Resilient e-Communications Networks

September | 10

Incentives and Challenges for Information Sharing in the Context of Network and Information Security

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 expertise 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.

Acknowledgements

This report was prepared by Neil Robinson and Emma Disley from RAND Europe on behalf of ENISA. This study is part of ENISA's Resilience and CIIP Programme. The report sets out findings from a research project into the incentives and barriers to information sharing in the field of Critical Information Infrastructure Protection (CIIP). The aim of this research is to identify those barriers to and incentives for sharing information which are, in day-to-day practice, the most significant facilitators and inhibitors. Through starting to prioritise barriers and incentives this project aims to indicate where policy-makers and other stakeholders might act to facilitate greater information sharing in peer-to-peer groups, such as Information Exchanges (IE) and Information Sharing Analysis Centres (ISACs). ENISA would also like to thank the staff at RAND Europe for their professionalism and dedication that resulted in this report.

Contact details:

For contacting ENISA or for general enquiries on ENISA's Resilience and CIIP Programme, please use the following details:
Dr. Evangelos Ouzounis, Programme Manager, Resilience and CIIP Programme,
Technical Competence Department, ENISA.

Email: resilience@enisa.europa.eu Web: http://www.enisa.europa.eu/resilience

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.

Executive Summary

The importance of information sharing to ensuring network and information security is widely acknowledged by both policy-makers and by the technical and practitioner community – for example, in the European Programme on Critical Infrastructure Protection (EPCIP) and in the 2004 Availability and Robustness of Electronic Communications Infrastructures (ARECI) study, which noted that formal means for sharing information should be set up in order to "improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe". A 2009 gap analysis conducted by ENISA of good practice in respect of telecommunication network operators identified information sharing as a set of useful best practice.

Given the acknowledged importance of information sharing, this report sets out findings from a research project into the barriers to and incentives for information sharing in the field of network and information security, in the context of peer-to-peer groups such as Information Exchanges (IE) and Information Sharing Analysis Centres (ISACs).

Methods and approach

The information in this report is drawn from three sources:

- A review of available literature – both academic and non-academic publications,
- Interviews with key informants working in the field of network and information security and in IEs,
- A two-round Delphi exercise with network and information security professionals.

The aim of this project is to identify those barriers and incentives which are most important in day-to-day practice in IEs and ISACs. This research differs from other work in this field in being firmly grounded in the experiences of practitioners and those involved in IE and Information Sharing activities. Nonetheless we only managed to speak to a limited number of experts from a handful of countries. Therefore, the findings of this research are a first step to developing an evidence base in this field, but we do not claim they are generalisable to all kinds of IEs.

Incentives and challenges for information sharing

Our findings indicate that many of the barriers and incentives commonly identified in the available literature are of relatively low importance to practitioners and security officials currently working in IEs. As part of this research we asked practitioners to rank a list of barriers and incentives in terms of their relative importance.

Our findings indicate that the incentives which are most important are:

- Economic incentives stemming from cost savings;
- Incentives stemming from the quality, value, and use of information shared.

While the barriers which are the most important are:

- Poor quality information;
- Misaligned economic incentives stemming from reputational risks;
- Poor management.

Recommendations for stakeholders

Following the prioritisation exercise, we sought to identify a number of recommendations for different stakeholders. These recommendations derive from the views of expert participants at an interactive workshop held in July 2010. The key recommendations, by stakeholder, are summarised below.

European Institutions /ENISA

- Play an active role in developing a European-level platform;
- Encourage participation by Member States and relevant stakeholders;
- Play a role in linking different, existing national IEs;
- Address issues regarding the legal framework for information sharing – better understanding of legal regimes, legal barriers, encourage consistency;
- Create, develop, and maintain skills and expertise needed to establish and operate IEs;
- Encourage information sharing beyond the confines of the ICT sector;
- ENISA: Undertake a facilitating function – acting as the secretariat to IEs, managing and running meetings;
- ENISA: Broaden focus from security to business resilience and continuity;
- ENISA: Commission or conduct research and investigation into the barriers and incentives for information sharing;
- ENISA: Map the legal environment for information sharing across the EU.

National Governments

- Establish IEs where none exist;
- Host IEs – provide administrative resources, funding, and chairing meetings;
- Take some responsibility to ensure the legal framework was conducive to information sharing;
- Co-operate with other Member States;
- Ensure that their participation in IEs is well-resourced, meaningful, and effective;
- Sensitively publicise the benefits of IEs;
- Identify sectors in which platforms exist which could be used as forums for information sharing.

The Private Sector

- Be transparent and share information responsibly - IEs provide an excellent opportunity for openness;
- Use IEs to improve security voluntarily - IEs can help avoid regulatory interest and strong regulatory action which might be counter-productive;
- Set up one or more private sector only IEs as a pilot

1. Introduction

Policy Context

Increasing reliance on national and international infrastructures for essential services such as telecoms, transport, and energy means that threats to or cyber attacks on these systems can have highly disruptive effects on modern society, and the safety and welfare of the population. Public e-Communication networks form an underpinning infrastructure which enables other forms of critical infrastructure such as energy transmission or distribution networks, financial services and transportation. Given that much of Europe's (and the world's) critical infrastructure is owned and controlled by the private sector, it is widely accepted that the threat posed to these infrastructures can be minimised, and the response to an attack can be more effective, if all relevant organisations - from public and private sectors - share information about vulnerabilities, threats and attacks.

The sharing of network and information security information between operators of critical infrastructure such as providers of public e-communication networks is recognised by many security experts as an important step in improving the overall state of Network and Information Security (NIS).

In 2004, the European Commission published a Communication to the Council and the European Parliament on "Critical Infrastructure Protection in the fight against terrorism" (COM(2004) 702 final) known as the European Programme for Critical Infrastructure Protection (EPCIP). This programme was clear in identifying the importance of information sharing, and its role as a key strategic area for Europe and noted that "the constraints of competition, liability and information sensitivity need to be balanced against a need for a more secure critical infrastructure."

Resolution 2007/C68/01 of the European Council of 2007 invited Member States to *"encourage where appropriate in co-operation with ENISA, effective exchanges of information and co-operation between the relevant organisations and agencies at the national level"* and *"called upon Network Operators, service providers and the private sector to share and implement good security practices*."

The European Commission identified that the public authorities in the Member States and at EU level have a key role to play in properly informing citizens, to enable them to contribute to their own safety and security, in its communication on a strategy for a Secure Information Society (COM(2006)251).

In its Critical Information Infrastructure Protection (CIIP) Action Plan (COM (2009) 149) the European Commission launched an initiative to protect critical information infrastructures from large scale cyber-attacks and disruption. The actions set out in this plan complement existing measures in the area of police and judicial cooperation to prevent, fight and prosecute criminal and terrorist activities targeting CIIs. Measures in the Action Plan aim to improve preparedness (for example, by defining a baseline of capabilities and services of national/governmental Computer Emergency Response Teams), improving detection (by providing adequate early warning systems), and to improve readiness for mitigation and recovery (for example, by encouraging Member States to develop contingency plans), among other things.

The agenda of cooperation in CIIP was further advanced by a Ministerial Conference in Tallinn in April 2009, which reviewed the CIIP policy being proposed by the European Commission, with the aim of advancing coordination and cooperation between Member States in this field. The Conference Conclusions subsequently confirmed that a European-wide effort was needed in the approach to CIIP.

Most recently, in December 2009 the European Council Issued its Resolution on 'a collaborative European approach to Network and Information Security' (2009/C 321/01) – which highlights 'the importance of multi-stakeholder models such as Public Private Partnerships (PPPs)' as one tool to be used in a more co-ordinated European approach to Network and Information Security.

What is information sharing?

By 'information sharing' we mean the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice. The most popular structure to facilitate this sharing is a 'trusted' forum or platform where private sector infrastructure owners or operators can meet face-to-face at regular intervals and hold informal, un-attributable discussions. Frequently (but not exclusively), such groups are moderated or facilitated by a public sector agent. These may be within Public-Private-Partnerships (PPPs) or other more formal or informal mechanisms (e.g. established by communications regulatory authorities or collectively by industry).

The European Public Private Partnership for Resilience (EP3R)

The natural evolution following Resolution 2007/C68/01 was an impetus for the development of a public private platform to facilitate this exchange of information. This is known as the European Public Private Partnership for Resilience (EP3R).

The aim of establishing a European Forum for Member States to share information and good policy practices on security and resilience of CIIs was stated in the European Commission CIIP action Plan ((COM (2009) 149), and the proposal to establish EP3R received a broad support at the Ministerial Conference on CIIP which was held in Tallinn on 27-28 April 2009; the document outlining the conclusions of this conference stated that "*flexible arrangements – for example, in the form of Public-Private Partnerships or a Forum of Member States – are essential to ensure that […] understanding and information exchange is followed by concrete action at the strategic and tactical levels*". Support for EP3R was further reiterated by the Council Resolution on "a collaborative European approach to network and information security" that was adopted on 18 December (2009 2009/C 321/01).

The general objectives of the EP3R were identified as:

- Provide a flexible European-wide governance framework to involve relevant public and private stakeholders in public policy discussion and strategic decision-making;

- Focus on prevention and preparedness matters with a European and international dimension;
- Function as a forum to discuss the public policy priorities, economic and market dimensions of challenges and measures for resilience of CIIs (including appropriate positive and negative incentives for stakeholders) as well as to clarify responsibilities;
- Serve as a platform for global outreach on public policy, economic and market matters relevant to resilience of CIIs.

Whilst the high-level objectives are to:

- Provide a platform for information sharing and stock taking of good policy and industrial practices in order to foster a common understanding on the economic and market dimensions of security and resilience in the context of CIIP as well as on the roles and responsibilities of public and private stakeholders;
- Discuss public policy priorities, objectives and measures with a view to define framework conditions and socio-economic incentives to improve the coherence and coordination of policies for security and resilience in Europe;
- Identify and promote the adoption of good baseline practices for security and resilience, with a view to pursue minimum security and resilience standards and coordinated risk assessment approaches.

Finally, the key principles of the EP3R were identified as:

- Complementarity: EP3R should build upon, complement and leverage the existing national public-private initiatives whilst respecting national responsibility;
- Trust: EP3R should provide the structure, processed and environment for trusted collaboration, including the protection of sensitive information from disclosure;
- Value: emphasis on bi-directional exchanges between public and private sector participants and providing value for both governments and industry. EP3R should aim to deliver concrete results;
- Openness: open to all stakeholders contributing to the security and resilience of CIIs, balancing the need for a high degree of representation with the potential for a higher number of participants to lower the level of trust.

The European context

Although the EP3R and various other initiatives are aimed at solving the challenges of information sharing from a European perspective, there are a number of particular characteristics to any pan-European policy-making which render EU action complex. These may be clearly seen in the different legal structures across EU Member States, for example the implications of the difference between the Common Law versus Continental legal code may be relevant in determining what constitutes an acceptable boundary between information provided in a trusted forum such as an IE and what might be required to be provided under a more procedurally orientated application of legal norms.

There are also different approaches to sharing across the EU, with some countries preferring a sectoral stratification of their membership and others being made up of representatives from a number of different critical infrastructure sectors (e.g. oil and gas as well as e-communications).

Finally, the differing approaches to regulation and co-operation may also have an impact. This can be seen in the way in which the regulator and regulated entities interact. For example, in some countries there may be more of an outcome based regulatory approach, whereby both regulators and regulated jointly agree on outcomes to be achieved that are socially important, and work co-operatively to achieve them. While in other countries, for various cultural or historic reasons, there may be a somewhat clearer distinction between the regulated and regulator, where the regulator acts reflecting socio-economic expectations of their role to act as an aggressive and 'tough' watchdog on those it regulates. This is not to say that both approaches are mutually exclusive: indeed they are both driven by complex socio-cultural, economic, and legal factors. Nonetheless, they both have an impact on information sharing, for example determining whether information sharing is a bottom-up, voluntary, and organic process initiated by the regulated or whether it is a mandated one in the context of a rules based system surrounding the issuance of operator licenses for public e-communications networks.

It remains to be seen whether there is enough evidence to support a causal link between these different models, and extent and quality of information shared. Any EU effort must take these differences into account and be wary of the implications of Member State differences when trying to establish any such platform.

National Initiatives

Many countries have also established sector-specific information sharing partnerships between the government and the private sector, for example:

- the UK Centre for the Protection of National Infrastructure (CPNI) has been pro-active in the development of a number of different information sharing models, including sectoral based Information Exchanges, (IE), of which there are now 16 and which are loosely based on the US NSIE model;
- The Swiss Reporting and Analysis Centre for Information Assurance (MELANI) is an organisation which comprises a number of different sectoral groups and which organises workshops once or twice a year;
- The Dutch Cybercrime Information Exchange is a cross-sectoral group which meets bi-monthly in a face-to-face setting;
- The Spanish Grupo Trabalho Securidad (GTS) is a highly informal 'invitation only' self-regulatory platform set up to share information across different infrastructure owner/operators;
- The German Information Exchange is run by the Bundesamt für Sicherheit in der Informationstechnik (BSI – Federal Office for Information Security) and is a broad group utilising Single Points of Contact (SPoC) per sector

European and International projects and initiatives

Whilst there are differences between aforementioned partnerships and those operating in other countries, in this report we use the term 'Information Exchange' (IE) to refer generally to all such public-private information sharing partnerships. ENISA's 2009 Good Practice Guide for Information Sharing defines IE as:

"An Information Exchange is a form of strategic partnership among key public and private stakeholders. In the NIS field, these can sometimes be referred to as 'Network Security Information Exchanges' (NSIEs) although it is recognised that alternative names can also be used."

IEs fulfil a different role from Information Sharing Analysis Centres (ISACs) in supporting information sharing. This is chiefly in respect of the focus of the latter on analysis, and the input and output of data provided by the group. In general, IEs operate on a basis where the free flow of information in the meeting is prized as the output. ISACs, by comparison, include more explicit provisions for the capture of data for reports, analysis and 'product' as an output. Although this is not to say that IEs do not produce such products – the group may commission reports or may voluntarily sub-divide into smaller 'working groups' to produce specific reports if it is in the overall interest.

There are a number of international and European activities, projects and initiatives underway aimed at supporting information sharing. These include:

- Efforts to develop a new addition to the suite of Information Security Standards (ISS) of a cyber-security information exchange framework in the form of the Draft Recommendation ITU-X.Cybex, Cybersecurity information exchange framework;
- EU initiatives such as a project commissioned by the European Commission's Directorate-General Justice, Freedom and Security as part of the policy effort to improve Critical Infrastructure Protection (CIP). The aim of the Messaging Standard for Sharing Security Information (MS3i) project is to support the development of a management messaging standard in the area of security information sharing, particularly in relation to Critical Infrastructure Protection. The requirements identified during the project were incorporated into data and proposals to back up technical submissions to ISO/IEC SC27 WG1 to support a standard on information sharing;
- The 2004 study into the Availability and Robustness of Electronic Communications Infrastructures (ARECI) reviewed and developed a set of good practices amongst e-communications providers. This study noted the importance of information sharing and recommended that:

"Member States and the Private Sector should establish formal means for sharing information that can improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe".

More specifically, the ARECI report indicated that:

"Private Sector enterprises that own critical communications infrastructure must jointly establish a trusted environment for sharing information to improve the protection and rapid restoration of that infrastructure."

- The National and European Information Sharing and Alerting System (NEISAS) project is another relevant initiative, as part of the EU Seventh Framework Programme for Research and Technological Development (FP7). The aim of this project to investigate the trusted sharing of security information between and within EU Member States. NEISAS will create a framework and prototype national platform which will also provide the capability for bilateral exchange of trusted security information at the EU level between national platforms;

- The US based Information Sharing and Analysis Centre (ISAC) Council is a relatively new development aimed at establishing a framework for valuable interaction between ISACs and government. It has produced a number of white papers and documentation describing for example, the importance of information sharing and processes for vetting and establishing trust between participants.

ENISA's activities in the field of Information Sharing

ENISA's activities are aimed at helping enable the implementation of EU policies by the private sector. It does this by assuming the role of a mediator, supporting the operationalisation of EU policies by promoting good practices amongst both EU Member States and within the private sector.

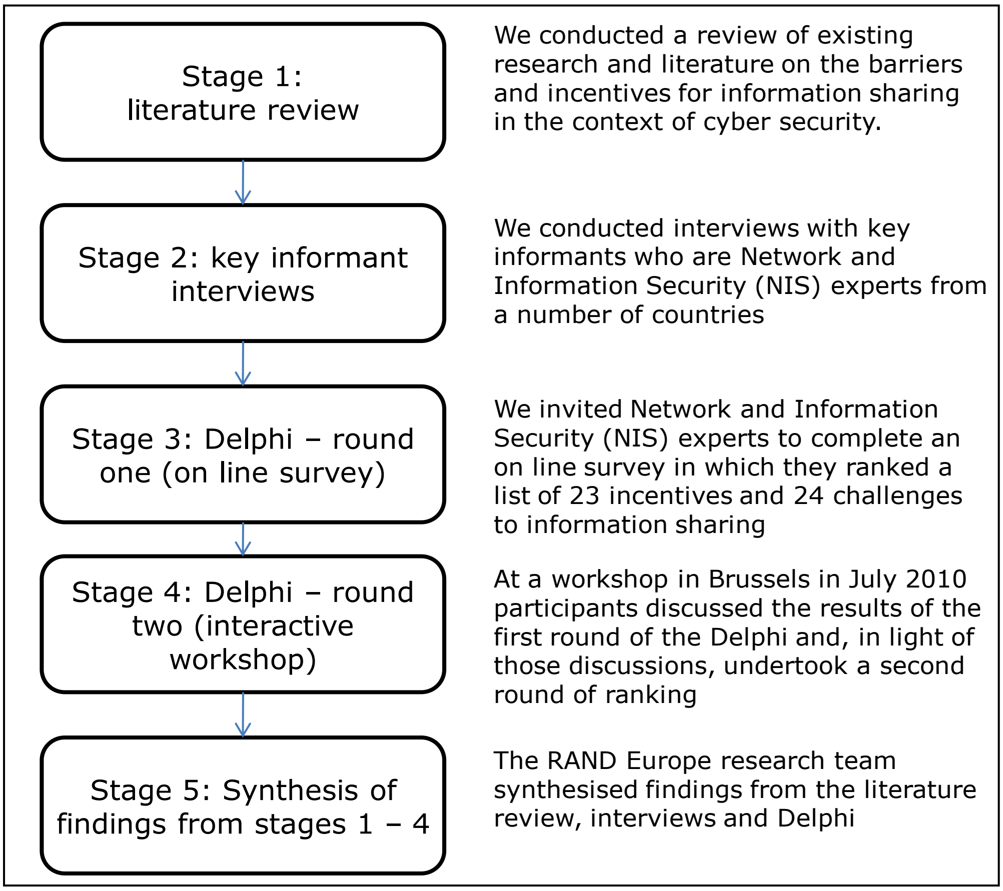
In 2009 ENISA issued its Good Practice Guide (GPG) on Information Sharing, which assists Member States and other relevant stakeholders in setting up and running Network Security Information Exchanges in their own countries. ENISA also works to promote information sharing at the national level, and in 2007 published the findings of a feasibility study for a European Information Sharing and Alerting System (EISAS). In this study ENISA was asked to analyse the current state of affairs as regards systems and initiatives across Europe that have the goal of disseminating appropriate and timely information on Network and Information Security (NIS) vulnerabilities, threats, risks and alerts.

Scope and Audience

This report deals with Information Sharing in the context of EU public policy efforts to address Critical Infrastructure Protection, specifically with regard to the providers of public e-Communication networks (the main "customer" of ENISA's resilience programme). The specific focus of this report is thus the sharing of different types of network and information security information between peers in mechanisms or models such as Information Exchanges (IE) or Information Sharing Analysis Centres (ISACs). This study does not cover other aspects of information sharing such as the public disclosure of security vulnerabilities or the notification of breaches of personal data but notes that some of the theoretical or empirical evidence from these domains may have a bearing on the sharing of information for CIP. Typical stakeholders for whom this report would be of interest include: public sector representatives (those involved in either setting national level NIS policy or the establishment or ongoing management of IEs or ISACs) and private sector IE/ISAC participants, specifically those owner- operators of public e-Communication networks and other relevant elements of the Information Infrastructure. The report will be of broader interest to those in the NIS community more generally given its focus on participation in IE as a way to address NIS risks.

Research aims and approach

This study aims to identify the most important incentives for and challenges to information sharing, in order to inform decision making about how information sharing can be facilitated by European Institutions or bodies, Member States, and the private sector. Given the national initiatives, and European and other international efforts and platforms, this study comes at an important time. As can be seen from the Council Resolution and the EP3R, there is increasing appetite to bring into focus IE as another tool to enhance the resilience of critical infrastructures. The approach taken in this study had five stages – these are summarised in Figure 1 (cf. Annex 1 Page 45).



Stage 1: literature review

We conducted a review of existing research and literature on the barriers and incentives for information sharing in the context of cyber security.

Stage 2: key informant interviews

We conducted interviews with key informants who are Network and Information Security (NIS) experts from a number of countries

Stage 3: Delphi – round one (on line survey)

We invited Network and Information Security (NIS) experts to complete an on line survey in which they ranked a list of 23 incentives and 24 challenges to information sharing

Stage 4: Delphi – round two (interactive workshop)

At a workshop in Brussels in July 2010 participants discussed the results of the first round of the Delphi and, in light of those discussions, undertook a second round of ranking

Stage 5: Synthesis of findings from stages 1 – 4

The RAND Europe research team synthesised findings from the literature review, interviews and Delphi

Figure 1: Research approach

Strengths and limitations of the research approach

In our Delphi exercise and key informant interviews the aim was to learn about the experiences and opinions of individuals who are experts in information sharing and who are actively involved in such arrangements. We realise that the participants in this research represent a very small proportion of the community of network and information security professionals. The findings from the Delphi and interviews are not necessarily intended to be representative or generalisable to all IEs in different countries and sectors.

The framework for classification of incentives and challenges

Given the multi-stakeholder complexity of this policy area, which involves public and private sector organisations, we classified each incentive or challenge according to whether it specifically operates or is important at the level of:

- the individual (psychological);
- organisational (participant) or
- governmental or agency hosting or chairing the group or forum.

For example, the incentive of 'clear processes and structures for sharing' may be relevant when viewed from an organisational, individual and governmental perspective:

- organisational since a set of common ground rules aids organisations in understanding the ‘rules of the game’;
- at the individual level as someone would feel empowered and incentivised to share after having been made aware of what is considered as acceptable conduct; and
- from the perspective of the government since there will need to be a degree of involvement on the governmental side in order to bring about this incentive.

Moreover, the incentives or challenges are also classified according to whether they occur in respect of joining a group or IE (ex-ante – i.e. as precursor factors influencing a stakeholder decision to participate in the group) or sharing information once in the group or IE. This distinction is important and reflects the obvious barrier between the phase of an organisation or individual considering membership and then actually sharing information. The latter may be seen through analysing the behaviour of ‘lurkers’ who have been attracted to joining supposedly by the incentive of access to useful information but then do not actively participate in the sharing of information - despite the existence of Non-Disclosure Agreements (NDAs) or Codes of Conduct to the contrary

Structure of the report

This report is divided into three further chapters.

- Chapter 2 draws together findings from the literature review, interviews and Delphi, and outlines incentives to information sharing. Chapter 3 does the same for the challenges and barriers to information sharing.
- Chapter 4 sets out recommendations for action on the part of various stakeholders, suggested by expert participants at an interactive workshop.
- Chapter 5 provides a brief summary and conclusions.
- Appendix 1 presents the methodology and summarises the literature drawn upon in this report. Appendix 2 lists key informant interviewees. Appendix 3 sets out the findings from the first and second round of the Delphi.

2. Incentives to Information Sharing

In this chapter we set out the incentives to information sharing identified in this research project. We have arrived at this list of incentives as a result of the literature review, key informant interviews and the two-round Delphi exercise. Based on findings from the Delphi we have grouped these incentives according to whether they were considered to be of high, medium or low importance. These groupings are loose categorisations, intended to broadly indicate relative importance. This chapter discusses those of high importance first and those of low importance last.

High	Medium	Low
1. Economic incentives stemming from cost savings; 2. Incentives stemming from the quality, value and use of information shared;	3. The presence of trust among IE participants; 4. Incentives from receiving privileged information from government or security services; 5. Incentives deriving from the processes and structures for sharing; 6. Allowing IE participants' autonomy but ensuring company buy-in;	7. Economic incentives from the provision of subsidies; 8. Economic incentives stemming from gaining voice and influence; 9. Economic incentives stemming from the use of cyber insurance; 10. Incentives stemming from the reputational benefits of participation; 11. Incentives from receiving the benefits of expert analysis, advice, and knowledge; 12. Incentives stemming from participants' personal preferences, values, and attitudes.

Incentives which were ranked of high importance

Economic incentives stemming from cost savings – How can these be evidenced and disseminated?

Participants at the workshop rated the efficient allocation of information security resources and cost savings as the most important incentive for information sharing. Further, participants felt it might be more accurate to describe many of the other incentives discussed in this chapter as 'enablers' of the efficient allocation of information security resources, rather than incentives.

We cannot fully appreciate the operation of this incentive, however, without considering the corresponding barrier: the lack of robust information about the economic returns on participation in an IE. In the literature there is some, albeit limited, evidence as to the operational benefit of information sharing. It is suggested that cost-savings may stem from quicker reactions to threats, vulnerabilities and attacks, or from anticipating network failures (ENISA, 2009: p. 15). The financial services ISAC in the US 'has been credited with helping its members avoid the widespread denial of service attacks launched in February 2000' (Anderson, 2001: p. 2).

Along the same lines our key informant interviewees (cf. Appendix 2 "List of Interviewees": 2 and 3) were of the opinion that there were many good news stories where IEs had played a tangible and beneficial role in responding to a cyber-security threat or attack. They suggested that if these were more widely known about then other organisations might be encouraged to both attend IEs and share information (cf. Appendix 2: interviewee 6).

In the interactive workshop (round two of the Delphi exercise) participants thought that the response to a particular incident might raise awareness within an organisation (possibly at a high level) of the existence of an information sharing partnership, resulting in a mandate for participation by that organisation. An instance was reported to us (cf. Appendix 2: interviewee 6) where phishing attacks prompted organisations in one sector to form an IE.

Risks of publicising IEs

The idea of using successes to 'advertise' the benefits of information sharing, however, runs into unresolved issues about the degree to which it is appropriate to publicise the membership and activities of an IE. Interviewee 1 told us that it was important in his IE that there was no publicity and no media. Others (interviewees 2 and 3) told us that they seek permission before disseminating examples of success. Whilst publicising instances of success could demonstrate the value of sharing, it also carries risk; for example, it could create the perception of a cartel.

Categorisation: Economic incentives stemming from cost savings

Clearly incentives relating to cost savings operate at the organisational level (since understanding the rationale and possible cost savings will be a business based decision). It might also be applicable at the governmental level to support more targeted investment of public resources to better protect critical infrastructures (since by definition the sharing of information by the private sector allows the public sector to understand where resources may be targeted). It works a- priori (i.e. when an organisation is assessing the viability or business case of joining) as well as the act of sharing of information once a member.

At what level does this incentive operate?	How does it operate?
• Organisational • Governmental	• Joining • Sharing

Incentives stemming from the quality, value and usefulness of information shared

In both the first and second rounds of the Delphi (and during the discussion in the workshop) incentives relating to the nature and quality of information shared were consistently highly rated – second only to the cost savings achieved through information sharing. Sharing good quality information is the best way to prove the value of an IE and to build trust. The theme of quality information featured heavily in our interviews and is also picked up within the available literature. The quality of information can be broken down into the following categories.

Data must be timely and specific

A survey of ISACs in the US found that participants had concerns over the timeliness and specificity of information shared by government – it was often not specific enough to be actionable, or participants heard information at the same time or after news coverage (United States General Accounting Office (US GAO), 2004: p. 32).

Participants must share information which is of equal value

IE participants interviewed by Messenger reported that part of their motivation to share information stemmed from the expectation that they would receive information of equal value at some point in the future (Messenger, 2006: p. 5). A similar point is made by Aviram and Tor, who argue that a risk to information sharing could be posed if all parties to the exchange do not have information which is of similar utility (Aviram and Tor, 2004: p. 242).

Information shared must be relevant to participants' concerns

The US GAO notes that one potential problem to overcome in IEs is ensuring that the group maintains a focus on emerging issues which are of interest to members (United States General Accounting Office, 2001: p. 2). This means that participants continue to benefit from (and are incentivised to maintain) participation. Anecdotal evidence suggests that in certain isolated cases, participants discuss and share information not exclusively related to CIP issues but which they jointly deem of interest and relevant to their concerns.

In the first round of the Delphi, respondents rated 'discovery of solutions to specific NIS problems' as fifth (out of 17). However, it was considered less important in the workshop. It could be that participants did not separate gaining useful information from the broader incentive of getting returns on investment in information sharing.

As well as a need to share information within the IE, there is an onus on members to use that information in their home companies as well as possible. It is not clear the extent to which this is currently being done (cf. Appendix 2: interviewees 2 and 3). The more that information is fed into internal processes, the more likely it is that any benefits of participation might be realised. There is a related need to report back to the IE which subjects are of interest to those within the home company.

Sharing information at a suitable level

During the interactive workshop (Delphi Round Two) there was discussion as to the level of information which should be shared. It is for each IE to decide whether they are interested in between high-level strategic information that helps to understand the direction of threats and more 'operational level' information. In turn, this related to the positioning of the IE: at the preparatory level or at a tactical level? In our interviews it was reported that it was possible to share information at a level which was detailed enough to be useful, but which did not give away highly sensitive data (cf. Appendix 2: interviewee 4).

Categorisation: Incentives stemming from the quality, value and usefulness of information shared

The complex multi-stakeholder aspect of what is deemed 'relevant' by all parties in such public private enterprises suggests that this incentive operates at both the participant level and also the governmental facilitator. For example, (depending on the nature of the role of the governmental entity in any IE) there may be asymmetrical information as to what constitutes concerns between the private sector participants and the government who will, for example, have access to different (potentially classified) information. Similarly, this incentive might have an effect during the business decision-making about whether to participate in the first instance, but also whether once a member they feel they are getting good 'value for money' in terms of the information flows of the platform.

At what level does this incentive operate?	How does it operate?
• Individual • Organisational • Governmental/ host	• Joining • Sharing

Incentives which were ranked of medium importance

The presence of trust amongst IE participants

All of the organisations identified trust as the essential underlying element to successful relationships and said that trust could be built only over time and primarily through personal relationship .(United States General Accounting Office (GAO), 2001: p. 2)

The need for trust among participants at IEs is noted extensively in the relevant literature, was mentioned by key informant interviewees, and was identified in the Delphi as an important incentive for information sharing. Within the literature there appears to be considerable agreement as to how trust can be built and maintained:

- Trust must be built over time and through personal relationships (Suter, 2007: p. 12);
- Membership should be as constant as possible (Office of the Manager National Communication Systems, 2001: p. 17; United States General Accounting Office, 2001: p. 7);
- Regular, face-to-face meetings (United States General Accounting Office, 2001: p. 2);
- Creating separate IEs for network providers and vendors/ suppliers might mean members are more willing to share with a limited audience (ENISA, 2009: p. 16).

Findings from recent empirical research cast some light on the detail of how trust develops and is maintained. Based on interviews with IE participants in Europe and America, Messenger (2006) distinguishes five different forms of trust:

- Deterrence-based: trust is backed up by negative consequences (e.g. a legal obligation to share);
- Calculus-based: trust is a way to receive a reward;

- Knowledge-based: trust is based on knowledge of the person enabling a predication of how they will act;
- Identification-based: trust is based on a perception that other participants have similar desires and intentions;
- Pre-emptive or referential-based: trust is based on a reference from already trusted or respected peer.

Anecdotal evidence also suggests that the number of members of an IE should be kept to a minimum in order to facilitate personal relationships. Messenger's interviewees believed that knowledge-based trust is the most 'appropriate' for participants in an IE, and this has implications for the way IEs are constituted and run: this kind of trust develops through interaction over time between individuals. Thus, it is important that IEs have consistent membership. Messenger's research also indicated that this kind of trust could be generated by seeing participants dealing with high-pressured situations in which there were difficult decisions to be made about how to deal with sensitive information.

Findings from our interviews and the Delphi are in line with Messenger's research. An interviewee (1) reported that in his IE, lack of attendance at meetings results in expulsion from the group (thus ensuring consistent and regular face-to-face contact), and that new members were allowed by invitation only and needed to be proposed by an existing member (thus creating referential-based trust). Another interviewee (5) described an incident where the IE helped in the response to an incident which 'proved' the value and ability of the IE and the host (thus creaking knowledge-based trust).

Categorisation: The presence of trust amongst IE participants

The presence of trust operates as an incentive at all levels. Whilst the interaction of personalities is important for creating trust, it may also be established at the organisational level due to aspects of commonality amongst participants. Finally, trust plays a role at the governmental level since the participants have to place their individual trust, and that of their organisation in the government hosting the IE, that information provided during the interactions will not be passed on. The incentive operates both as a lever to organisations to join a group (e.g. seeing that it is a trustworthy forum may precipitate potential members to join) and as an incentive for the sharing of information once in the group.

At what level does this incentive operate?	How does it operate?
• Individual • Organisational • Governmental	• Joining • Sharing

Incentives from receiving privileged information from government or security services

One possible driver for participation in IEs is gaining access to information from government, law enforcement or security services, which is not available from any other sources (ENISA, 2009: p. 10). This incentive refers specifically to information the government or law enforcement agencies have chosen to release to the IE participants given their membership of a trusted community.

Findings from the Delphi confirmed that this is an important incentive. Participants reported that access to restricted or classified information or non-public information from government was welcomed in an IE and represented high-quality information. Interviewees (2 and 3) confirmed that the ability to find out what government was thinking about a particular issue was one attraction of membership, and other said that gathering information from intelligence services was a strong incentive (interviewee 5).

In the workshop there was a discussion about the precise role of law enforcement agencies in IEs. Some IEs involve participants from law enforcement agencies who attend meetings, whereas some prefer to include law enforcement in an 'outer ring' of trust. What is important is that this information can filter into an IE; it does not necessarily mandate attendance by law enforcement. Information collected from our key informant interviews indicates that in some IEs law enforcement might be involved sometimes, with the permission of members.

Categorisation: Incentives from receiving privileged information from government or security services

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Joining • Sharing

Incentives deriving from the processes and structures for sharing

There is considerable agreement in the literature that the structures set up within IEs for information sharing are important to building and maintaining trust between participants, and facilitating the timely sharing of information:

> *To make information sharing real it is essential to lower the practical risks of sharing information through both technical means and policies, and to develop internal systems that are capable of supporting operational requirements without interfering with core business. Consequently, the technical means used must be simple, inexpensive, secure and easily built into business (United States General Accounting Office, 2004: p. 33)*

Responses to the Delphi confirmed that clear rules, processes and structures in an IE are an incentive to (or enable) information sharing. It could be that these processes work by building or ensuring trust, which in turn facilitates information sharing.
Findings from our interviewees (cf. Appendix 2: 1 and 5) suggest that it is not always important to have a highly complex structure. Some IEs prefer minimal rules for sharing information. What is perhaps important is that the 'rules', however minimal, are clear, understood and followed, and are appropriate to the IE. Groups which have high levels of pre-existing trust might need less rules and procedures than newly-formed groups in which participants do not know each other so well.

We consider separately the following elements of structure: leadership, processing and labelling information, storage and access.

IE leadership

Different IEs have different leadership arrangements. In many IEs a government department acts as a facilitator. The literature suggests the following may be important:

- The presence of a mutually-trusted third party to chair meetings and broker information exchange (Messenger, 2006);
- The ISACs in the US facilitated trust by scrutinising and authenticating members (United States General Accounting Office, 2004: p. 31).

Two interviewees (cf. Appendix 2: 2 and 3) working in a semi-independent organisation which hosts an IE reported that in their experience, leadership of an IE was very important. The host can shape the tone and environment of an IE, and ensure that is used (and perceived) as not a cartel, and not a forum for lobbying government. They can also remind participants who are not sharing information of the importance and consequences of continued reticence.

Processing and labelling of shared information

Many IEs have a system for assessing, grading, storing, and permitting the sharing of information. Such arrangements may make participants feel more in control of information, and thus incentivise sharing. The literature mentions the following arrangements may encourage information sharing:

- Allowing control of information to rest with the organisation which originally shared it is very important (United States General Accounting Office, 2004: p. 31). This means that a participant can share knowing that he is still in control of the information.
- Participants sign up to formal non-disclosure agreements (Suter, 2007: p. 14) and reach agreement about how to use and protect shared information (United States General Accounting Office, 2001: p. 2).
- Confidentiality arrangements can ensure that confidential and commercially sensitive information is properly managed and reasonably protected from unauthorised use or disclosure - for example the 'deed of confidentiality' issued by the Australian Government.
- Developing standard terms for describing and communicating information (Cavusoglu, et al., 2005).
- Anonymising or particularly anonymising data can ameliorate some of the risk taken by the sharing organisation (Messenger, 2006: p. 5).
- Having mechanisms to handle violations within the IE (United States General Accounting Office, 2001: 7).

Secure storage and access to shared data

The way in which shared information is stored may provide assurance to participants. For example:

- There should be effective and secure communications including secure websites (United States General Accounting Office, 2001: p. 2);
- The provision of an encrypted email and secure web portal to participants (United States General Accounting Office, 2004: p. 31).

Clear goal

When an IE has a clear mandate and goal this can incentivise or facilitate information sharing through to ensuring that the IE shares information of use to all participants. Delphi respondents ranked this as a relatively important incentive.

Categorisation: Incentives deriving from the processes and structures for sharing

At what level does this incentive operate?	How does it operate?
• Individual • Organisational • Governmental/ host	• Joining • Sharing

Allowing IE participants' autonomy but ensuring organisational-level support

Messenger's research into sharing in IEs suggests that information sharing may be facilitated through permitting participants some autonomy to make decisions about what to share and how to use received information. A participant needs to feel 'empowered' by his or her organisation to share information and needs to have the ability to effect appropriate changes in response to information shared (Messenger, 2006: p. 5).

The US GAO similarly reports that it was important to the success of information sharing that the senior management of participating companies supported the idea of sharing and assigned resources to IE participation (United States General Accounting Office, 2001: p.2).

Allowing IE participants' autonomy was ranked highly in the first round of the Delphi, but slightly less so in the second round – in which the overriding need to show the economic returns from information sharing dominated discussions. Participants also thought it was important that every organisation which sends a representative to an IE is engaged, supportive, and recognises the importance of information sharing. Interviewee 1 (cf. Appendix 2) explained that all participants in his IE must bring an official commitment from senior management.

Categorisation: Allowing IE participants' autonomy but ensuring organisational-level support

This incentive operates at the individual participant level (since the act of sharing is very often delegated to the level of the individual in a specific meeting) and only comes into play ex-post once an organisation has joined such a group.

At what level does this incentive operate?	How does it operate?
• Individual	• Joining

Incentives ranked of low importance

Economic incentives stemming from the provision of subsidies

The idea of using subsidies in order to incentivise information sharing is suggested as a potential incentive in the literature, but it was ranked very low (receiving no votes in the second round) by Delphi respondents. Neither was it mentioned by interviewees.

The idea is that companies could be incentivised to participate in IEs and to share information through the provision of subsidies, with the amount of the subsidy linked to the extent of sharing which takes place (e.g. socially optimal or simply enough for a firm to internalise its externalities). Government subsidised insurance could also be considered (Gordon, et al., 2003: p. 480). Aviram (2004) argues, however, that we have to be careful to only subsidise organisations which participate effectively.

Categorisation: Economic incentives stemming from the provision of subsidies

Were this incentive to operate in practice, it might do so at the organisational level (a decision taken on the basis of a business case and the cost benefit analysis of any subsidy vs. the internal and external costs of participation) and might come into effect both before a participant decides to join but also during membership in respect of the sharing of information.

At what level does this incentive operate?	How does it operate?
• Organisational	• Joining • Sharing

Economic incentives stemming from gaining voice and influence

Participating in an IE might provide private companies with a point of contact with government officials and regulators, and this might be attractive for some companies because of the potential to influence or have an inside view on government policy, and the possibility of avoiding the introduction of misplaced regulation (ENISA, 2009: p. 15).

It might also be that official government statements of support for IEs provide an incentive for private entities to participate; officials at two of the 15 ISACS surveyed by the US GAO said that it was important that the federal government voice its support for ISACs as the principle tool for communicating threats (United States General Accounting Office, 2004: p. 310).

No empirical evidence from the literature could be found as to whether participating in an IE actually provides opportunities to communicate with government. Findings from the Delphi were that this was not regarded as an important incentive by respondents (it was ranked 11th out of 17 in round one and sixth out of eight in second round). Although some interviewees reported that the ability to have an influence over government thinking featured, to some extent, in their IEs (cf. Appendix 2: interviewees 1 and 4).

As to why there was a disjuncture between the literature and the practical experience of NIS experts, during the workshop some participants said that in some IEs governments and regulators were not always welcomed since they exposed participants to greater scrutiny. One participant said it was important that IEs which do have government participation are not seen as a forum for big business to lobby or influence decision-making.

On the other hand, findings from the workshop indicate, given the current lack of mandated information sharing, participating in voluntary IEs was a way for different sectors to prove they could act responsibly and share information without further regulation or governmental input. In this sense, whether governments participate or not, participating in an IE is a way for organisations to communicate that they are serious and responsible about information sharing.

Categorisation: Economic incentives stemming from gaining voice and influence
This incentive could operate at the organisational level (since the organisation may want to internally promote its participation as a way to demonstrate a perception that it has influence or voice). It can operate both as an attraction to become involved but also, as anecdotal evidence suggests, upon the sharing of information once participants are engaged (e.g. if those supplying the information can see that it has been positively received).

At what level does this incentive operate?	How does it operate?
• Organisational	• Joining • Sharing

Economic incentives stemming from use of cyber insurance

Some writing in this field have suggested that cyber insurance could play a role in incentivising the industry to attend to information security (Cukier et al., 2005: p. 32 and Boehme et al., 2010). Cyber insurance policies cover damage caused by a full array of security problems, including viruses, worms, denial of service attacks, and data theft or corruption. Statistics indicated that it is still quite rare for organisations to have cyber insurance, but most observers expect the number of policyholders to increase over time (Hahn and Layne-Farrar, 2006: p. 350).

The reason why insurance could be used to incentivise sharing is that companies who took out such insurance might be offered cheaper premiums if they participated in an IE. A similar effect may be achieved if sector regulators were to include in their audit checklists whether a firm is a member of an IE.

However, findings from the Delphi workshop suggest that in practice the cyber insurance market does not operate in this way at all. Merely participating in an IE is not sufficient to lower cyber insurance premiums, where they are taken, since insurance companies want to see more tangible action before lower premiums are offered. It could be that this changes as the cyber insurance market matures. Another factor preventing the use of cyber insurance as an incentive is the lack of actuarial data on the effects of participating in an IE. In turn, this is linked to the general absence of robust information on the cost-effectiveness of information sharing.

Categorisation: Incentives stemming from the reputational benefits of participation

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Joining • Sharing

Incentives from receiving the benefits of expert analysis, advice and knowledge

Many IEs are able to offer some analysis services, perhaps employing IT experts. When participants share information this can be analysed and results of the analysis returned to the participant so that they are better informed about the nature of the attack, threat or vulnerability. The provision of expert analysis is an identifiable benefit of membership, and might be an incentive to join. The provision of expert analysis, and in particular real-time analysis, was identified as important in research by the US GAO (2001: p. 2). Similarly, the ability to analyse 'raw' data on incidents, threats, and vulnerabilities from a number of sources, and then to share this analysis in an appropriate, timely, and useful way, was described as a priority for the US Federal Government in setting up critical information protection (Relyea and Seifert, 2005: 23). IEs might also be able to provide participants with information about new technologies and/or information about security management practices (United States General Accounting Office, 2001).

There were mixed results in the Delphi exercise as to relative importance of this incentive. It was ranked highly in the first round, but in the second round workshop participants did not assign it any importance at all. Findings from our key informant interviews, however, suggest that provision of high-quality 'products' is considered by some operating in the field to be an important feature of a good IE. Interviewees 2 and 3 reported that in their IE there were frequently presentations and other products that provide a 'rich environment to add value'.

Further, the Delphi also asked respondents to consider the importance of access to pooled information from many participants and sources, and this was ranked to be of high to medium importance. This kind of information allows participants a 'rich picture' of a threat or issue. Of course, one other service which an IE might offer which would provide a further incentive to join, is more robust information about the cost of security breaches (as discussed in section 2.1.1). A survey of cyber security decision-making in US companies found that businesses were particularly interested in such information (Rowe and Gallaher, 2006). IEs may have the capacity to undertake such research.

Categorisation: Incentives from receiving the benefits of expert analysis, advice and knowledge

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Joining • Sharing

Incentives stemming from participants' personal preferences, values and attitudes

The personality of the representative sent to the IE may act as a facilitator to information sharing. For example, empirical research into individuals who 'log on' to internet chat rooms but do not contribute or post information (called 'lurkers' by researchers, cf. aforementioned) suggests they trust other members of the community less than those who post more often (Ridings et al., 2006). Messenger's research suggests that the frame of mind of participants can have an effect upon their sharing behaviour (2006).

This incentive operates at the individual level. We postulate it is linked to the type of individuals that work in the field of NIS. Although this could be the subject of further research, even a cursory understanding of the motivations and belief systems of those who hold technical or operational positions in NIS suggests that individuals possessing certain personality characteristics (e.g. perhaps as defined by the Myers-Briggs Type Indicator) work in this field: such as altruism, a desire to see the right thing done, and willingness to work collectively to solve problems.

Categorisation: Incentives stemming from participants' personal preferences, values and attitudes

At what level does this incentive operate?	How does it operate?
• Individual	• Joining • Sharing

3. Challenges and barriers to information sharing

As with the chapter on incentives, in this chapter we list the challenges and barriers to information sharing roughly in order of importance, as ranked by Delphi participants. There are some overlaps, and these categories should be taken as indicative.

High	Medium	Low
1. Poor quality information; 2. Misaligned economic incentives stemming from reputational risks; 3. Poor management;	4. Type of participants; 5. Legal Barriers related to fear of legal or regulatory action; 6. Fear or leaks; 7. Group size; 8. Misaligned economic incentives stemming from group behaviour – externalities; 9. Social barriers from government; 10. Misaligned economic incentives stemming from poor decision-making about investment in security; 11. Norms of rivalry;	12. Legal barriers related to Freedom of Information; 13. Misaligned economic incentives stemming from the costs of participating in IEs; 14. Misaligned economic incentives stemming from competitive markets; 15. Legal barriers related to competition law violations.

Barriers ranked of high importance

Barriers posed by the kind of information shared

The inverse of the incentive reported in section 2.1.2, above, Delphi participants reported that the most significant barrier was poor quality of information shared.

Categorisation: Barriers posed by the kind of information shared

At what level does this incentive operate?	How does it operate?
• Individual • Organisational • Governmental/ host	• Joining • Sharing

Barriers posed by participants and poor management

In the Delphi exercise respondents identified a number of barriers which stemmed from how IEs are constituted and managed. This accords with the discussion in the previous chapter that strong management was an important enabler or incentive for information sharing.

Firstly, there was a strong preference for participants to be technical or security experts, rather than people with responsibilities for sales, marketing or other commercial activities (cf. Appendix 2: interviewees 2 and 3 also reported this). It was thought that the position of such individuals was incompatible with creating a trusted environment for information sharing, since they would be influenced by commercial considerations. One interviewee (1) said that the IE in which he participated was limited to skilled information security managers among which there could be a peer-to-peer relationship, and that members had a 'gentlemen's agreement' that information would not be used commercially. In the workshop discussion participants reported that finding the correct representative for an IE within a particular organisation could be an iterative process

As mentioned above, there was a discussion at the workshop as to whether government representatives should sit on IEs. The same interviewee (1) reported that representatives from the state did not participate, since it was not always necessary, and made other participants feel more comfortable. Instead, information was reported back to government on an informal and case-by-case basis when necessary. Whilst prizing information from government, interviewees 2 and 3 were aware of the risk of appearing too close to government.

Secondly, poor management by the chair or host was ranked highly as a challenge to participation and sharing. Management could include both management of the content of meetings, and the administrative arrangements. Interviewees themselves working in an organising hosting and IE described their responsibility to take an active management role; managing communications and messages internally and externally; setting standards for information sharing; and where necessary sanitising information which is too commercially sensitive. They also acted as a gatekeeper between the IE and law enforcement. Another interviewee (4) reported that the chair could provide 'company neutral' analysis.

Thirdly, if a group was too big, the less likely it was that members would have common interest, and the less likely it was that trusting relationships would develop. This was ranked as a barrier of medium importance. One interviewee (1) said that one element contributing to the success of the IE in which he participated was limiting the numbers of participants.

Lastly, diversity among participants was not considered to be an important barrier to information sharing.

Categorisation: Barriers posed by participants and poor management

The way in which an IE is constituted and managed might act to prevent joining in the first place, and inhibit sharing amongst members. This could affect individual participants and organisations. Governments may decide not to participate or to share openly if the organisation and members of a forum are inappropriate.

At what level does this incentive operate?	How does it operate?
• Individual • Organisational • Governmental/ host	• Joining • Sharing

Misaligned economic incentives stemming from reputational risks

Private companies participating in IEs have a strong interest in protecting their reputation. Reputation might relate to the quality of service provision, level of customer service, or to holding personal information about customers securely. Therefore, disclosing information about an attack or vulnerability risks damaging or losing consumer trust and reputation with investors (Camp, 2006: p. 6; Information Assurance Advisory Council, 2004: p. 2).

Information about the quality of service provided by a company is commercially sensitive between competitors, thus presents a barrier to sharing information about attacks and vulnerabilities (ENISA, 2009: 16).

Findings from the Delphi support the claim that risks to reputation are of high concern and represent a significant barrier to information sharing – this was ranked as the second most important barrier, after poor quality information, in the second round. Correspondingly, fear that information shared would be leaked was also very highly rated as a barrier to sharing. What is interesting is that the chance of getting a good reputation through participation in an IE was not important, where as the risk of getting a negative reputation through participating and sharing is ranked as a significant problem.

Categorisation: Misaligned economic incentives stemming from reputational risks

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Joining

Barriers ranked of medium importance

Legal Barriers related to fear of legal or regulatory action

The fear that a disclosure will lead to legal action against a participant company is a potential barrier mentioned in the literature (Aviram, 2004: p. 13; Baer, 2003: p. 3). The concern is that security breaches which caused loss to service users or which caused the leaking of customers' private information may result in actions against the company. Related to this, there could be concern that a disclosure in an IE could result in action by a regulator (ENISA, 2009: 16).

Whilst the possibility of disclosures opening up legal liability seems real, Cukier et al. (2005) note that they could not identify any examples where it has happened.

The view of those respondents who took part in our survey was that, although they reported more concern about regulatory action than either freedom of information or non-compliance with competition law, it still ranked relatively low.

Categorisation: Legal Barriers related to fear of legal or regulatory action

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Joining • Sharing

Group size

If a group was too big, the less likely it was that members would have common interest, and the less likely it was that trusting relationships would develop. This was ranked as a barrier of medium importance.

Although participants at the workshop agreed that group size was important, they did not say how many participants was ideal, or the point at which the group became too big. Further, discussion of group size might also take into account the need for cross-sector participants, and the ideal number of participants from different stakeholders. This is an area for further research, or where further information might usefully be sought from experts and practitioners.

Categorisation: Group size

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Joining • Sharing

Misaligned economic incentives stemming from group behaviour

Economic theory suggests that information will only be shared in an IE when the benefits of doing so outweigh the costs. Particularly, economic theory suggests two ways in which economic incentives can be misaligned when individuals act in groups: externalities and free-riders.

Externalities

When a participant in an IE weighs up the benefits and costs of information sharing there is potentially a problem of externalities. Externalities are usually understood as impacts or consequences not transmitted through prices which may be incurred unintentionally by an actor. These may be either costs (known as negative externalities) or benefits (known as positive externalities). This is where the participant only takes into account the direct benefits to himself of information sharing, and not the wider benefits which may accrue to other members of the group. This means that, from a societal perspective, the act of sharing is under-valued (Hahn and Layne-Farrar, 2006: p.317) and the participant might be less inclined to share information. The participant also might not put the same effort into producing information as he would have done if the benefit to all who could use the information were taken into account (Aviram and Tor, 2004: p.238).

Thus, members of an IE may have an incentive to under-invest in information sharing (compared with the socially optimal amount of investment) since they do not reap all the benefits of doing so.

Given the large number of people who are indirectly affected by network security, the network members are unlikely to be able to internalize the externalities (Aviram and Tor, 2004: p.15)

Whilst the concept of externalities is well-established within the economics literature there is some disagreement about the extent to which externalities impact upon the behaviour of organisations. In relation to externalities in software vulnerabilities and network security (which may hold some transferable lessons for IEs), it is pointed out that many firms are already spending a great deal on network security measures, which provides some counter-evidence as to the inhibitive effect of externalities (Hahn and Layne-Farrar, 2006: p. 324). In relation to IEs, we know that a number of private organisations in several countries are signed up to IEs. Further, the software vulnerabilities literature suggests that individuals who act to protect themselves do make themselves less vulnerable than those who do not. Transferring this argument to IEs, it could be that the benefit to an individual of information sharing is sufficient to incentivise sharing behaviour.

Evidence from our Delphi suggests that whilst failure to see wider benefits beyond those to an individual organisation is somewhat a barrier to information sharing, it is not one of the main barriers. In the first round of the Delphi this was ranked the third most important barrier, but this dropped significantly in the second round, where workshop participants ranked it as a medium to low priority.

Free-riders

A second barrier suggested by the economics literature, and stemming from misaligned economic incentives, is the problem of free-riding: that a member of an IE may be tempted to 'free-ride' and under-invest in information sharing in the hope of obtaining helpful information from other members for little or no cost.

The free-rider problem arises (at least in theory) from the fact that information is non-exclusive but excludable; once information has been produced or acquired it may be shared and put to use by others at little additional cost, but it may also be hoarded and not shared (Aviram and Tor, 2004: p. 238).

Findings from the Delphi suggest that this is not a significant barrier to information sharing – respondents said that fear of free-riders was not on their minds when deciding whether to participate or share (it was ranked lower than externalities, but is discussed here because it is similar to the issue of externalities).

Further, whilst economists portray free-riding as a rational calculation in which an actor tries to maximise benefit and minimise cost, .empirical research into individuals who 'log on' to internet chat rooms or online communities but do not contribute or post information (whom researchers called 'lurkers') suggests a slightly different picture. A survey of these individuals revealed although there were some lurkers who 'got what they wanted' without posting themselves, the motivation for apparent free riding was more complicated, for example, a fear that comments would be mocked or their credibility undermined. The researchers conclude:

> *The implication from this study is that there is much that we can do to make the community a more interesting, satisfying and comfortable environment for both lurkers and posters (Preece, et al., 2004)*

This could possibly have implications for understanding the motivations for non-sharing in IEs, and devising measures which can be taken by facilitators to improve sharing, and receives some support from our interviewees, who noted that responses to non-participation at an IE must taken into account the reasons behind that. For example, a small company may have less to contribute that a larger one, and would feel uncomfortable if they were challenged.

A finding from the Delphi exercise which does not support the assertions in the literature that free riding is a significant problem, is that a small number of respondents said that they were incentivised by 'giving help to others'. Clearly, this was much lower in importance than other incentives, but it does not suggest as calculating or self interested a picture as economic theory might suggest.

Categorisation: Misaligned economic incentives stemming from group behaviour

These barriers operate against sharing information within the group

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Sharing

Social barriers stemming from government

The National Commission on Terrorist Attacks Upon the United States highlighted what it considered to be a significant impediment to comprehensive intelligence analysis — the 'need-to-know' culture of information protection. The commission suggested that, while the federal government has access to huge volumes of information, procedural and organisational cultural barriers undermined the government's ability to capitalise on these resources (Relyea and Seifert, 2005: p. 2).

Delphi respondents appeared to have some sympathy with this view. The 'culture of secrecy within government' was rated of medium importance in both rounds of the Delphi, as was the disincentive which could arise of the public sector seems to be receiving but not sharing information. This corresponds with the finding that information from the public sector is highly prized.

Categorisation: Social barriers stemming from government

At what level does this incentive operate?	How does it operate?
• Individual • Organisational • Governmental/ host	• Joining • Sharing

Misaligned economic incentives stemming from poor decision-making about investment in security

There is evidence that organisations may not view their network and information security investment decisions in the same way that they view other investment decisions:

Rarely does an organization undertake a sophisticated or even semi-sophisticated financial analysis (i.e., cost-benefit or rate-of-return analysis) prior to making the investment or deciding on the level of investment that is needed (Rowe and Gallaher, 2006)

In research looking at financial disclosures under the US Sarbanes–Oxley Act, Ghose and Rajan point out that compliance (which we might see as subject to similar pressures and drivers as information sharing and participation in an IE) demands upfront investment, where as benefits are hard to quantify and come later (Ghose and Rajan, 2006: 4). There is little robust data about the returns on investment in security – for example, an organisation may not be able to determine how many attacks have been deterred or prevented through their security measures:

> *Perhaps the greatest barrier to information sharing stems from practical and business considerations in that, although important, the benefits of sharing information are often difficult to discern, while the risks and costs of sharing are direct and foreseeable (United States General Accounting Office, 2004: p. 33)*

The idea of 'ambiguity aversion' is instructive here, describing decision makers' preference for options with more certain outcome probabilities over options with less certain outcome probabilities but equal expected values (Aviram and Tor, 2004: p. 260). Aviram and Tor argue that 'findings on ambiguity aversion suggest that rivals may choose to sacrifice a measure of expected value to avoid the ambiguous course of action of a novel information sharing agreement' (p. 263).

Poor information about the relative benefits and costs, and aversion to uncertainty could lead to a lack of information sharing because companies do not think it is worth the time or the investment. It could also be self-fulfilling, since without sharing information it is less likely that a better assessment (made with fuller information) will be undertaken. It might also interact with a 'status quo bias', which would operate against information sharing unless there are huge and clear benefits to be gained from sharing.

These ideas from the economics literature are supported, and somewhat contextualised, by findings from recent empirical research based on interviews with private sector participants of IEs (Messenger, 2006). This research provides support for the idea that the costs are easier to quantify than the benefits; interviewees reported that negative consequences 'loomed large' in their assessments. Further, findings from this research suggest that information sharing in IEs is influenced by participants' expectations as to possible benefits and costs, rather than more tangible, actual outcomes (Messenger, 2006: 4).

However, findings from our Delphi suggest a slightly different interpretation. The need to see the savings and benefits from participation in IE was ranked the most important incentive, which suggests that (at least among our participants) network and information security was considered important. The problem of poorly informed decision making about network and information security – ambiguity aversion – was ranked as an insignificant barrier; it did not explain reluctance to participate in IEs or share information. Rather, discussion from the workshop suggests that it is the lack of robust data about the benefits of participation which are the core problem.

There are some suggestions in the literature as to how assessments about benefits and costs can be improved (and thus potential barriers to information sharing removed). These accord with the discussions at the interactive workshop.

- A better understanding of risk could therefore facilitate information sharing (Information Assurance Advisory Council, 2004: 2);
- Participants' expectations can change over time, and develop through personal experience (Messenger, 2006);

- Past or present co-operative relationships among competitors can lead to a better perceptions of risks (Aviram and Tor, 2004: 267);
- Successful past collaborations can reduce the ambiguity associated with perspective information sharing (Messenger, 2006: 268).

Categorisation: Misaligned economic incentives stemming from poor decision-making about investment in security

At what level does this incentive operate?	How does it operate?
• Individual • Organisational • Governmental/ host	• Joining • Sharing

Norms of rivalry

Social norms are likely to exist among participants within an IE, and academics have suggested that such norms might operate so as to decrease the efficiency of information sharing (Aviram and Tor, 2004: p. 251). Participants may continue to conform to an obsolete norm even when the situation has changed so that a different norm is needed.

Particularly, norms of rivalry between competitors might operate so as to create a significant barrier to information sharing. Aviram and Tor argue that the competitive model is 'deeply embedded in our culture, and is directly promoted in the training of business decision makers' (p. 252). Such norms are more likely to exist in concentrated markets where rivals continually and repeatedly battle with one another. Alternatively where there is a history of co-operation or collaboration, rivalry norms may have less of an impact (p. 267).

The tradition of secrecy and non-cooperation were rated of medium to low importance by our Delphi respondents.

Categorisation: Norms of rivalry

At what level does this incentive operate?	How does it operate?
• Individual • Organisational • Governmental/ host	• Joining • Sharing

Barriers ranked of low importance

Legal barriers related to Freedom of Information

Most countries have Freedom of Information laws, under which the public can request access to information held by government. One possible barrier to sharing information in IEs is that participants fear the information they share might be subject to a freedom of information request by a member of the public. This would result in sensitive information about their vulnerabilities or security being released to the public (Aviram, 2004: p. 13; Baer, 2003: p. 3).

There is no empirical evidence to support these claims, and some academics writing on this topic have suggested that these legal concerns are 'not substantial enough' to explain poor information sharing (Aviram, 2004: p. 13).

As with barriers stemming from competition law (discussed below), respondents to our survey ranked barriers stemming from freedom of information requests as being of relatively low importance (as did interviewees [5]). However, it might be that the barriers posed by legislation differ between countries.

Categorisation: Legal barriers related to Freedom of Information

At what level does this incentive operate?	How does it operate?
• Organisational	• Joining • Sharing

Misaligned economic incentives stemming from the costs of participating in IEs

There are costs of participating in an IE. At the most basic level these are the costs of staff time to attend meetings, but other costs might stem from collecting and collating information to share or from subscription fees (charged by some models of information sharing platform). Most IEs have secure websites and employ the services of expert analysts to process information shared by participants. Administering meetings also bears a cost (United States General Accounting Office, 2001: 2).

Findings from a survey of 15 ISACs in the US indicate the difficulty of expanding membership to small entities which need security support but which have insufficient resources to actively contribute and pay for support. The Financial Services ISAC in the US responded to this by establishing an ISAC which provides different levels of service – ranging from a free basic service to fees for value-added services – to help ensure that no company or group is excluded because of cost (United States General Accounting Office, 2004: p. 30).

Among those who responded to the Delphi survey and participated in the interactive workshop, costs of taking part in an IE were rated among the least important barriers. Nor were participants overly concerned by the time and staff commitments needed to attend one or more IEs. Of course, the relative cost of participating is highly dependent on the size of the organisation and the kind of IE (how much preparation etc. is involved). So it could be that these particular respondents did not find this a problem, but others – from smaller organisations – might have done. In our key informant interviews it was reported (cf. Appendix 2: interviewees 2 and 3) that the cost of participation were easily offset by the value of the advice gained from peers and the host.

Categorisation: Misaligned economic incentives stemming from the costs of participating in IEs

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Joining • Sharing

Misaligned economic incentives stemming from competitive markets

Loosing competitive edge

Many IEs will involve participants from rival firms competing to provide, for example, telecoms or electricity services to customers in the same market. In this situation, economic theory suggests that a slightly different version of the 'prisoner's dilemma' could arise. Withholding information from a competitor gives a participant in an IE an edge in competing with rivals. There could also be significant hidden cost in sharing the information: tougher competition from the now more knowledgeable (and thus more effective) rivals (Aviram, 2004: 38).

Perhaps unexpectedly, the experience of Delphi respondents suggests that fear of losing competitive edge was not an important consideration. However, they did believe that if participants with sales of commercial responsibilities are present at an IE, this can act as a significant barrier to information sharing by making the environment of the IE more competitive (as discussed in 3.1.2).

Non-sharing as a predatory act: degradation

Some writers argue that participants may refuse to share information in order to harm rivals (Aviram and Tor, 2004: p. 243). The notion here is that a competitive advantage can be attained not only through 'positive' effects of improving services, but also through a 'negative' effect of harming the good and services of a competitor.

Degradation is likely in industries which are 'network industries' – such as energy, transportation, communications, and the financial sectors (Aviram and Tor, 2004: p. 266). It is more likely in situations where there is one organisation, larger than the others, which is able to impact the market, but can also occur where differentiated firms have some idiosyncratic advantages and disadvantages vis-à-vis their competitors, where degradation could be effectively used to exploit one firm's relative advantage over its competitors.
This was not mentioned at all in the Delphi workshop or in interviews.

Categorisation: Misaligned economic incentives stemming from competitive markets

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Sharing

Legal barriers related to competition rules violations

The literature mentions that IE participants might have concerns about possible violations of anti-trust or fair-competition law (Aviram, 2004: p. 13; Baer, 2003: p. 21). We found no empirical evidence which tested this claim in the literature.

Fear of breaching competition law was ranked as the least important barrier in our Delphi survey, and was reported in interviews not to be a problem (cf. Appendix 2: interviewee 4).

Currently in the US anti-trust authorities review plans for ISAC's and issue 'business review letters' which approve the arrangements, although there is talk of exempting IEs from anti-trust rules (Aviram, 2004: p. 16).

Categorisation: Legal barriers related to competition rules violations

At what level does this incentive operate?	How does it operate?
• Individual • Organisational	• Joining • Sharing

4. Recommendations

This research project aimed to investigate the nature and relative importance of different barriers to and incentives for information sharing in the field of network and information security. From the literature, interviews and findings from the Delphi we have been able to identify a number of barriers and incentives which may have a significant impact upon information sharing practices.

Incentives

In terms of incentives, it is vital that organisations participating in IEs can see the quantitative, economic benefit of information sharing; this is the best way to incentivise participation and sharing. There is some anecdotal evidence that IEs have improved the response to incidents and improved members' security, but there is a lack of 'hard' evidence on this point. This means that it can be difficult for an organisation to decide whether, and how much, to invest in information sharing Stakeholders such as ENISA and the academic and research community may be able to help to address this – through commissioning and conducting research.

It is also important that the information shared at an IE is relevant to participants, is of high quality (from a reliable trustworthy source), and is at the appropriate level on the operational-strategic spectrum; different IEs will require different kinds of information. Participants must communicate about the kind of information which is useful to them, and IE hosts should do their best to plan and manage IEs so that information discussed meets requirements.

Barriers

As for barriers, participating in an IE carries risks to the reputation of organisations if sensitive information was to be leaked or widely disseminated. This risk, our research suggests, acts as a significant barrier to information sharing. This can, however, be mitigated through developing trust and ensuring appropriate rules and structures.

Recommendations for action by stakeholders

The purpose of identifying these barriers and incentives is to develop the available evidence-base for policymakers and others with an interest in this topic. With this policy-oriented goal in mind, we asked participants at the interactive workshop to suggest recommendations as to how different stakeholders could ensure the incentives identified were put in place, and barriers were overcome, and thus facilitate better a quantity and quality of information sharing. Below we set out and discuss the suggestions of workshop participants.

These recommendations are addressed to six stakeholder groups: European Institutions, including the EU body European Network and Information Security Agency (ENISA), national/ local governments, the private sector, users, and academics and researchers. We set out these recommendations below.

Although there was no prioritisation of the recommendations, a certain extent of clustering could be discerned: these included common ideas around the need for further investigation of the legal constrains of IEs (particularly pertinent as the profile of IEs and information sharing generally will increase given the policy priority attached to developments such as the EP3R), exhortations for the EU to drive forward progress on the EP3R and for national governments to use existing platforms to seed information sharing.

Finally, a cluster of recommendations could be discerned both for national governments and the private sector regarding recognition and dissemination of the value or benefit of IEs and information sharing mechanisms.

The European Institutions/ ENISA as an EU Body

Participants agreed that the **EU institutions/ ENISA as an EU body should play an active role in developing a European-level platform for information sharing**. Existing plans and discussions at the EU-level about the establishment of structures for information sharing, for example, through EP3R, were very much welcomed by participants, although all were keen to see moves towards implementation – either through EPPR or some suitable alternative. In this role, the EU should encourage participation by Member States and all relevant stakeholders (although there was recognition of the complexity of including all Member States/ relevant stakeholders and ensuring a trusted environment for sharing). Participants suggested that similar platforms in the US and Japan might be a source of good practices. A few participants' recommendations went further, suggesting that the EU should act to 'force' IEs in some circumstances.

As part of developing a new platform or platforms at the EU-Level, participants also thought the EU institutions had a role in **linking different, existing national IEs** – through a pan-European exchange of national exchanges.

The EU institutions also have the resources and jurisdiction to **address issues regarding the legal framework for information sharing**. They could carry our research to understand better the legal and regulatory frameworks in different Member States, how they operate in practice, what risks or barriers these pose to information sharing, and the extent to which the law varies across different countries. The EU could also look at European laws and regulations, and examine their implications for current and future needs for information sharing. The EU could act to encourage consistency between Member States, even developing a European legal framework to support secure information exchange.

Creating, developing, and maintaining skills and expertise needed to establish and operate IEs, was recommended as a potential role for the EU. This could be through ensuring that participants from different IEs in different sectors share their experience and learning. This helps to build capacity for information sharing.

Participants suggested that the EU should **encourage information sharing beyond the confines of the ICT sector**; businesses and organisations from all sectors use vulnerable technologies and should invest in information security. A narrow focus on ICT sector – particularly telecoms - is not an optimum approach. The EU should encourage a focus on critical users of ICT (e.g. energy, finance etc.), thus creating a more market-based approach.

It was recommended that ENISA could **undertake a facilitating function** – acting as the secretariat to IEs, managing and running meetings (including potentially running and administering EP3R). It was also recommended by some participants that ENISA could **broaden its focus from security to business resilience and continuity** – and in turn encourage the sharing of a wider type of information at IEs.

Participants felt that ENISA had an important role in commissioning or **conducting research and investigation into the barriers and incentives for information sharing**, including from the perspective of industry. From this research, ENISA can (continue) to issue good practice guidance on information sharing to a number of audiences. Also in its 'research and analysis' function, ENISA might undertake a mapping of the legal environment for information sharing across the EU, and investigate the implications of any inconsistencies identified.

National/Local Governments

In countries where there are currently no (or only a few) IEs, it was recommended that national governments should **start by establishing a 'small and simple' IE**; with a manageable number of participants and a fairly tight focus. Linked to this, participants recommended that national governments had a proper role in **hosting IEs** – providing administrative resources, **funding and chairing** meetings at national and/or local level.

One recommendation was that national governments should consider how to link CERTs with IEs, ISACs, WARPs, etc. in order that these groups have greater inter-operability.

Participants believed that national governments also had some **responsibility to ensure the legal framework was conducive to information sharing** (as well as the EU). This could involve analysis of the implications of domestic laws (for example national competition law) on information sharing. Individual **Member States should co-operate with each other** and with EU institutions to ensure greater consistency – as well as to learn lessons about operating IEs effectively.

Some participants recommended that national governments should **ensure that their participation in IEs is well-resourced, meaningful, and effective**, and is led by an individual of sufficient seniority and influence.

A role in **sensitively publicising the benefits of IEs** was also recommended (although we note here caveats from discussion earlier in the day – that too much publicity might damage trust, and that robust evidence of the economic benefits of participation in an IE is currently lacking). Since the benefits from IEs might only be realised and become apparent in the long term, national governments might provide investment, support and encouragement to newly-formed IEs. Linked to this, it was recommended that national governments should **invest in education** in relation to the methods and benefits of information sharing.

National governments may be able to **identify sectors in which existing platforms exist which could be used as forums for information sharing**. This means that IEs are not established unnecessarily and do not duplicate existing efforts. In turn, national governments should identify gaps and act to establish information sharing arrangements to fill them.

One recommendation was that national and/or local government could add value to the tactical- and operational-level information which is shared at IEs. Once this information is put into a wider context of other threats or sector-specific intelligence, the information shared becomes more useful to participants.

The Private Sector

Participants agreed and recommended that there was an onus on industry to be **transparent and share information responsibly**. This openness should be directed at those within the industry, as well as customers and the wider public. For example, vendors should openly discuss problems and thus increase the chance of finding constructive and timely solutions. IEs provide an excellent opportunity for such openness, given the protections afforded to information shared in such forums.

Some workshop participants recommended that industry could still make improvements in the way information learned at IEs was used within their organisation – information had the potential to be more useful, and thus participation in an IE more cost-beneficial.

Participants saw IEs as a way for industry to **improve security voluntarily**. It was recommended that industry make the most of this opportunity since not doing so increases the chances of state and EU-level regulation. IEs can help avoid regulatory interest and strong regulatory action which might be counter-productive. One recommendation was to **set up one or more IEs for the private sector** only as a pilot. This would usefully investigate the advantages and disadvantages of a forum which did not include regulators or government.

Civil Society/Users

There were fewer recommendations for the wider public and users. Participants thought there could be value in ensuring that users have clearly identified and available mechanisms for reporting incidents. This needed to be provided alongside education, firstly, so users know the limits of the security measures they might consider infallible and understand security risks. Secondly, so that users know that they can share information about security threats and they know what information to share, when, and the benefit to themselves and others from doing this. Thirdly, education could overcome concerns that large companies participating in IEs are doing so to build ties with government and regulators, rather than improve security.

Some participants recommended setting up ‘cyberhood-watches’ – to encourage communities of users to report incidents and share information along the same model of neighbourhood watch. Others suggested there should be better communication channels so that citizens to play a more active role in NIS.

Academia and Research

Participants saw academics and researchers having an important role in undertaking research and analysis to address existing knowledge gaps. For example, work to identify, describe, and quantify the benefits and costs of participating in IEs; undertaking case-study research into instances where attacks might have been prevented, or their impact lessened, or there have been more, better, or more timely information sharing. Research must be able to inform future policy-making in this field.

Appendix 1 - Methodology and Reviewed Literature

Methods and approach

The information in this report is drawn from three sources:

- A review of available literature – both academic and non-academic publications,
- Interviews with key informants working in the field of network and information security and in IEs,
- A two-round Delphi exercise with network and information security professionals.

The aim of this project is to identify those barriers and incentives which are the most important in day-to-day practice in IEs and ISACs.

From our literature review we identified a long-list of barriers and incentives to information sharing. We then asked respondents to rank these barriers and incentives in a Delphi exercise. We also discussed the long-list of barriers and incentives during interviews with key informants.
0
The available literature on information sharing is fairly limited – being largely theoretical and lacking and empirical basis. This research project goes some way to beginning to create an evidence base to inform policy and practice in relation to information sharing for network and information security.

The strength of our approach is that we have been able to speak to expert practitioners to try to understand how the different barriers and incentives identified in the literature operate in practice. The limitations of our approach are that we have spoken to a limited number of experts, from a handful of countries and sectors. The barriers to information sharing might be very specific to country and industry sector. Therefore the findings of this research are a first step to developing an evidence base in this field, but we do not claim they are generalisable to all kinds of IEs.

Literature Review

We conducted a targeted literature review to find information on the barriers and incentives to information sharing in IEs. Figure 2, below, outlines our research approach. Our starting point for the review was the literature which was known to the RAND research team (from their knowledge on this area) and to the commissioning team at ENISA. We followed-up citations and references in this literature to extend the number of relevant sources. We also identified literature by searching databases such as Google scholar. Using the search terms such as ‘information sharing AND cyber security’. We searched for articles in peer-reviewed journals, books and ‘grey literature’ (non-peer reviewed pieces written by information sharing organisations, think-tanks and so on).

We were looking for literature which specifically addressed peer-to-peer information sharing, therefore we excluded literature on, for example, CERTS, software vulnerabilities, public information sharing platforms and so on. We looked for literature written in English since 2000. In total we identified and read over 50 articles, of which 22 we considered to hold relevant information. Relevant references are listed in Table 1.

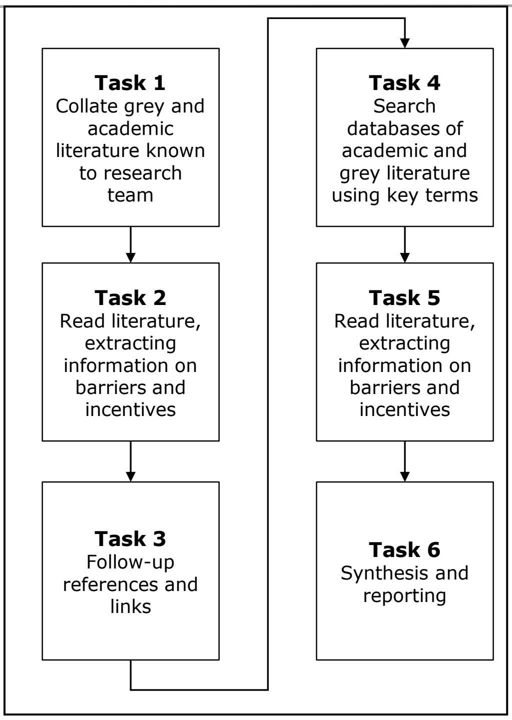

Task 1
Collate grey and academic literature known to research team
Task 2
Read literature, extracting information on barriers and incentives
Task 3
Follow-up references and links
Task 4
Search databases of academic and grey literature using key terms
Task 5
Read literature, extracting information on barriers and incentives
Task 6
Synthesis and reporting

Figure 2: Overview of Research Approach

Quality of the available literature and the evidence base

The literature on the barriers and incentives to information sharing in IE is limited. We identified only 7 sources which had an empirical element -i.e. which had looked at practices of information sharing. Only 4 of these looked specifically at information sharing within IE, and none of these had a robust enough methodology to enable conclusions to be drawn as to the cause of sharing or not sharing.

Much written about on this topic is theoretical – especially from the field of economics. This is useful for hypothesis building, but is a weak basis for policy making in absence of empirical evidence.

Lastly, there are some peripherally-relevant areas of literatures (software vulnerabilities etc) which might have some transferrable lessons.

Table 1: list of reviewed literature

	Author	**Topic**	**Empirical, theoretical, or review?**	**Peer reviewed/ grey literature?**
1.	Anderson (2001)	Software vulnerabilities	Largely theoretical drawing on some real-life examples.	Conference paper

2.	Aviram (2004)	Into private cyber-security associations (IEs)	Theoretical	Working paper (non peer-reviewed)
3.	Aviram & Tor (2004)	Anti-trust law/ economics	Largely theoretical, including literature review	Peer-reviewed journal
4.	Baer (2003)	IT security	Theoretical – drawing on some real-life examples	Peer-reviewed journal
5.	Camp (2006)	Economics of Information Security	Theoretical	Reviewed journal
6.	Cavusogly (et al (2005)	Vulnerability disclosure	Theoretical – economic model	Conference paper
7.	Cukier et al (2005)	CI protection	Review	Report of a conference
8.	ENISA 2009	IEs	Good practice guide	
9.	Gal-Or & Ghose (2005)	Economics - Information exchange for IT security	Theoretical	Peer-reviewed journal
10	Ghose & Rajan (2006)	Impact of Regulatory Information Disclosure (SOX)	Theoretical	Conference paper
11	Gordon et al (2003)	Information exchange on IT security	Theoretical	Peer-reviewed journal
12	Hahn & Layne-Farrar (2006)	Law on software security	Theoretical, including literature review	Peer-reviewed journal
13	Information Assurance Advisory Council (2004)	Information sharing	Empirical	Grey literature – not peer-reviewed
14	Messenger (2006)	Information sharing in IEs	Empirical	Grey literature – not peer reviewed
15	Office of the Manager of National Communication Systems (2001)	Description of an ISAC	Good practice guide	
16	Preece et al (2003)	Behaviour in chat rooms	Empirical	Peer-reviewed journal
17	Relyea & Seifert (2005)	Information Sharing for Homeland Security	Review of existing arrangements for information sharing	Grey literature – report to congress
18	Rowe & Gallaher (2006)	Investment in cyber security	Empirical	Grey literature. Not peer-reviewed

19	Suter (2007)	Review of IE models	Review of existing arrangements for information sharing	Grey literature. Not peer - reviewed
20	US GAO (2001)	Review of IE arrangements in US	Partly empirical	Grey literature
21	US GAO (2004)	Review of IE arrangements in US	Partly empirical	Grey literature
22	Wang (2006)	Effect of disclosures under SOX	Empirical	Conference paper

Key informant interviews

We conducted interviews with experts, practitioners and academics working in the field of information security. We identified interviewees through

- ENISA’s contacts and network – including attendees at a workshop in March#
- RAND Europe research team’s contacts

This strategy was intended to identify a number of individuals who had expertise in the barriers and incentives to information sharing. The sample of interviewees was not intended to be representative, or to yield generaliable results.

In total we conducted nine interviews. Interviewees are listed in Appendix 3.

The interviews we conducted over the telephone by members of the RAND Europe research team. We did not use a detailed protocol to structure the interviews and the precise questions asked. We instead identified a number of broad questions and topics to discuss with each interviewee – this provided some guidance, but did not attempt to pre-judge interviewees views and perspectives. This is appropriate for an exploratory piece of research. The broad topics for the interview were as follows:

- The drivers of participation in such information exchanges
- Key challenges for the information sharing within these exchanges
- Key incentives which might encourage, support or make organisations share more information
- The organisational and procedural issues associated with participation in such groups
- Key legal and regulatory challenges and incentives
- How challenges and incentives differ, for example, between sectors or according to the membership of different groups.

In order to encourage interviewees to be as open as possible in their responses we did not make a recording of the interviewees. Immediately after the interview the interviewee wrote a detailed note of the interview.

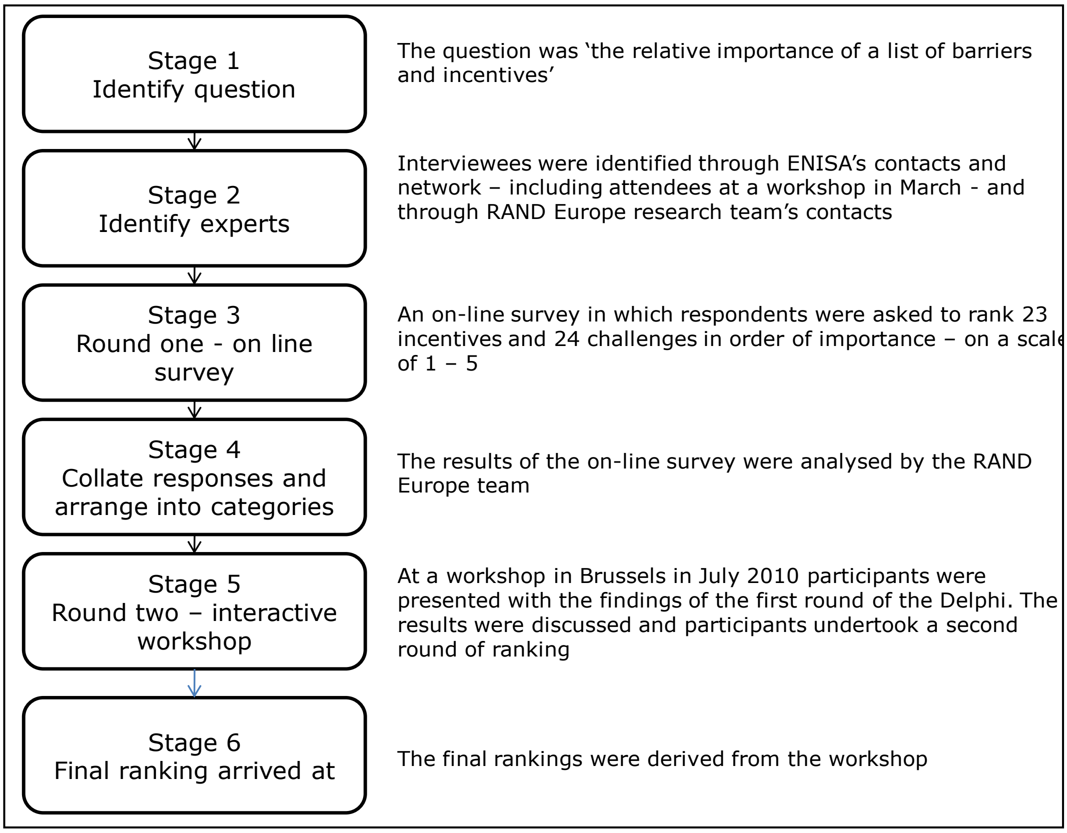
The interview notes were then analysed in order to identify key themes and ideas, and to draw out information relevant to the different barriers and incentives identified in the literature.

The Delphi

A Delphi exercise is a structured way in which to collect large amounts of qualitative information – principally expert opinion – from experts in a field. A Delphi uses ranking, scoring and feedback to arrive at consensus on a set of issues.

A Delphi is a good way to collect data on an issue like the barriers and incentives to information sharing, because this is a topic on which subjective judgements, gathered on a collective basis, could help to inform decision-making.

The Delphi process is outlined in Figure 3.
The results of round one and round two of the Delphi are in Appendix 4



Stage 1
Identify question

The question was 'the relative importance of a list of barriers and incentives'

Stage 2
Identify experts

Interviewees were identified through ENISA's contacts and network – including attendees at a workshop in March - and through RAND Europe research team's contacts

Stage 3
Round one - on line survey

An on-line survey in which respondents were asked to rank 23 incentives and 24 challenges in order of importance – on a scale of 1 – 5

Stage 4
Collate responses and arrange into categories

The results of the on-line survey were analysed by the RAND Europe team

Stage 5
Round two – interactive workshop

At a workshop in Brussels in July 2010 participants were presented with the findings of the first round of the Delphi. The results were discussed and participants undertook a second round of ranking

Stage 6
Final ranking arrived at

The final rankings were derived from the workshop

Figure 3: The Delphi process

Appendix 2: List of References

- Anderson, R. (2001). *Why information security is hard. An economic perspective (Paper presented at the ACSAC conference 2001)*: Proceedings of the 17th Annual Computer Security Applications Conference. Available at www.acsac.org/2001/papers/110.pdf
- Aviram, A. (2004). *Network Responses to Network Threats: The Evolution into Private Security Associations (Florida State University College of Law Working Paper number 115)*: Available at http://ssrn.com/abstract=570342. Accessed on 3rd March 2010.
- Aviram, A., & Tor, A. (2004). Overcoming Impediments to Information Sharing. *Alabama Law Review, 55*(2), 231 - 280.
- Baer, W. S. (2003). Rewarding IT security in the marketplace. *Contemporary Security Policy, 24*(1), 190-208.
- Böehm, R. and Schwartz, G. (2010) Modelling Cyber-Insurance: Towards A Unifying Framework (Working Paper) presented at the Workshop on the Economics of Information Security (WEIS), Harvard, June 2010
- Camp, L. J. (2006). The state of economics of information security. *I/S A journal of law and policy, 2*(2), 189 - 205.
- Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2005). *Emerging Issues in responsible vulnerability disclosure (Paper presented at the Workshop on Information Technology and*
- *Systems (WITS'2004)*: Available at http://infosecon.net/workshop/pdf/cavusoglu.pdf. Accessed 30th April 2010.
- Cukier, K. N., Mayer-Schonberger, V., & Branscomb, L. M. (2005). *Ensuring (and Insuring?) Critical Information Infrastructure Protection (John F Kennedy School of Government Faculty Research Working Paper Series RWP05-55)*: Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=832628. Accessed 26th April 2010.
- ENISA (2009). *Good Practice Guide Network Security Information Exchanges*: Available at http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide. Accessed 13th February 2010.
- Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research, 16*(2).
- Ghose, A., & Rajan, U. (2006). *The economic impact of regulatory information disclosure on information security investments, competition and social welfare (Paper presented at the Workshop on Economics of Information Security 2006)*: Available at http://weis2006.econinfosec.org/docs/37.pdf. Accessed 30th April 2010.
- Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy, 22*(461-485).

- Hahn, R. W., & Layne-Farrar, A. (2006). The Law and Economics of Software Security *Harvard Journal of Law and Public Policy, 30*, 283-354.
- Information Assurance Advisory Council (2004). *Sharing is protecting*: Available at http://www.iaac.org.uk/Default.aspx?tabid=62. Accessed 13th February 2010.
- Messenger, M. (2006). *Cyber-security: Why would I tell you? Research briefing*.
- Office of the Manager National Communication Systems (2001). *Guide To Understanding The National Coordinating Center For Telecommunications And The Network Security Information Exchanges*: Available at: http://www.ncs.gov/nstac/reports/2000/NCC_NSIE.pdf/. Accessed 4th March 2010.
- Preece, J., Nonnecke, B., & Andrews, D. (2004). The top five reasons for lurking: improving community experiences for everyone. *Computers in Human Behaviour, 20*(2), 201-223.
- Relyea, H. C., & Seifert, J. W. (2005). *Information Sharing for Homeland Security: A Brief Overview (CRS Report for Congress)*: Available at http://www.fas.org/sgp/crs/RL32597.pdf. Accessed 27th April 2010.
- Ridings, C., Gefen, D., & Arinze, B. (2006). Psychological Barriers: Lurker and Poster Motivation in Online Communities. *Communications of the Association for Information Systems, 198*, 329 - 354.
- Rowe, B. R., & Gallaher, M. P. (2006). *Private Sector Cyber Security Investment Strategies: An Empirical Analysis (Interim report)*: Available at
- Suter, M. (2007). *A Generic National Framework For Critical Information Infrastructure Protection (CIIP)* Zurich Center for Security Studies, ETH Zurich
- United States General Accounting Office (2001). *Information Sharing. Practices that can benefit critical infrastructure protection*. Washington, D.C: GAO. .
- United States General Accounting Office (2004). *Critical Infrastructure protection. Establishing Effective Information Sharing with Infrastructure Sectors*: Available at www.surfacetransportationisac.org/SupDocs/d04699t.pdf.
- Wang, T.-W., Rees, J., & Kannan, K. (2008). Reading the Disclosures with New Eyes: Bridging the Gap between Information Security Disclosures and Incidents (Paper presented at the Workshop on the Economics of Information Security): Available at http://weis2008.econinfosec.org/papers/Wang.pdf.

Appendix 3 –Interviewees

Interviewee number	Country	Description
1	Spain	Telecommunications industry. Participant in an IE
2 & 3	UK	Representative from CPNI
4	US	Representative from IT ISAC
5	Switzerland	Representative from MELANI
6	Luxemburg	Representative from Ministry of Economy and Foreign Trade
7	Sweden	Representative from Swedish Contingency Agency
8	UK	Consultant
9	US	Representative from Financial Services-ISAC

Appendix 4 – Results of the Delphi

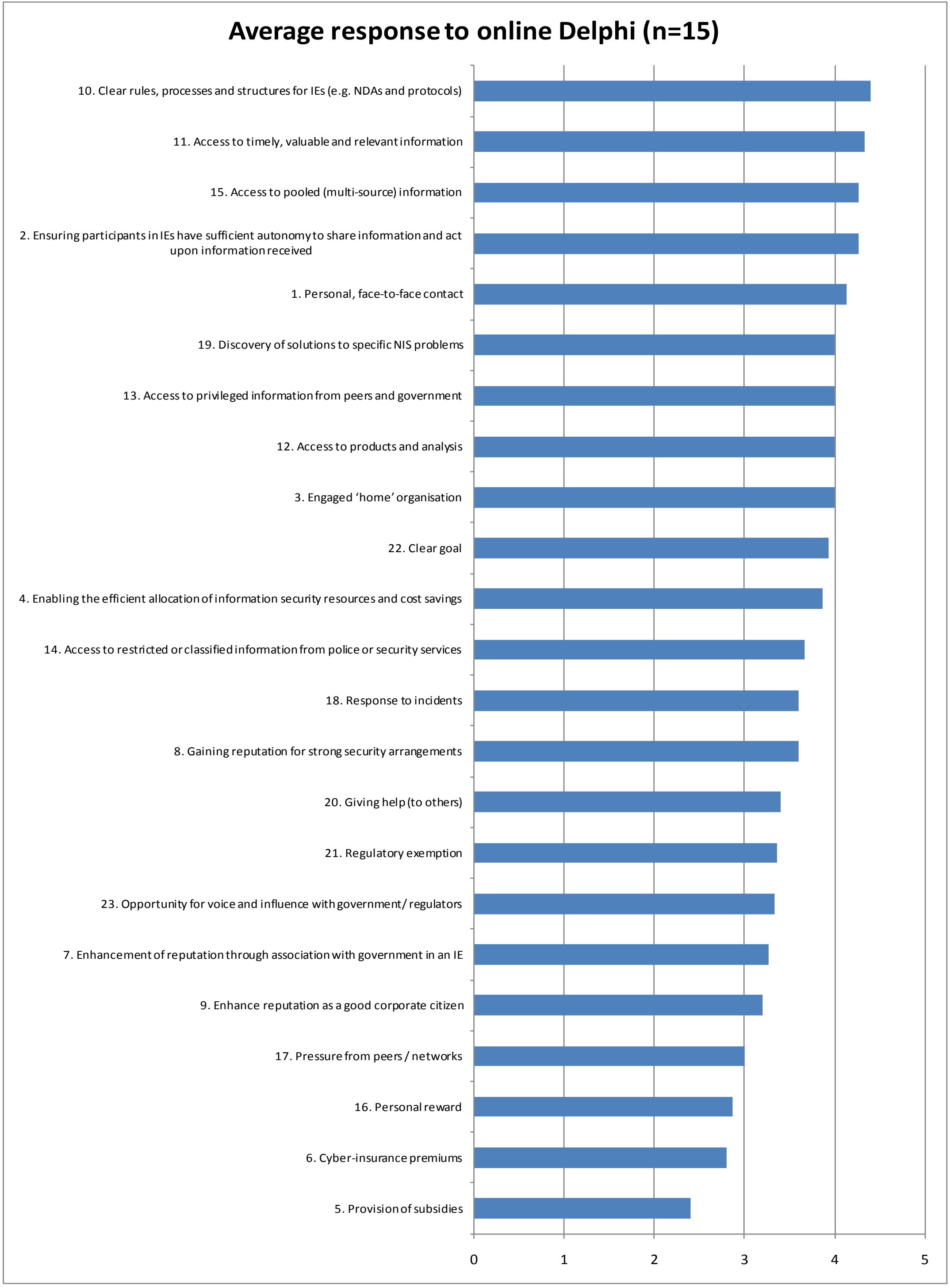


Figure 4: Responses to question 1: From your perspective, what are the most important incentives to information sharing? Results from online survey (Round One)

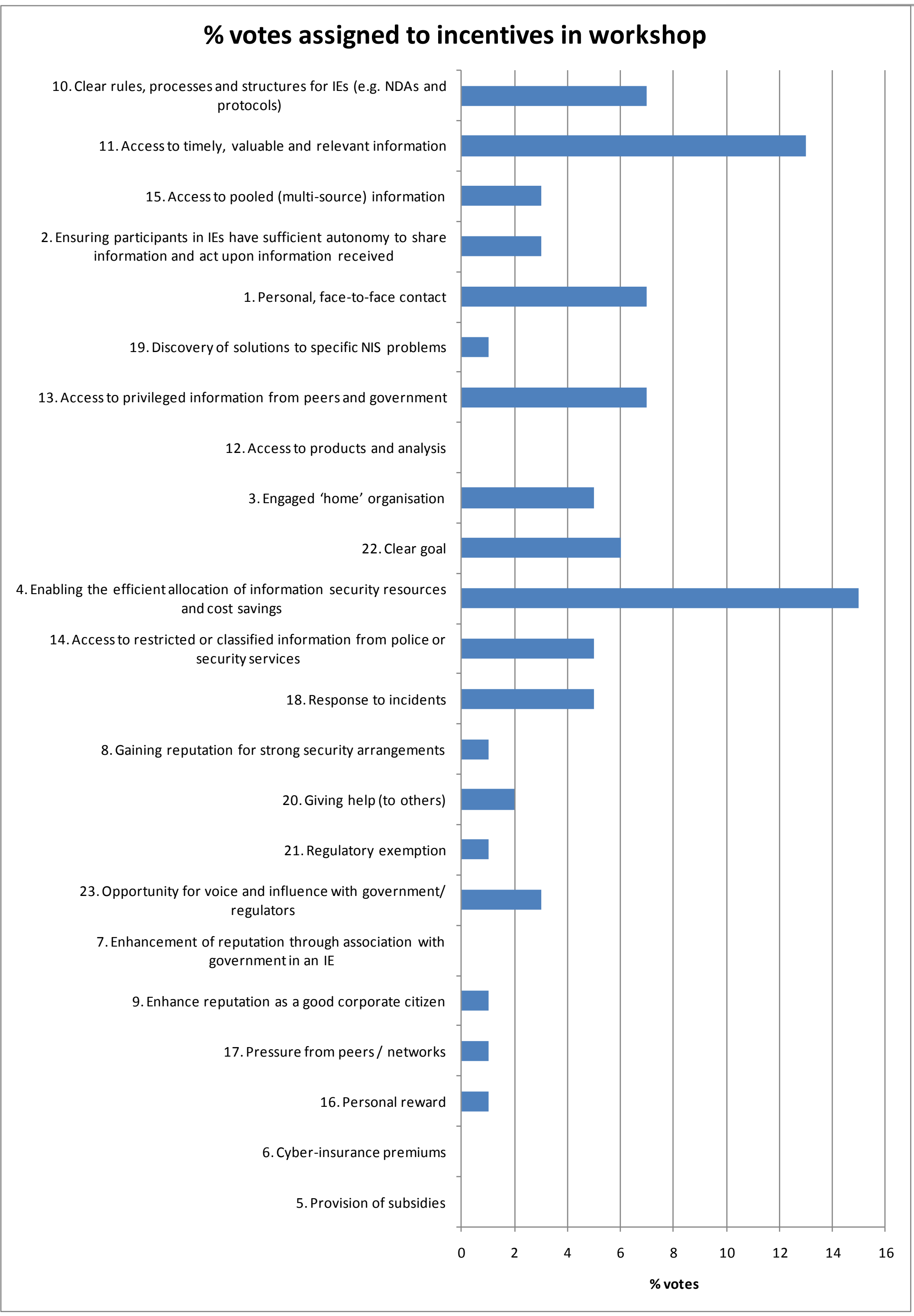


Figure 5: Responses to question 1: From your perspective, what are the most important incentives to information sharing? Results from workshop (Round Two)

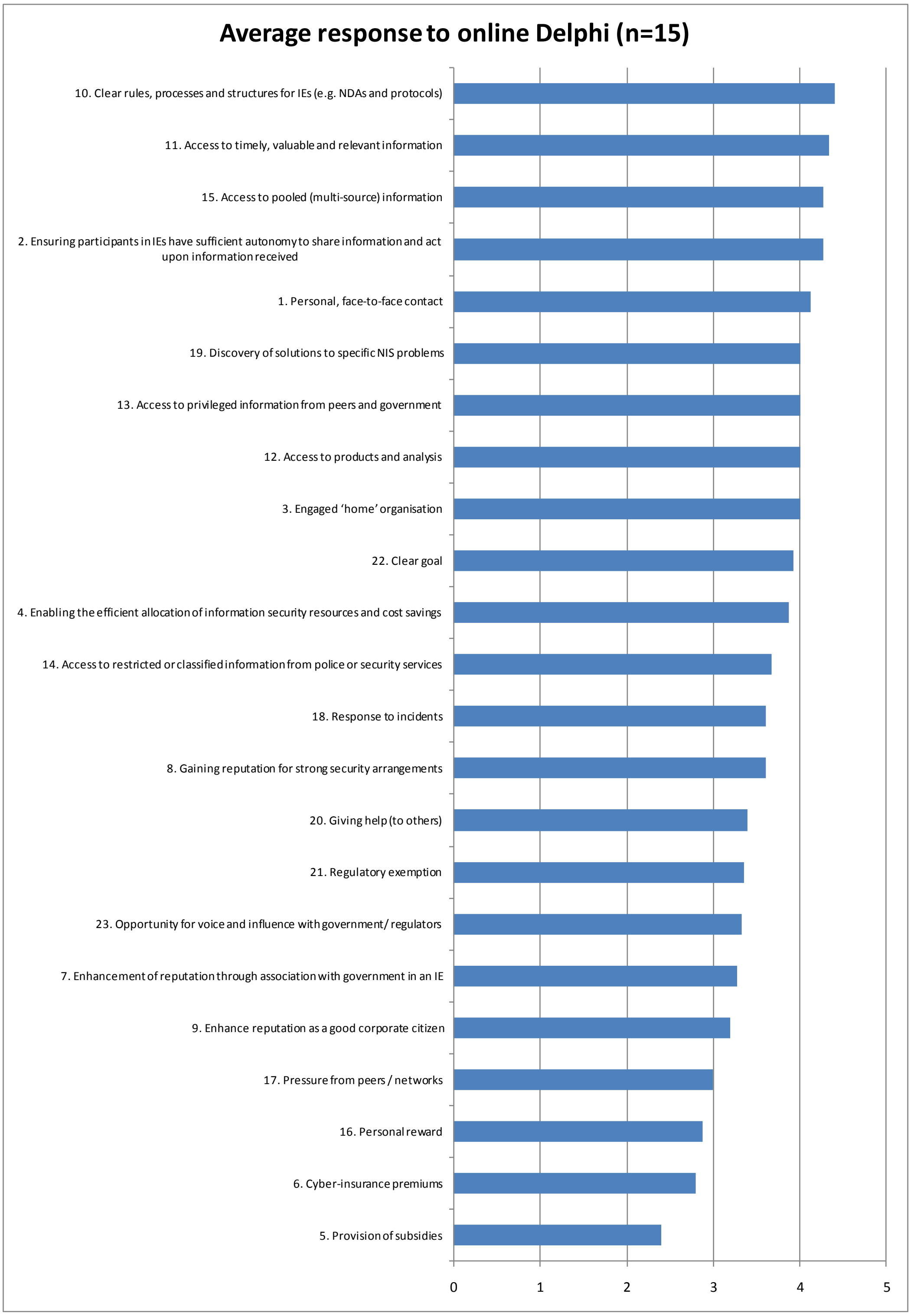


Figure 6: Responses to question 1: From your perspective, what are the most important barriers to information sharing? Results from online survey (Round One)

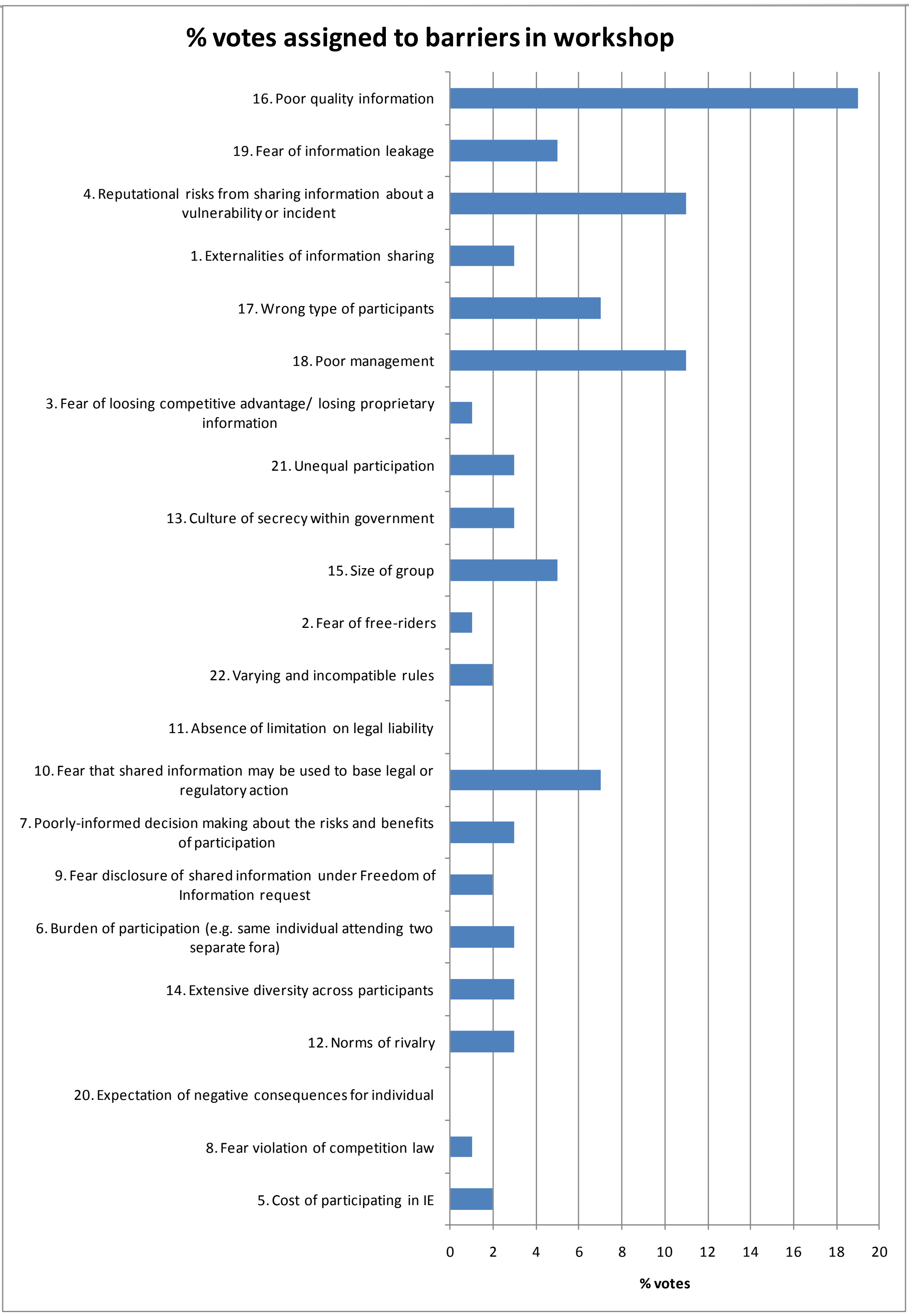


Figure 7: Responses to question 2: From your perspective, what are the most important barriers to information sharing? Results from workshop (Round Two)