



EUROPEAN COMMISSION
Information Society and Media Directorate-General
Audiovisual, Media, Internet
Internet; Network and Information Security

REPORT

WORKSHOP ON

**THE EU POLICY DIMENSION OF VULNERABILITY MANAGEMENT
AND DISCLOSURE PROCESS**

31 March 2009

DISCLAIMER

**This report does not necessarily
represent the views of the Commission**

1. MAIN OUTCOMES OF THE WORKSHOP	2
2. CONTEXT	3
3. REPORT ON THE SESSIONS.....	5
3.1. Setting the scene.....	5
3.2. Exchange of experiences and lessons learnt	6
3.3. Open discussion on vulnerability management and disclosure in the EU	8
4. CONCLUSION	11

1. MAIN OUTCOMES OF THE WORKSHOP

Vulnerability management involves complex processes and comes along with technological and political challenges. The stakeholders include vulnerability finders, product vendors, governments, corporate customers and private end users.

Lessons learnt: the sharing of vulnerability information requires mutual trust

Currently, there is a lack of trust between stakeholders that severely hinders the sharing of vulnerability information. A **high level of trust is even more required** for the sharing of information on vulnerabilities affecting Critical Information Infrastructure (CII).

Lessons learnt: Coordination is needed

Some degree of **coordination between the stakeholders** is needed in particular to manage the most complex vulnerabilities. Additionally, **trusted national points of contact would be desirable** to disseminate early warning information to local vendors and (CII) operators and to support the various stakeholders in particular with regards to the assessment of national impacts. National/governmental Computer Emergency Response Teams (CERTs) could serve as such national points of contact and as trusted intermediaries facilitating the cooperation between stakeholders.

Lessons learnt: Coordination requires a lot of resources

The role of the coordinator in the vulnerability management and disclosure process **requires comprehensive resources**. Currently many national/governmental CERTs are considered as under-funded and understaffed, severely limiting response capabilities.

Lessons learnt: Raising awareness

There is a need to **raise the maturity level** of the vulnerability scene, to share good practices and raise awareness, in particular, among the EU industry stakeholders. The question of incentives versus liabilities should be carefully assessed.

Lessons learnt: Invest in more research

There would be the need to **invest in research** to complement the huge effort undergone in the U.S. such as via the National Vulnerability Database¹ sponsored by DHS National Cybersecurity Division / US-CERT. Research on testing methodologies, securing complex systems and secure programming would also help reduce or cope with vulnerabilities.

Lessons learnt: The way forward

Strict and inflexible policies would not help to deal with changing complex risks. The establishment of a strong and trusted **European Public Private Partnership for Resilience (EP3R)** to support the exchange of information and knowledge could be the vehicle for going forward. It could favour an enhanced cooperation and coordination between EU stakeholders with regards vulnerability management.

The specific issues of legal framework, information sharing of sensitive information and economic incentives could be further analysed under this framework. In addition, the **baseline of capabilities and services for national/governmental CERTs** (to be developed in coordination with the European Network and Information Security Agency - ENISA) to foster pan-European cooperation between CERTs could possibly include aspects related to vulnerability management and coordination.

¹ See <http://nvd.nist.gov/>

2. CONTEXT

The European Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP) on 30 March 2009² with the following objectives:

- To foster cooperation, exchange of information and transfer of good policy practices between Member States via the newly-established **European Forum**.
- To develop a **public-private partnership** at the European level to support sharing of information and dissemination of good practices between public and private stakeholders with the aim of ensuring the resilience of CII.
- To enhance **incident response capabilities** in the EU by increasing national capacities, possibly built on national or governmental Computer Emergency Response Teams/Computer Security Incidents Response Teams (CERTs/CSIRTs) as well as by encouraging and supporting the European cooperation between these entities with a view to facilitate the exchange of information, technical measures and good practices.
- To promote the organisation of **national and European exercises for contingency planning and disaster recovery** on simulated large-scale network security incidents.
- To reinforce **international cooperation** on global issues, in particular on resilience and stability of the Internet.

The initiative on CIIP specifically proposes to establish a strong and trusted **European Public Private Partnership for Resilience (EP3R)** to support the exchange of information and knowledge between public and private stakeholders on specific topics with an EU and international dimension. The setting-up of the EP3R would follow a step-by-step approach so that, on the one hand, stakeholders would discuss and design the necessary building blocks that would best match their requirements and, on the other hand, the work on the key challenges that require this kind of approach could immediately start. The workshop on the EU policy dimension of vulnerability management and disclosure process was organised in that context.

The workshop aimed to explore the policy dimension of vulnerability management, in particular the aspects of risks assessment and responsible vulnerability disclosure. To this end, the workshop fostered the exchanges and discussions on 1) experiences regarding vulnerability management and disclosure approaches as well as lessons learnt; 2) the importance of responsible vulnerability disclosure and the challenges coordinators (e.g. CERTs) face 3) the prerequisites for an effective sharing of vulnerability information and 4) industry practices for vulnerability management.

The workshop brought together around 70 participants from Member States bodies, academia, industry and European institutions. There were 25 delegates from national public bodies of 14 Member States plus Norway. They represented ministries of interior affairs,

² See Commission communication on Critical Information Infrastructure Protection, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM (2009)149 of 30.3.2009 at http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

transport and telecommunications, national/governmental CERTs and National Regulatory Authorities.

The workshop followed the subsequent structure:

- (1) A first session on **setting the scene**. This session is reported in chapter 3.1;
- (2) A track dedicated to **exchanges of experience and lessons learnt** with regard to vulnerability management and disclosure. This session is reported in chapter 3.2;
- (3) A session for **open discussion on vulnerability management and disclosure in the EU**. This session focused on the issues of risk assessment, coordination of vulnerability disclosures and deployment of solutions. It is reported in chapter 3.3;
- (4) A final session on **the way forward** summarised the outcomes of the workshop. This session is reported in chapter 1 which records the main outcomes of the workshop.

3. REPORT ON THE SESSIONS

This chapter presents the views expressed by the participants in the sessions on setting the scene, exchanges of experience and lessons learnt, as well as in the open discussion on vulnerability management and disclosure in the EU.

3.1. Setting the scene

This session provided an overview of the recent developments in the area of Critical Information Infrastructure Protection (CIIP) and the state of play on vulnerability disclosure.

The very day before the workshop, the Commission adopted a policy initiative on Critical Information Infrastructure Protection (CIIP)³. This initiative proposes a number of concrete actions, structured in five pillars: (1) preparedness and prevention, (2) detection and response, (3) mitigation and recovery, (4) international cooperation and (5) development of the ICT sector specific criteria to identify and designate the European Critical Information Infrastructures.

Within the context of vulnerability disclosure and management the following proposed actions are of special significance:

- Establishment of a European Public Private Partnership for Resilience (EP3R);
- Development of a baseline of capabilities and services for national/governmental CERTs to foster pan-European cooperation.

Discussing the state of play on vulnerability disclosure, one of the speakers identified numerous problems. Most vulnerabilities can be traced to a lack of awareness, poor implementation quality or the growth of complexity. Vulnerabilities are not simple to eradicate. Due to the diversity of software engineering paradigms, programming languages, software libraries and other factors, there is rarely one simple way to fix any given vulnerability. Software vulnerabilities will remain for the foreseeable future. While we would need to understand how to change the way to design software to reduce vulnerabilities, it was recognised that changing behaviour would take time. It was suggested that raising awareness, positive incentives and liabilities should be considered as the "low hanging fruit".

Vulnerability disclosure is an issue involving many stakeholders: vendors (the recipients of vulnerability information), finders (the providers of vulnerability information) and coordinators. It was highlighted, that vulnerability disclosure is not just a technical problem but also involves politics (e.g. when it concerns national security) and complex processes.

The USA National Infrastructure Advisory Council's (NIAC) Vulnerability Disclosure Framework of 2004⁴ was referred to in a written statement as one example of an existing

³ See Commission communication on Critical Information Infrastructure Protection, "*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*", COM (2009)149 of 30.3.2009.

⁴ See *Vulnerability disclosure framework final report and recommendations*, United States Department of Homeland Security's National Infrastructure Advisory Council. (Government report). January 13, 2004. <http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf>

analysis which attempts to define roles and responsibilities of stakeholders in vulnerability disclosure and management and provide recommendations to enhance the management of software vulnerabilities.

3.2. Exchange of experiences and lessons learnt

In this session representatives from national/governmental CERTs and from private sector stakeholders exchanged their experiences regarding vulnerability management and disclosure processes. A representative from a national CERT noted that, ideally, we would not need any coordinators. But practically, the complexity of some vulnerabilities and the lack of trust between vendors and finders necessitates some degree of coordination. It was considered that if coordinators are needed then the less are involved in any given project the better.

A slightly different view was that, at governmental level, security organisations (like national/governmental CERTs) have the responsibility to build a trusted information society. Therefore, they need to know the details of vulnerabilities. Thus, controlled disclosure is preferred in order to increase network security by, in particular, providing the most relevant details to security regulation bodies and operators of CII.

The decision for a public authority to engage in coordination activities depends on whether the country's interests are at stake, whether enough resources can be prioritized for a given project and whether the coordinator would indeed add value. The different phases of a vulnerability coordination project were depicted: discovery of a vulnerability, vulnerability verification, assessment of its impact (in particular on Critical Infrastructures), initiation of the coordination, remediation/mitigation (including approaching affected vendors, signing non disclosure agreements, disclosing material, supporting vendors, developing mitigation guides and handling public relations), disseminating early-warning information and general disclosure which includes releasing final fix and advisory.

A speaker noted that a vulnerability management policy should include clarity on what the coordinator is doing as well as on confidentiality rules and disclosure policy.

It was noted that in the case of multi-vendor coordination, a challenging aspect is that the levels of awareness and disclosure strategies vary from one vendor to the other. Another important factor to be considered is the logistic of mass deployments. The example given was related to mobile telephony whereas embedded software is not always easy to update. Eventually, it was mentioned that some industries that depend on ICTs (like those depending on Supervisory Control And Data Acquisition - SCADA - systems) are not necessarily well prepared to cope with ICTs vulnerabilities or even prepared to change their management culture – which refrains from changing a running system – to adapt themselves to the challenges brought about their dependence on ICTs.

Two speakers identified patch management as the first line of defence against vulnerabilities. In particular, the spread of Conficker demonstrated how many Internet-connected systems are not patched in a timely fashion.

A representative from the private sector described the complex and resource-intensive vulnerability management and disclosure process from a vendor's perspective. The use of standards (e.g. CVSS, CVE and the proposed ISO/IEC 29147), established customer-vendor contacts and personal trust relationships with CERTs were identified as critical success factors.

One speaker reported on the current status of the proposed standard ISO 29147 “Responsible Vulnerability Disclosure”. This standard would be applicable to all manufacturers (software, hardware, cars, trains, etc). The focus of the standard would be on the finder-vendor and vendor-user relationships, not covering CERT-vendor relationships. Vendors' internal processes and procedures are also out of the scope. The standard's status is currently in the 2nd Working Draft. The final draft might be ready for voting in one year and half to 2 years and half.

The following issues were identified by one or more speakers as major challenges:

- *Resources:* It was stressed that the task of coordination requires many resources. One national CERT currently employs only two part-time vulnerability coordinators. This limits the CERT's capacity to one big case per year. Another national CERT reported to have a team of five full-time vulnerability coordinators employed.
- *Trust:* The issue of trust (and the lack thereof) was identified as critical to responsible vulnerability disclosure. Trust is an important prerequisite for the exchange of confidential vulnerability information. Finders sometimes pursue political or financial goals, increasing the tendency of vendors to mistrust finders. Also, the dissemination of early warning information among a close circle of stakeholders implies a certain level of secrecy which requires high levels of trust that are hard to establish. Establishing national processes for an exchange of sensitive information and developing an adequate level of trust among the partners is tedious and complex. The EU challenge in this connection lies within establishing or, respectively, strengthening and supporting national competences.
- *Adding value:* The coordinator should add value by providing services not available elsewhere. For instance, by providing advice regarding policy or process, supplying contacts, offering mediation or specific programme (e.g. SCADA Vendor Engagement Programme). It should not replicate what others are doing.
- *Partnerships:* Information and experience sharing should be facilitated so that partners can benefit of each other lessons learnt. A speaker presented a national Information Exchange platform that is used to exchange (sensitive) information on vulnerabilities.
- *Pan-European and international cooperation with regard to the protection of Critical Information Infrastructure:* Global cooperation is needed because countries are facing similar issues in particular due to the fact that the architecture of information systems and the software used are often the same. The cooperation with CERTs and vendors in other Member States has become a necessity. Unfortunately, it is sometimes difficult to identify trustworthy national points of contact. One speaker identified the Vendor Special Interest Group – Vendor SIG⁵ of the Forum of Incident Response and Security Team (FIRST) as an important private-sector initiative that provides a global forum for Internet infrastructure vendors. There are currently 29 participating vendors.
- *Encouraging patch deployment:* Currently, the "fix-it-later" approach is still prevalent in the private as well as in the public sector. Changing this attitude constitutes a major challenge for CERTs as well as for vendors.

⁵ See <http://www.first.org/vendor-sig/>

A representative from the private sector identified the current legal framework as a major obstacle for security research. It was noted that in some Member States reverse engineering or the dissemination of vulnerability information could constitute a criminal act. This severely hinders security research. This call for the creation of a sustainable environment that would protect and encourage security research, facilitate responsible reporting (e.g. protecting whistleblowers and not criminalising responsible reporting), prepare (e.g. create networks before they are needed and prepare international response procedures), decentralise preparations while centralizing response and promote EU-wide enforcement of law.

Furthermore, a participant suggested that the European Commission could propose near-real time translation of warning and alert information from and to all EU languages as a mean to encourage the exchange of vulnerability information.

Finally, all speakers addressed the issue of software quality. Most of the speakers agreed that clear economic incentives would be needed to encourage investments in more secure software. It was also noted that customers often do not demand or are not willing to pay for more secure software.

3.3. Open discussion on vulnerability management and disclosure in the EU

This session gave the participants the possibility for an open discussion of the issues, particularly focusing on risk assessment, coordination of vulnerability disclosures and deployment of solutions.

Risk assessment

Referring to the Study "Availability and Robustness of Electronic Communications Infrastructures"⁶ conducted for the European Commission, one participant remarked that there will always be new threats that cannot be anticipated. It is therefore important to focus on the intrinsic vulnerabilities of Critical Information Infrastructure.

A representative from a vendor of networking equipment noted that to allow for a comparison of risk assessment results, common risk assessment techniques would be required. Another participant suggested that scenarios and use cases should be developed to support the creation of faster risk assessment procedures.

A representative from the private sector noted that a public-private partnership could provide significant benefits in the area of risk assessment. The Industry Consortium for the Advancement of Security on the Internet (ICASI)⁷ was referred to as a positive example of a private-sector initiative.

Coordination of vulnerability disclosures

It was remarked that considerations on vulnerability management must acknowledge that all major vendors operate on global scale and that national and regional solutions would always yield suboptimal results. While governments are bounded by national borders all major vendors always operate on international level.

⁶ See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm

⁷ See <http://www.icasi.org>

Global vulnerability coordination should not be undertaken lightly. It is a complex task with specific demands. It was mentioned that the proliferation of vulnerability coordinators at the global level could be harmful for all involved parties and should be strongly discouraged.

Numerous participants from the private and the public sector emphasized the importance of trust-based relationships. There was agreement that the establishment of mutual trust takes time and cannot be forced by regulation. A participant noted that vulnerability information is often confidential and can therefore not be easily distributed to private partners.

Some existing information exchanges (e.g., the Information Sharing and Analysis Centers - ISACs⁸ in the USA, the UK Network Security Information Exchange - UK NSIE⁹, the Dutch Cybercrime Information Exchange - NICC¹⁰) were pointed out as good models to exchange (sensitive) information on vulnerabilities. Governments were encouraged to further investigate their viability. It was warned that fragmentation must be avoided. It would be unproductive to have multiple separate national information exchanges discussing the same issues with the same people. It was further suggested in a written statement that benefits could be gained by mapping the existing information flows (currently there are a variety of information sharing channels in which vulnerability information may be shared between industry and government) to perform a gap analysis to identify where improvements to trans-national information sharing could be achieved.

A participant mentioned that there are multiple examples of successful partnership between individual governments and the industry and we should build upon that foundation. What is needed is to see how to extend this to include the others. The model must provide very high level of trust between all parties and be scalable. A federated model may be better suited than a centralized one.

For some participants the distinction between Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) was not sufficiently clear. The question was raised why a special communication platform is needed for CIIP. One participant specifically referred to the Critical Infrastructure Warning Information Network (CIWIN) as a possible tool to facilitate vulnerability information sharing. A representative from the Commission pointed out, that CIWIN is limited to information sharing between Member States. The European Public-Private Partnership for Resilience (EP3R) would provide a platform for information exchange between the public and the private sector.

Some participants agreed that the *modus operandi* regarding vulnerability management is still rather re-active. A more pro-active and participatory scheme would be needed. This scheme would have to include CERTs, vendors and affected customers. It was pointed out that the communication with the private sector should be bi-directional. Especially international companies sometimes do not see any added value in sharing their vulnerability and incident-related information.

Some participants remarked that national/governmental CERTs should be provided with more resources by their respective Member States. The CERTs in all Member States should have the same capabilities. This would allow for the development of further standards for

⁸ See <http://www.isaccouncil.org> and <https://www.it-isac.org/>

⁹ See <http://www.cpni.gov.uk/Products/information.aspx>

¹⁰ See http://www.samentagencybercrime.nl/UserFiles/File/NICC%20brochure_uk.pdf

cooperation. The Commission should provide support regarding budget issues of national/governmental CERTs. One participant suggested that to help CERTs, more security research teams could be involved in the process.

Some participants from the private sector pointed out that for international vendors to fully cooperate with CERTs in all Member States, many resources would be required on the vendor's part. For international vendors, a single European point of contact would therefore be most effective.

Participants agreed that the legal risks of vulnerability research should be reduced. Legal obstacles to information sharing were also discussed. Under the current legal framework of many Member States the confidentiality of vulnerability and incident-related information cannot be ensured due to the possibility of requests under national freedom-of-information laws. A representative from the Commission noted that such issues could be the subject of discussions in the European Public-Private Partnership for Resilience (EP3R).

Deployment of solutions

Representatives from vendors highlighted the difficulty of convincing customers to apply patches. This problem does not only concern home users but also corporate customers. The "fix-it-later" approach is still prevalent in many organisations.

One participant pointed out that vendors should produce higher-quality software, limiting the number of patches that need to be deployed in production systems.

Economic incentives

Many participants agreed that there is a lack of economic incentives for vendors to increase the quality and security of their products. It was noted that it is considered extremely difficult to produce software without bugs while staying competitive. The point was raised that with regard to Critical Infrastructure, the argument of "lack of incentives" could not be accepted. If the market could not deliver the level of security needed for Critical Information Infrastructure, regulation would be in order. A participant noted that the way to draft regulation is to discuss with stakeholders and agree on a minimum set of requirements. One participant suggested that regulation might also be seen as a way of protecting a company's investments in the area of security.

In complement, it was remarked that security should not be left to the argument that users do not want more security. The cost of insecure software is actually very high. A participant commented, however, that he cannot successfully convince his CEO to invest because of the lack of information in particular on the cost of insecurity. There is the need for dialogue with the Critical Infrastructures owners to assess the actual impacts.

4. CONCLUSION

The workshop on the EU policy dimension of vulnerability management and disclosure process was organised in the context of establishing a strong and trusted **European Public Private Partnership for Resilience** of Critical Information Infrastructures. EP3R will provide the platform to support the exchange of information and knowledge between public and private stakeholders on specific topics with an EU and international dimension. The creation of EP3R is one of the actions proposed by the European Commission within its Communication on Critical Information Infrastructure Protection of 30 March 2009.

The establishment of EP3R follows a twofold step-by-step approach:

- On the one hand, stakeholders will be invited to provide their views on EP3R and discuss the way forward to its creation, in particular with regard to principles for its establishment, objectives and composition.
- On the other hand, reflections on key and specific challenges that require a European Public Private Partnership approach will be initiated. The workshop on the EU policy dimension of vulnerability management and disclosure process is the first occurrence in that respect.

In the next step, the Commission will build on the experiences presented and gained at this workshop and propose further activities and discussions towards the establishment of EP3R. The CIIP communication of March 2009 envisages a roadmap and a plan for EP3R by the end of 2009; its establishment by mid of 2010 and the production of first results by the end of 2010.

./.