for electronic communications networks and services. According to the European Commission proposal, this would require notification to be made where a network security breach was responsible for the disclosure of personal data. According to the commissioned study "Security Economics and the Internal Market" this is a very narrow definition as it is being put forward specifically for one sector and will only deal with a small fraction of the cases that a California-style law would cover. Actually, security breach notifications should cover confidentiality and integrity of data (related to data privacy) as well as availability of services (availability).

Moreover, the reports recommends as well as informing the data subjects of a security breach, a central clearing house should be informed as well. Legislation should set out minimum standards of clarity for notifications. Finally, notifications should include clear advice on what individuals and companies should do to mitigate the risks they run as a result of the disclosure; in the US many notifications have just puzzled their recipients rather than giving them helpful advice.

Replying to the invitation for comments, 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. Concerns raised by stakeholders included the following issues: information on triggering event, entities covered, information covered, penalties and enforcement imposed.

ENISA reckons security breach notification, applied consistently across the European Union, would reveal the scope of information security problems. Recent security breach incidents have already heightened awareness of the importance of protecting and the need to respond effectively to a breach that poses privacy risks.

In drawing conclusions based on the report and on replies received by stakeholders commenting on its recommendations, ENISA decided to further look into the issue of security breach notification. As relevant legislation on privacy is currently under review – whereas data protection might be reviewed and amended in the forthcoming two years – ENISA allocated a subordinate priority to follow-up activities to the issue. ENISA plans to take the issue forward in the second half of 2009. By means of (e.g.) setting up an ad hoc Working Group comprising experts in the area of information security, e-privacy, data protection NRAs, and resilience NRAs including representatives from industry and consumer organisations as well academia.

In line with its scope of activities and tasks, ENISA aims at best practices for implementing security breach notification provisions. To address the objective, looking at and taking into consideration existing legislation covering privacy and data protection as well as strategies and policies on the availability and resilience of networks should be regarded. Finally, ENISA’s stock taking on the resilience of public eCommunications networks revealed a number of policies deployed at national level aiming at enhancing the availability and resilience of public networks.

2. Secure Software Engineering: Report Findings, Recommendation, Stakeholders’ Comments

ENISA acknowledges the importance of the overall issue of secure software engineering under which the report findings and stakeholders’ comments on the following recommendations can be subsumed:

“Secure Equipment by Default” (Recommendation 5), Responsible Vulnerability Disclosure and Fast Patching (Recommendation 6), and Security Patches (Recommendation 7).

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 “Security Economics and the Internal Market” by Prof. Ross Anderson et al. 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.

Replying to the invitation for comments, industry stakeholders 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, and decreasing competitiveness. Public authority respondents shared industry stakeholders’ concerns with regard to the impact on innovation power of smaller companies. Instead of shifting liability to vendors it was suggested moving towards using best-practices on an ongoing basis. In addition to “secure-by-default” these may include practices such as Secure Software Development Lifecycle, Security Capability Maturity Model, etc.

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.

According to recent research 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 report “Security Economics and the Internal Market” suggests that liability can be considered an incentive for cutting down on response time by companies.

Almost all stakeholders commenting on the recommendations 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. It was argued that disclosure of vulnerabilities should be on a “*need to know*” basis. Some stakeholders called 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.

With regard to security patches the report “Security Economics and the Internal Market” states that vendors dissuade people from patching by bundling patches with upgrades and with disfeatures such as digital rights management (DRM). Therefore, the recommendation is that security patches be offered for free, and that patches be kept separate from feature updates. It is argued 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.

Almost all stakeholders commenting on this recommendation agreed that security patches indeed should be offered for free because – it was argued – 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. In this context, the idea of a “central portal” that publishes *compliance* and *performance* information in order to improve transparency was mentioned.

Equally high agreement was obtained on the issue of separating security patches from new feature updates. However, individual business models might interfere with this requirement as some vendors sell their products at a very low price, or even give them away for free, but charge for continuous support. With the current prevailing 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.

The issue of end-users being held liable for infections in case they turn off automated patching or security defaults was controversial. Most notably, industry stakeholders reasoned that such liability may not be desirable since many end-users, especially business users, intentionally turn off automated patching in order to verify, select and approve patches, and hence to ensure robustness and minimum disruption of their information systems. A question that might arise in this context is how to ensure robustness and minimum disruption of information systems without turning of automated patching? Or more generally, what are alternative or complementary incentive instruments to end-user liability?

In drawing conclusions based on the report and on replies received by stakeholders commenting on its recommendations, ENISA decided to further look into the issue of secure software engineering. In order to overcome some of the identified problems and to achieve a wider commitment by all stakeholders it was suggested to carefully study potential impacts of recommendations, to conduct an evaluation of alternative solutions, to follow an evolutionary process, and to involve relevant stakeholder groups.

In the area of security economics, follow-up activities on the issue of secure software engineering will be a priority in 2009. ENISA plans to take the issue forward in the first half of 2009 by means of setting up a Virtual Working Group comprising experts in the area of secure software engineering, looking at the broad spectrum from requirements to software disposal. The group is expected to include

representatives from industry and consumer organisations as well decision-makers and academia. In line with its scope of activities and tasks, ENISA aims at recommendations for different actors, such as vendors, users/consumers, policy makers, security researchers and educators, to address the objective, looking at and taking into consideration their different roles and needs.

Terms of Reference (ToR) for the future Virtual Working Group (VWG) on Secure Software Engineering will have to be agreed upon by participating experts. However, the following issues and questions derived from the report and stakeholders' comments might be addressed by the VWG:

- What are alternatives to self-certification? What are quick and inexpensive testing methods?
- What would be methods to minimise the complexity and side-effects regarding innovation, increasing costs, decreasing competitiveness, etc.
- Would automated patching and appropriate patch management methods help to make information systems more secure by cutting down on / eliminating customer-apply-time?
- Would self-regulation, disclosure of other types of cyber risks, publication of threats and True Downtime Costs (TDC), and/or market forces make vulnerable systems more secure?
- Would incentive-based cyber trust be a good starting point?
- What are incentives for vendors to follow best practices when developing patches?
- How would it be technically and logistically viable to integrate security and patching with current vendors' business models?
- How can negative impact and tension between different groups of stakeholders be avoided?
- Which are the right messages and means towards extensive awareness to educate users in order to avoid unintentional mistakes?

Outlook

ENISA aims at 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. In providing a platform, ENISA will join forces with external experts 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.

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

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”, evaluation of stakeholder replies and planned follow-up activities, 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