ECONOMIC EFFICIENCY OF SECURITY BREACH NOTIFICATION

ANALYSIS AND RECOMMENDATIONS

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of expertise for the European Union (EU), its Member States (MS), the private sector and Europe's citizens. As an EU agency, ENISA's role is to work with these groups to develop advice and recommendations on good practice in information security. The agency assists MS in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. In carrying out its work programme, ENISA seeks to enhance existing expertise in MS by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

Contact details

For contacting ENISA or for general enquiries on the Economics of Security, please use the following details:

Louis Marinos, Senior Expert Risk Analysis & Management

Email: louis.marinos@enisa.europa.eu

Aristidis Psarras, Awareness Raising Officer

Email: aristidis.psarras@enisa.europa.eu

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

table of contents

1. Executive Summary

This work constitutes part of the ENISA Work Programme 2011 in the area of Economics of Security. The purpose of this document is to assess the economic efficiency of security breach notification and to develop recommendations that will help to increase it.

This work is based on the findings of the report 'Economics of Security: Facing the Challenges'. The highest prioritised area of Economics of Security that has been identified by the ENISA Working Group has been taken and further analysed. This area is 'Information Sharing and Notification Schemes'. Thus, this work implements an 'early win' approach that has been decided by the ENISA team and approved by the ENISA management.

The aim of this approach was to use available resources and to analyse the economic aspects of security breach notification, which is predicted to be the most prominent topic on the radar of European and national stakeholders in the near future. To this extent this work is a preparatory contribution to a high-priority topic in the area of Economics of Security.

This work is based on a SWOT analysis carried out after a survey of 19 existing European and international organisations that perform activities in the area of security breach notification – that is, CERTs/CSIRTs, WARPs (Warning Advice and Report Points), Security solution providers and academic institutions. In this report we refer to these organisations as Security Information Exchange Schemes (SIESs). Furthermore, this work sets the parameters characterising the economic efficiency of security breach notification and comes up

with six recommendations for better economic efficiency. In short, these recommendations are:

Recommendation 1: Reflect on the role of security breach notification in the value chain of SIESs, including further guidance of participating organisations. Affected stakeholders are industrial stakeholders with particular emphasis on software and hardware developers, but also SMEs operating ICT infrastructures for their service provisioning, public institutions, banks, etc. Security breach notification will enable these organisations to apply better protection with fewer resources.

Recommendation 2: SIESs should follow a consistent approach in covering all relevant areas of ICT while avoiding overlaps among them. SIESs should try to specialise in various areas of ICT in order to be more efficient in the detection and analysis of breaches/incidents

Recommendation 3: Achieve improvements of efficiency and effectiveness via economies of scale. EU coordination needs to be achieved in order to maximise the data collection and processing required, while collaboration of national actors would be further facilitated. Knowledge about reported breaches needs to be fed back into the processes of all stakeholders involved in the value chain (i.e. SIESs, participating organisations, regulators, national security agencies, etc.)

Recommendation 4: Improve international cooperation to enhance establishment of security breach notification. Having regard to the prominent role of the European Commission in these efforts we see the need for ENISA to further intensify its efforts to support and complement the activities of the European Commission due to its particular competences, expertise and unique position. In particular, it will be important to demonstrate the role of security breach notification in the overall improvement of security and in cost effectiveness.

Recommendation 5: Proposal for improvements in measuring the actual economic impact of the SIES. SIESs have a prime role and interest in the collection of such data that would further support a proper assessment of the efficiency of the entire Security Management life-cycle. Security breach and security incident information is the key element to achieve this goal. This is a major contribution towards cyber security.

Recommendation 6: Elaboration of sustainable measurement instruments. A measuring instrument would help in answering important questions such as ‘when do we have a security breach’, and ‘when does it have to be reported’? There is a need to elaborate on the qualitative and quantitative criteria for measurements and classification practices for security breaches. Such practices could be coordinated at national level by competent authorities or services.

Last but not least, with both the issued recommendations and the developed material, this work can be used to support on-going activities in the areas of CERTs, EISAS, information security exchange, reporting of security breaches and data breach notification at all levels (i.e. ENISA, Commission, Member States and relevant stakeholders).

2. Introduction

In 2010 ENISA updated its stock taking1 of the existing incident management, information sharing and information exchange schemes in the Member States.

This stock taking mainly covered the CERTs and, as described in the document, it aimed to serve as an inventory of CERT activities in Europe that would include publicly listed teams, cooperation, support and standardisation activities.

As a result of this representative work it is useful to highlight three main categories of shared information:

1. Good NIS (National Information Sharing) Practice;
2. Alerts & Warnings;
3. Detection and Information brokerage for a timely analysis of the incident.

Although there are many national initiatives, they do not exist in every Member State and they differ significantly both in scope and depth. Therefore in the context of its mandate and mission, ENISA seeks to provide support to every Member State in reaching an adequate maturity level. In order to complement the national initiatives, the European Commission asked ENISA to produce the EISAS (European Information Sharing and Alert System) Roadmap.[2] The challenges, required activities and timeline for the EISAS project are described in the Roadmap document as well as in the report 'Incentives and Challenges for Information Sharing in the Context of Network and Information Security'.[3]

This document provides guidance in effectively establishing security breach notification that would support the effort to establish a pan-European Information Sharing system.

In this respect it is essential to identify the barriers that need to be overcome in order to establish and deploy security breach notification. Such barriers are thought to include:

1. Poor quality of information;
2. Misaligned economic incentives stemming from reputational risks by sharing information;
3. Poor management and poor facilitation of information sharing.

It is also equally important to note major incentives that would prompt constituents to use such a system and share information. Such incentives would likely include:

1. Economic incentives stemming from cost savings from proactive incident avoidance;

1 Inventory of CERT activities in Europe http://www.enisa.europa.eu/act/cert/background/inv/inventory

2 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

3 http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing

2. Incentives stemming from the quality, value and use of information shared.

Furthermore, the establishment of EISAS-type Security Information Exchange Schemes (SIESs) is already provided for under the current regulatory framework. Article 4 of the Directive 2002/58/EC makes provision for requirements for network service providers to notify their subscribers regarding data breaches. Moreover, in relation to ENISA's report on Data Breach Notifications[4] published in January 2011, it must be highlighted that ENISA's work is complementary to the above-mentioned regulatory framework.

An additional outcome of ENISA's work on the same subject in 2011 was the analysis conducted by the Agency on economic drivers and barriers in a number of areas (including legal, policy, technical and educational aspects). Through this analysis, areas of improvement were identified in order to boost security and resilience in public systems and networks and consequently in relevant products and services. One of these areas is 'Information sharing and notification schemes'. The results of this analysis are described in the ENISA report 'Economics of Security: Facing the Challenges' and they were used as input for the present study. The report's major conclusions in the area of 'information sharing and Notification schemes' are therefore highlighted in this section and prior to the analysis that will follow. Figure 1 serves as a compass for the positioning of the information sharing and notification schemes in the context of the wider economic issues dealt with periodically by ENISA.

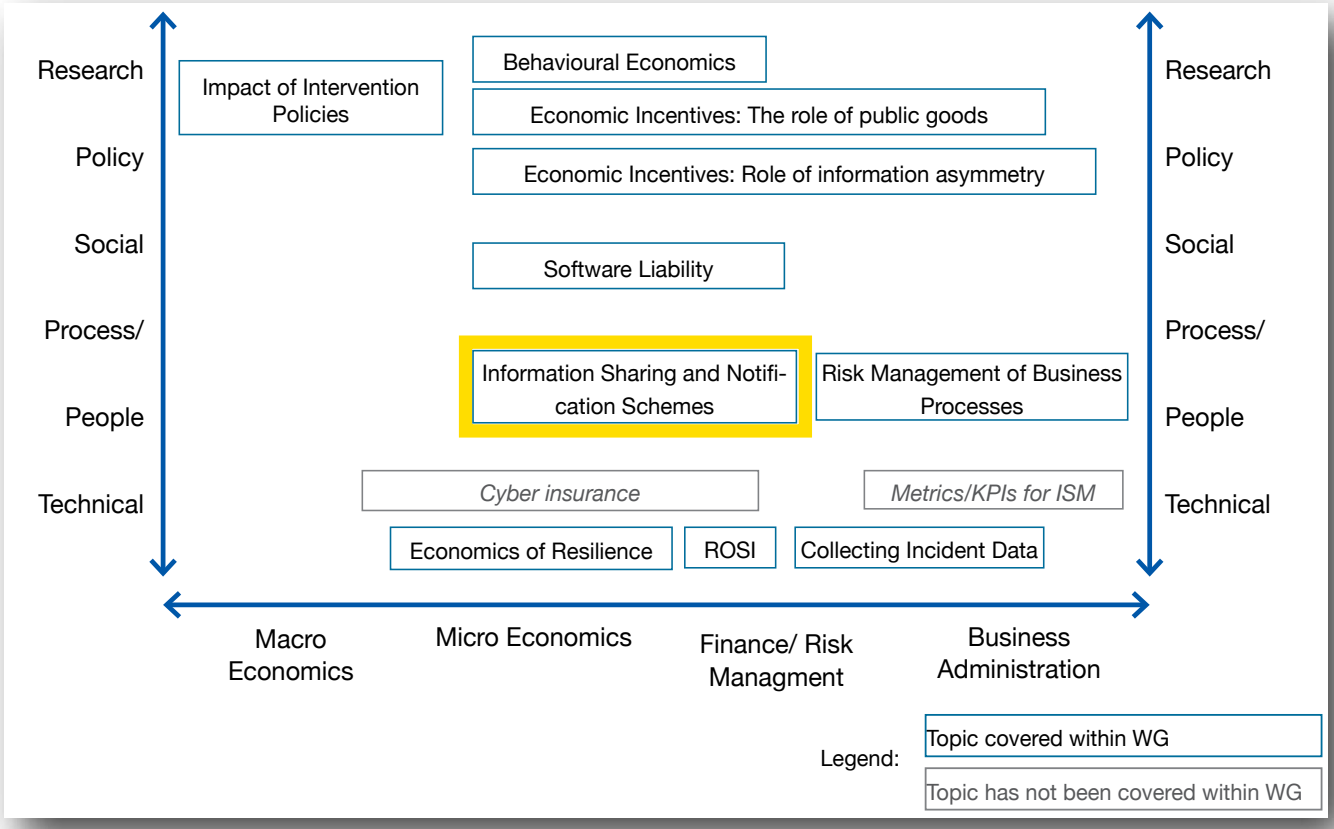


Figure 1: Overview of identified topics of Economics of Security (Source: 'Economics of Security: Facing the Challenges')

4 Data Breach Notification report http://www.enisa.europa.eu/act/it/dbn/

The present report provides information on:

1. Existing security breach notification practices in relevant European organisations;

2. Dynamics of the economic parameters related to the structure and characteristics of information security breach notification;

3. Economic efficiency of existing practices with respect to the current and estimated future demand on such services;

4. Recommendations to relevant actors (decision-makers both at the EU and national level, industry, academia, etc.) on strengthening the economic efficiency of security breach notification schemes. This will be especially useful in the current activities directed towards implementation of Art. 4[5] and the reporting of security incidents according to Art. 13a.[6]

This information should help policy-makers in Europe prepare for adequate policy responses in security breach notification.

5 Recommendations for technical implementation of Art. 4, http://www.enisa.europa.eu/act/it/risks-and-data-breaches/dbn/art4_tech/at_download/fullReport

6 ENISA report on 'Good Practices on Reporting Security Incidents', http://www.enisa.europa.eu/act/res/reporting-incidents/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1/at_download/fullReport

3. Scope

The scope of this study was limited to Security Information Exchange Schemes (SIESs) in the European Union; however, there has been some comparative analysis with schemes in the rest of the world. The types of schemes mentioned in Chapter 5 were within the scope of this report.

The security breach notifications discussed in this document refer to information security. While other types of security breach are of importance and relevance to the regulation, they are not considered within this document.

The term 'security breach notification' is used to indicate the process required to collect, process and communicate information about security breaches. The term 'security breach' describes an event where, due to a security incident, a violation of available security controls has taken place. This might lead to a loss of confidentiality, availability or integrity of data and services.

Hence, the term security breach notification covers activities and information relating to both data breaches and information security incidents. As such, it embraces content that is relevant to Article 4 of the reviewed ePrivacy Directive and Article 13a of the reformed Telecommunications Regulatory Package (Directive 2002/21/EC). This assumption is derived from and is validated by recent ENISA work on Data Breach Notification [7] and Reporting of Security Incidents.[8] The existing dependencies/overlaps are shown in Figure 2.

Looking in more detail at the concept of 'data breach notification',[9] the assumption made is that a data breach can be the result of an information security incident or of loss of user control. In both cases, the steps leading to a notification of the data breach are: detection and assessment, notification, collection of evidence and review and improvement. The view taken is that the data processor could either perform these steps alone or jointly with an external provider (e.g. a CERT) while maintaining responsibility for internal Risk Management procedures.

With regard to the reporting of security incidents,[10] a life cycle model is presented that concentrates on: identification of reporting needs and requirements, engaging in cooperation on the basis of threat communication, setting up of reporting procedures by defining priorities and follow-up processes and managing the reporting scheme by analysing the incidents, keeping statistics and examining feedback loops.

The content-wise overlap of data breach notification and reporting of incidents is evident: the core issue is incident management, together with assessment activities, communication and feedback loops for analysis and improvement. These aspects are included under the heading 'security breach notification', and relate especially

7 Recommendations for technical implementation of Art. 4, http://www.enisa.europa.eu/act/it/risks-and-data-breaches/dbn/art4_tech/at_download/fullReport

8 ENISA report on 'Good Practices on Reporting Security Incidents', http://www.enisa.europa.eu/act/res/reporting-incidents/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1/at_download/fullReport

9 Recommendations for technical implementation of Art. 4, http://www.enisa.europa.eu/act/it/risks-and-data-breaches/dbn/art4_tech/at_download/fullReport

10 ENISA report on 'Good Practices on Reporting Security Incidents', http://www.enisa.europa.eu/act/res/reporting-incidents/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1/at_download/fullReport

to the efficiency of the process: besides the typical incident and assessment activities (as defined in the risk management process), information on the effectiveness of applied controls, based on information from materialised breaches, makes up the core of our assumptions. These dependencies are also depicted in Figure 2 (see box labelled 'Security Breach Notification').

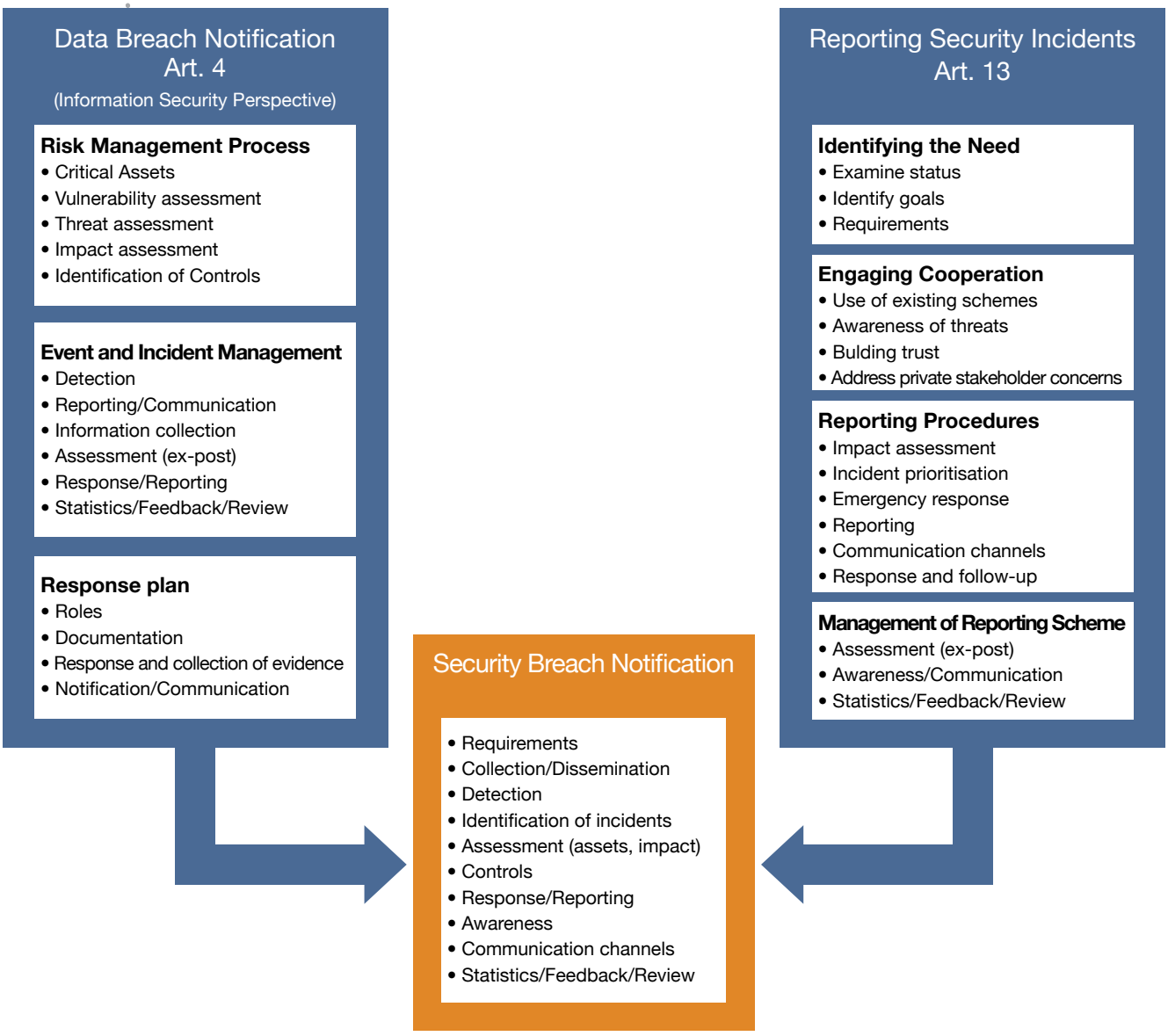


Figure 2: Content of 'security breach notification' as the term is used in this study

4. Methodology

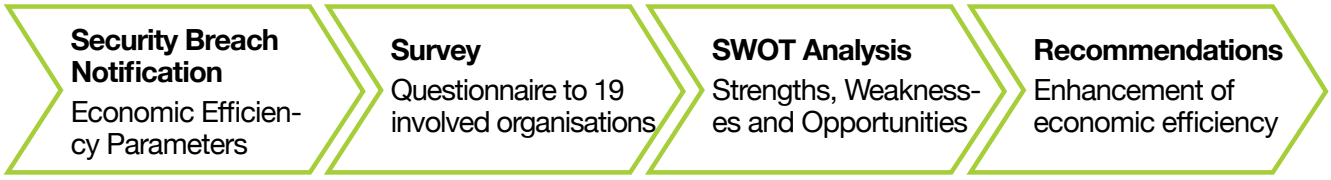
The following topics have been identified in relation to the economic efficiency of security breach notification:

- Requirements
- Collection/Dissemination
- Detection
- Identification of incidents
- Assessment (assets, impact)
- Controls
- Response/Reporting
- Awareness
- Communication channels
- Statistics/Feedback/Review

In fact, these topics appear to be the common elements between 'data breach notification' and 'security incident reporting'. In addition, these topics have been identified as essential parameters to measure efficiency by means of existing good practices applied within relevant organisations (i.e. CERTS, Exchange Schemes, academic institutions). When it comes to measuring economic efficiency, the experiences of **existing** organisations and the **efficiency of their good practices** have been considered particularly crucial to produce reliable results.

In the rest of the document, these topics are referred to as 'Economic Efficiency Parameters'. Because of their importance, they were used to draw up the questionnaire used to survey existing organisations. The process followed within this work is as follows:

Our approach for the survey has focused on:



- **Survey preparation and execution:** A number of preparatory tasks (identifying targets, drafting letter of introduction, drafting survey questions, selecting survey method) that will enable the smooth execution of the survey. The survey included filling in a questionnaire and a follow-up interview with key interlocutors. The respondents were selected on the basis of their geographical location and their domain of activity, with a view to working with a representative sample of security breach notification organisations in Europe.

- **SWOT Analysis and recommendations:** In this step conclusions were drawn on the basis of the survey results (questionnaire and interviews) in reference to the objectives of the study and in support of the formulation of recommendations.

The results of this online survey were analysed and additional information was acquired by follow-up interviews with a carefully selected sample of participants on the basis of their prior experience in the field.

Subsequent to the survey, the dynamics of the economic parameters related to the structure and characteristics of Security Information Exchange Schemes were analysed. This resulted in a list of parameters and elements for economic efficiency of security breach notification that is based on:

- The ENISA report 'Economics of Security: Facing the Challenges'
- The ENISA report 'Good Practices on Reporting Security Incidents'
- The ENISA report 'Implementation of Article 4', and
- ISACA's COBIT[11] (specifically DSS-07).

In particular:

- The economic efficiency parameters for a scheme were mapped to activities that a single organisation needs to perform;
- For each of the economic parameters, elements were identified that contribute to Strengths, Weaknesses, Opportunities or Threats in the SWOT analysis.

More details are presented in Chapter 6.

The survey answers (as well as information derived from the follow-up interviews) were used as input to determine in the SWOT analysis whether a SIES fulfilled the elements related to the parameters.

11 COBIT 5 Process Reference Guide Exposure Draft (2011)

5. Definitions and Stakeholders

We adopted some definitions from the report 'Economics of Security: Facing the Challenges', such as that for economic efficiency (of Security Breach Notification Schemes):

'Economic efficiency means to achieve the best possible level of security for the users of this service, while economising as much as possible on the resources employed and establish[ing] feedback loops.'

In this context, a SIES can be defined as an official plan or programme of actions to facilitate the detection, analysis and sharing of information about security incidents between several entities concerned. For the purposes of this study, we distinguish between several types of **existing** organisations/ stakeholders related to SIESs. The most common such organisations are CERTs and WARPs:

- **Computer Emergency Response Team (CERT):** A 'CERT' is an organisation that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.[12]

As indicated in the ENISA study on CERTs, there are already many active players in this field:

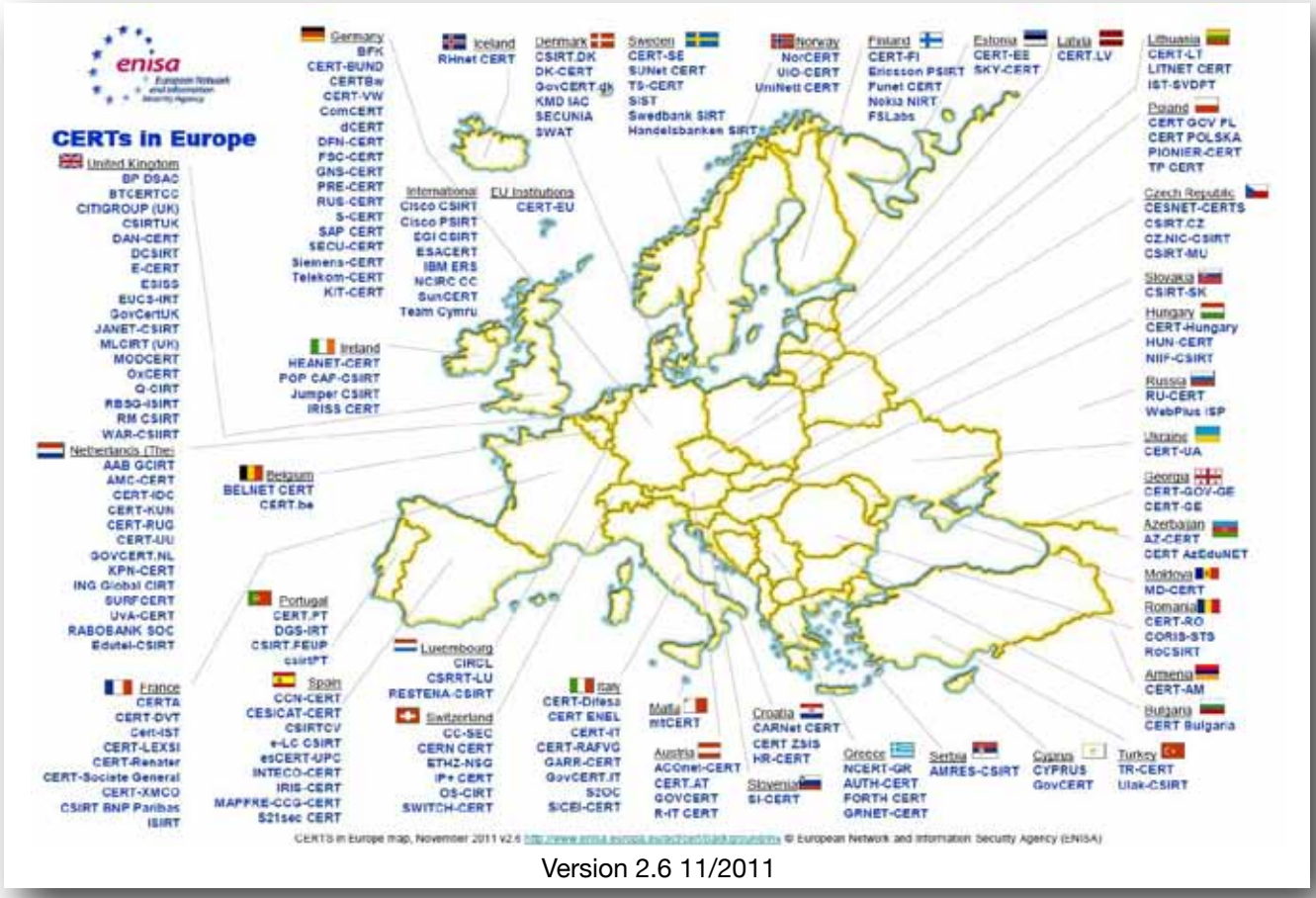


Figure 3: CERTs in Europe (source: ENISA[12])

12 http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe

- **Warning, Advice and Reporting Point (WARP):** WARPs are part of NISCC's information sharing strategy to protect the UK's Critical National Infrastructure from electronic attack. WARPs have been shown to be effective in improving information security by stimulating better communication of alerts and warnings, improving awareness and education, and encouraging incident reporting. Membership of a WARP can also reduce the costs of good security.[12]

There are, however, other types of organisations involved in security breach notification, such as Information Exchange Schemes (IES), Information Sharing and Alert Systems (ISAS) and Networks of Excellence, but the difference between them is very small. It is mainly their origin that differs. In particular:

- **Information Exchange Schemes (IES):** Information Exchange Schemes are typically strategic partnerships between public authorities and key private stakeholders, such as operators of National Critical Infrastructures, to provide them with additional expertise and information to support their information security process.
- **Information Sharing and Alert Systems (ISAS):** ISAS build upon and link together national, public and private initiatives. An EISAS system (European ISAS, as mentioned in the Introduction to this report) could potentially assist the public authorities in the Member States and at EU level in swiftly and properly informing citizens and SMEs on how to contribute, as end users, to their own safety and security.
- **Networks of excellence:** Networks of excellence are designed to strengthen scientific and technological excellence on a particular research topic through the durable integration of the research capacities of the participants. They aim to overcome the fragmentation of European research by gathering:
  - the critical mass of resources and
  - the expertise needed to provide European leadership.

Networks of excellence also have to spread excellence beyond the boundaries of the partnership.

In the present survey we have included CERTS, WARPS (Academic) Networks of Excellence in Incident Response, as well as a commercial provider of Information Sharing and Alert services to critical business sectors.

6. Parameters for economic efficiency of security breach notification schemes

In order to assess the efficiency of security breach notification, parameters influencing the efficiency of Security Information Exchange Schemes were developed.

These parameters can be seen as best practices, activities to take into account in order to increase efficiency and effectiveness of security breach notification with particular focus on economic aspects. To this extent, the parameters presented below represent the issues that we believe to influence economic efficiency. This material is a specialisation of the parameters mentioned in Chapter 3 above and in Figure 2.

We consider this information to be key, both within this report and for the work on Economics of Security. With some adaptations the parameters listed below can be reused as economic efficiency parameters outside the context of a SIES as well. It is worth mentioning that these parameters correspond to the material of the ENISA report 'Economics of Security: Facing the Challenges', which was developed in conjunction with the experts of an ad hoc Working Group.

The key elements are outlined with a view to interpret and assess the findings of the survey, in conjunction with the SWOT analysis presented in Chapter 8.

- **Collection and dissemination of information according to the needs of the organisations participating in the security breach notification**

  The efficiency of the security breach notification is improved when communication channels exist in order for accurate feedback loops to be facilitated. Moreover, information about the security requirements of participating organisations, and the methods used to assess these requirements, is of vital importance for the efficiencies to be achieved. Finally, the underlying intention of the actors responsible for an incident and the impact it may have had on the participants of the SIES has to be an inherent part of the information related to a security breach notification.

- **Assessment of economic perspective when establishing the security breach notification**

  A critical factor in efficient security breach notification is to assess the economic perspective right at the planning stage of the SIES and to take into account all the relevant information in designing and operating the SIES. Such an embedded process would facilitate the efficient deployment of the security breach notification as well as a targeted and effective policy development at the level of both the SIES and the participating organisations.

- **Determination/Assessment of business asset value at risk**

  Determining the business asset value at risk is a decisive factor in

defining whether the security breach notification is efficient in its operation. Depending on the information about vulnerability of assets, an appropriate forecast could be made of the risk and financial model to be applied to the SIES in question.

- **Quantification of costs caused by security incidents**

Quantification of costs is of paramount importance given that information about security incidents alone cannot provide sufficient evidence for decision-making process. In particular, the availability of statistical data regarding the financial and other impacts of security incidents is crucial in assessing the efficiency of the security breach notification and the SIES in general.

- **Focus on both proactive and protective measures/controls while achieving awareness at the level of participating organisations**

Proactive and protective measures at a coordination level should be deemed necessary for all participating organisations in order to achieve an effective security breach notification. In this respect the need for constant and reciprocal awareness between the actors will be catalytic in the effort to achieve the highest possible degree of coordination among the relevant constituents.

- **Statistics on information collected and disseminated about costs, level of reduction of vulnerabilities among participating organisations**

Available and accurate information that would facilitate the quantification of a number of key variables would support an objective evaluation of the deltas between estimates and actual figures by the participating organisations. Measurement of deltas should include elements such as the costs caused by security incidents, the number of affected assets, the increase in availability of critical components and the reductions of system penetrations.

- **Assessment of economic impact and economic return of offered services by means of feedback (for all types of participating organisations)**

Feedback loops are essential between the economic impact and return of the offered services. Such feedback loops should be synchronous in order to allow for the constant alignment of the policies and the cost–benefit evaluation by the participating organisations.

- **Assessment of barriers and benefits provided by SIES**

The assessment of barriers and benefits provided by the SIES is an essential element in order to be able to constantly benchmark their efficiency in terms of outcomes. Therefore a regular uptake of barriers and benefits is important, given that they form an essential element of the cost–benefit analysis.

- **Identification/detection of security incidents having the potential to impact business asset value**

Security incidents should also be measured in terms of the qualitative impact they may have on the business asset value. In this respect issues such as vulnerability of the respective assets, awareness of the underlying trends of the security incident and the profiling of the attacker and his potential motive should be constantly monitored.

- **Quantification of frequency of security incidents potentially impacting asset value**

The frequency of security incidents in conjunction with the possibility of impacting the asset value is essential information. This information provides an indication of the level of significance of the incidents under evaluation and is an important element of statistical information. However, this information is to be considered as merely an indication that needs to be used as an input for a more thorough analysis entailing also other factors such as the likelihood of an incident happening, quantification of the impact, etc.

- **Quantification of effectiveness of identified security controls**

The effectiveness of the identified security controls should be quantified with a view to establishing an adequate metric system that would be used as a benchmark. Indicative variables include the number of affected assets, the increase in the availability of critical components, and the reduction of system penetration. Such a benchmark should be paired in the assessment process with the qualitative factors in order to ensure an accurate outcome.

- **Calculation of ROSI**

ROSI (Return on Security Investment) is a well-known measurement method of economic efficiency. While it was launched many years ago, it remains a key parameter of major importance, mainly due to its soundness and wide acceptance. Many variations have been devised on the primary formula and its use but for many stakeholders, ROSI is always an important point of reference in this useful and dynamic evolution of metrics.

- **Identification and prioritisation of improvement areas for security controls**

As part of the integrated process for the constant development and evolution

of security controls, areas of improvement need to be identified and prioritised. The identification and prioritisation should be done at regular intervals, using criteria suitable to the area of interest under assessment.

- **Collection and brokerage of a broad range of information**

  The information to be assessed in the context of the SIES goes beyond that required for evaluating cost factors alone. A wide range of qualitative and quantitative information must be assessed for the sake of accuracy and cross-referencing. Such broader elements include the collection and brokerage with the Regulators and the users of technical vulnerabilities, collection and brokerage of information on electronic/physical attacks, Infections, malicious code, system malfunction and data breach notifications.

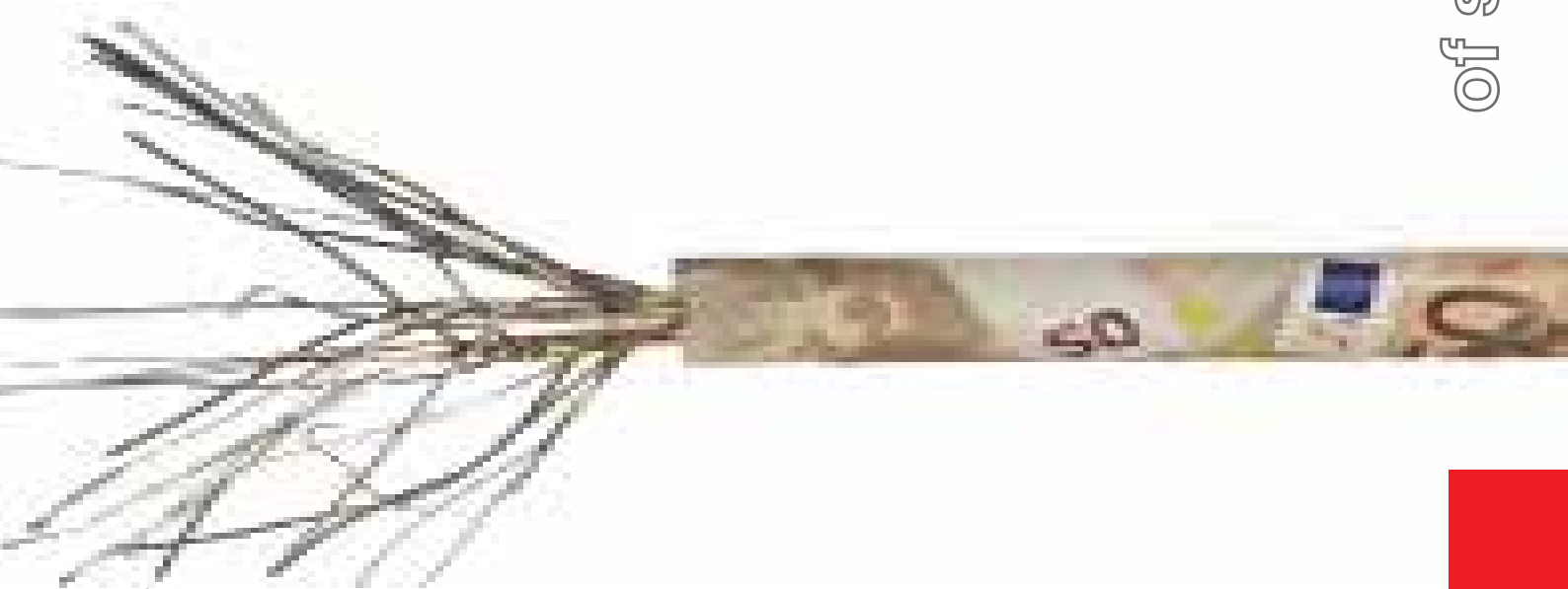
- **Facilitation of recording of incident data and availability of data pool**

  An effective and accurate registry of data related to security breaches should be established by all SIESs and participating organisations. Moreover, a data pool should be set up in order to include information related to security breaches in the monitored components, information regarding assets affected by security breaches, financial impact from security breaches and also information related to the reduction of vulnerabilities in the areas of responsibility of the various constituents.

- **Establishment of benchmarking for good practices**

  Looking towards a meaningful benchmarking, which would provide added value to the stakeholders, we propose considering the benchmarking of best practices. This could be organised and documented by entities that operate as trusted hubs among the Security Breach Notification organisations, e.g. ENISA. Evidently good practices and success stories are being shared between the constituents with greater transparency and accuracy. Therefore such benchmarking would facilitate awareness raising and information sharing between the participating organisations.

A key step in this study was to conduct a survey, in order to collect sufficient information about the security breach notification activities performed by organisations in and outside Europe, their (good) practices, size, cost patterns, etc.



7. The Survey

The results were supplemented with information gathered during follow-up interviews and they were used as input for the SWOT analysis. Even though we sought to, and did, obtain feedback from SIESs outside Europe, such input was primarily used as reference for comparative analysis and to gain a better understanding of the European landscape. Therefore, the recommendations of this report, which are derived largely from the results of the survey, focus on elements that would improve the economic efficiency of European SIESs, and the suggested actions refer mainly to European stakeholders.

In the following paragraphs, the respondents and results are described. The analysis of the results is described in Chapter 8 of this report, using a set of parameters defined in Chapter 6.

7.1 Survey respondents

The survey was completed by 19 participants. Fourteen of these participants were CERTs/CSIRTs, one was a WARP, one was a commercial provider of Information Sharing and Alert and the other three were academic institutions, members of Networks of Excellence in incident response. Most of these organisations were public sector organisations. Only four of them belonged to the private sector. An anonymised overview is depicted in Figure 4.

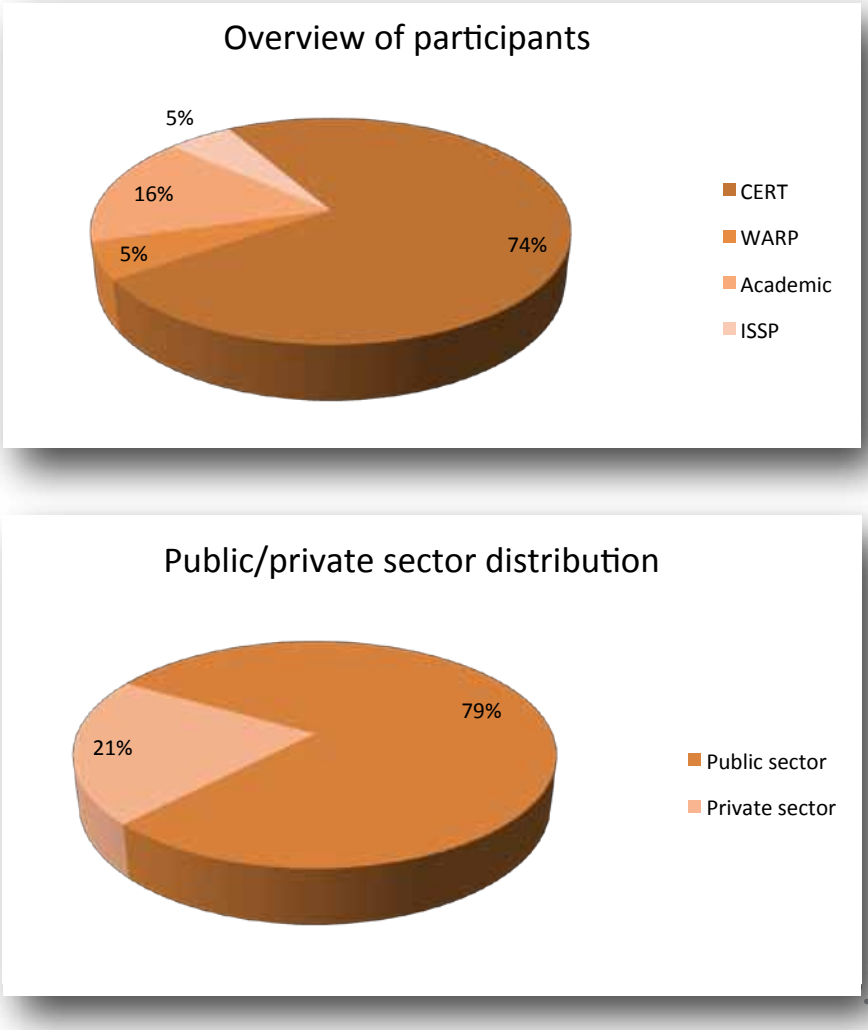


Figure 4: Survey respondents

7.2 Respondents from the following countries successfully answered the survey:

- EU: Greece, UK, Spain, Belgium, France, Luxembourg, Hungary, Romania, Albania, Denmark;
- Non-EU: Albania, Croatia, Serbia, Ukraine, Vietnam, Qatar.

7.3 Results

This section gives an overview of the answers to the survey questions. These results are analysed in Chapter 8 to determine the efficiency of the existing security breach notification practices in view of the current and estimated future demand for such services.

7.3.1 Size of organisation and amount and type of information dealt with

The organisations that participated in this survey vary widely in terms of the financial and human resources allocated annually to their operation, as well as the number of participating members. Although not all organisations were able to provide exact figures, we see that human resources allocated per year vary between and 2 and 25 people, while participating members in the SIES vary between 1 and 200. Finally the number of incidents dealt with per year differs significantly; the maximum is about 3,000 security incidents (not all of them causing a security breach). However, small as well as large organisations deal with a broad range of information, including information related to the incident and eventual breaches.

There is no significant difference in the amount and type of information dealt with by CERT, WARP, ISSP and academic organisations. The type of information dealt with is shown in Figure 5.

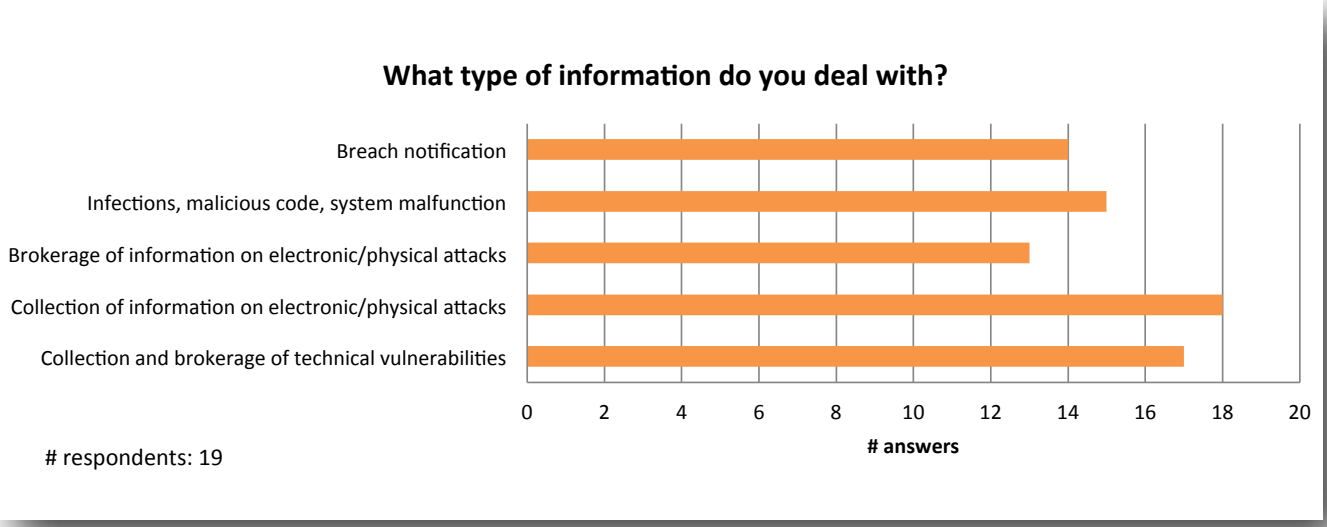


Figure 5: Type of information dealt with

The information that SIESs deal with is often limited to collection and brokerage of technical vulnerabilities and collection of information on electronic/physical attacks:

- In more than 30% of cases, SIESs do not deal with brokerage of information on electronic/physical attacks (i.e. vulnerabilities, threats, impact information).
- In more than 25% of cases, SIESs do not deal with information regarding security breaches (i.e. detection method, forensic information, impact, etc.).
- In more than 20% of cases, SIESs do not deal with information about materialised infections, malicious code and system malfunction.

One respondent indicated that they also deal with monitoring and surveillance of information systems.

7.3.2 Processes related to security breach notification

As mentioned in chapter 3 of this report, stakeholders performing security breach notification cover several actions and processes, which may vary from scheme to scheme depending on their focus and the requirements of participating organisations. We distinguish between six types of actions: prevention, preparation, detection, control, dissemination, and follow-up care.

The results of the survey show that the most important processes, covered by all but one of the respondent SIESs, is dissemination. Preventative actions are also widely undertaken. Preventive actions reduce vulnerability by reducing the chances of an event occurring, and are covered by almost 90% of the SIESs. Disseminative actions to communicate and publish the vulnerabilities identified are covered by almost 95% of the SIESs.

The actions covered by SIESs are, however, often limited to prevention and dissemination. The following actions are not covered on a regular basis:

- Actions to reduce the impact or damage caused by occurrence of an event; for example, training, exercises and back-ups (preparation) are not taken in more than 30% of the SIESs.
- Actions to detect and validate security breaches, incidents and vulnerabilities are not taken in more than 20% of the SIESs.
- Actions that reduce the duration of a malfunction or calamity to a minimum and that support recovery to the ‘normal situation’ as quickly as possible (repression) are not taken in more than 35% of the SIESs.
- Actions related to issues such as financial settlement (follow-up) are not taken by almost 70% of the SIESs.

These results are shown graphically in Figure 6.

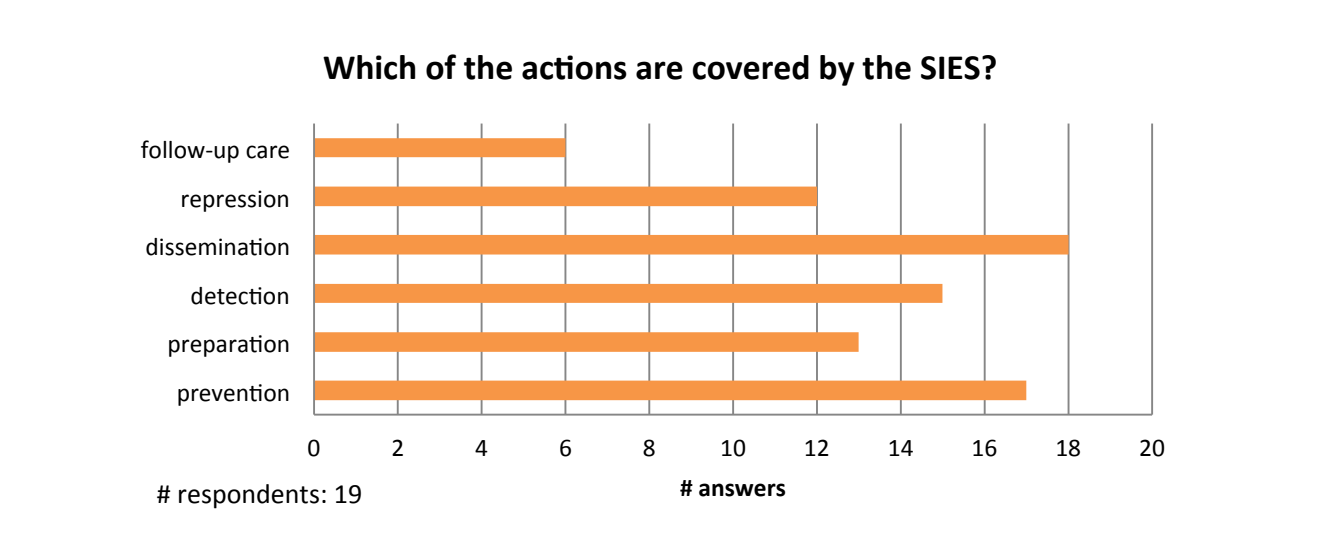


Figure 6: Actions covered by SIESs

In order to perform those actions, data about security incidents and breaches are collected. However, for a considerable number of SIESs, this data collection lacks coverage of important areas:

- More than 40% of the SIESs do not collect data about the underlying intention of security breaches and security incidents.
- More than 35% of the SIESs do not collect data about methods used to assess the vulnerability and existing measures.
- More than 35% of the SIESs do not collect data about the impact of security breaches and security incidents.
- More than 35% of the SIESs do not collect data about interdependency with other security breaches and security incidents or other sectors
- More than 35% of the SIESs do not collect data about the attacker and his potential motive.
- More than 30% of the SIESs do not collect data about the victims of security breaches and incidents.

This can be seen in Figure 7.

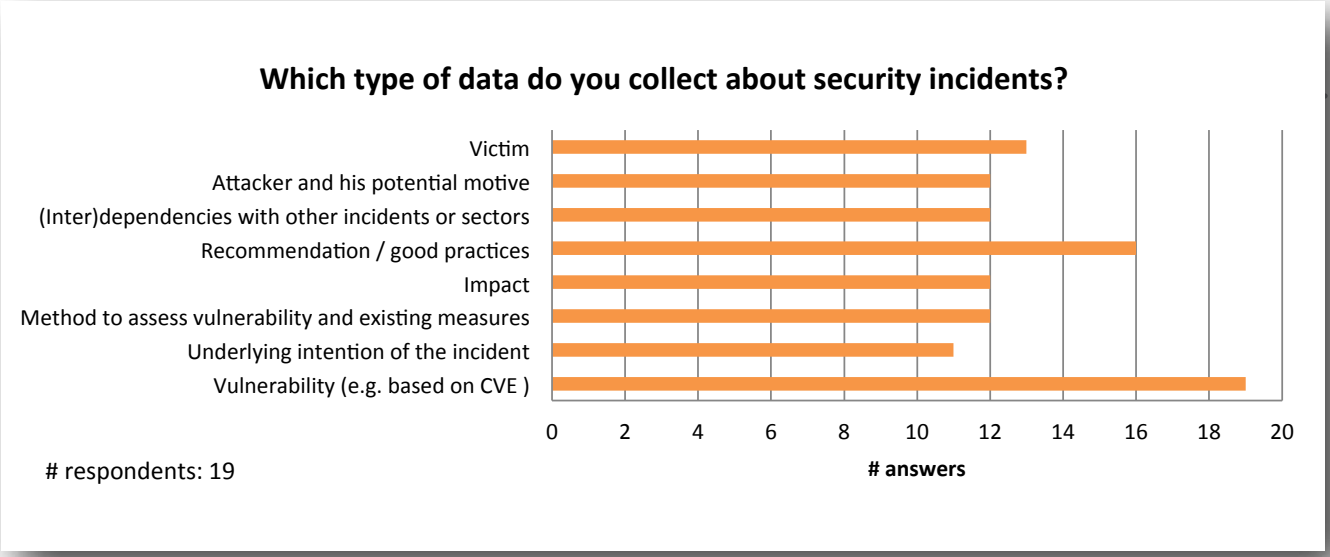


Figure 7: Security incident data collected

Regarding dissemination, the method of interacting with members is an important aspect to consider regarding security breach notification. For most of the SIESs, interaction with other members is not well developed. More than 30% of the SIESs do not exchange documentation and only 10% of the SIESs have a tool for automatic or ad hoc exchange of information. The interaction tools they use are email (100%) face-to-face (36%) and phone (84%). These results are shown in Figure 8.

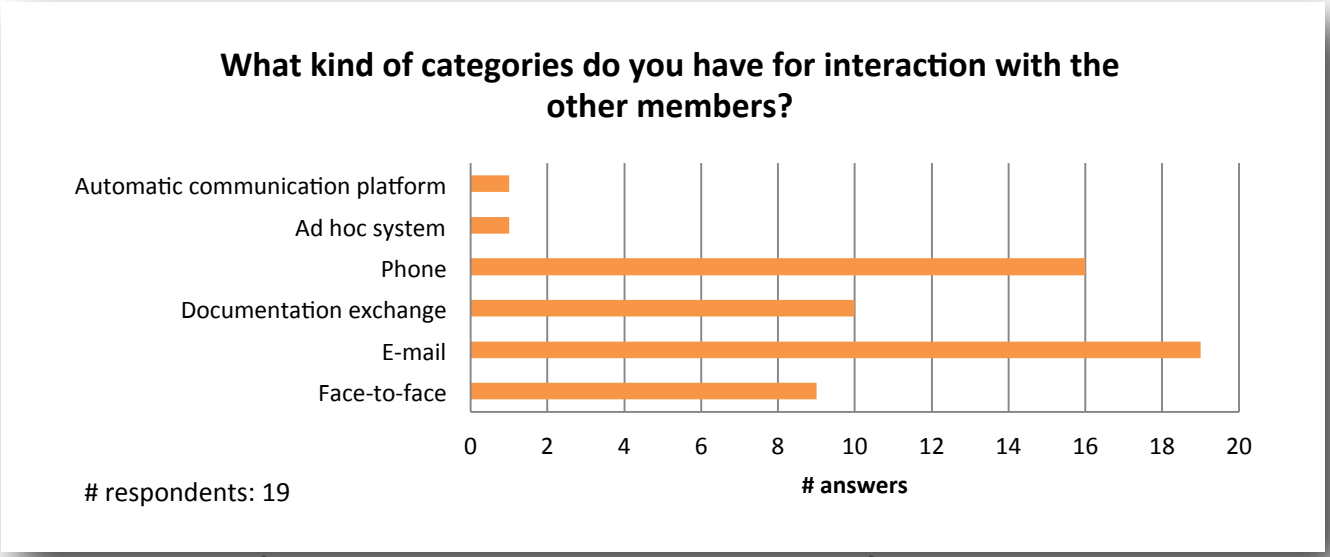


Figure 8: Methods of interacting with other members

7.3.3 Efficiency of security breach notification

As mentioned in Chapter 3 of this report, statistics, feedback and review are activities that should be considered to improve the efficiency of security breach notification.

However, the survey showed that many SIESs are failing to keep statistics on a significant amount of interesting data. The only information that all but one of the SIESs keep statistics about is security incidents in the monitored components. This can be seen in Figure 9.

- More than 40% of the SIESs do not keep statistics about assets affected by security incidents.
- Almost 80% of the SIESs do not keep statistics about the costs caused by security breaches and security incidents.
- More than 60% of the SIESs do not keep statistics about the vulnerabilities in their area of responsibility.
- More than 60% of the SIESs do not keep statistics about the reduction of affected assets; for example reduction of system take-overs and malicious components.
- Almost 80% of the SIESs do not keep statistics about the increase of availability of critical components such as important network components that are parts of communication infrastructure.
- Almost 70% of the SIESs do not keep statistics about the reduction of security breaches and security incidents.

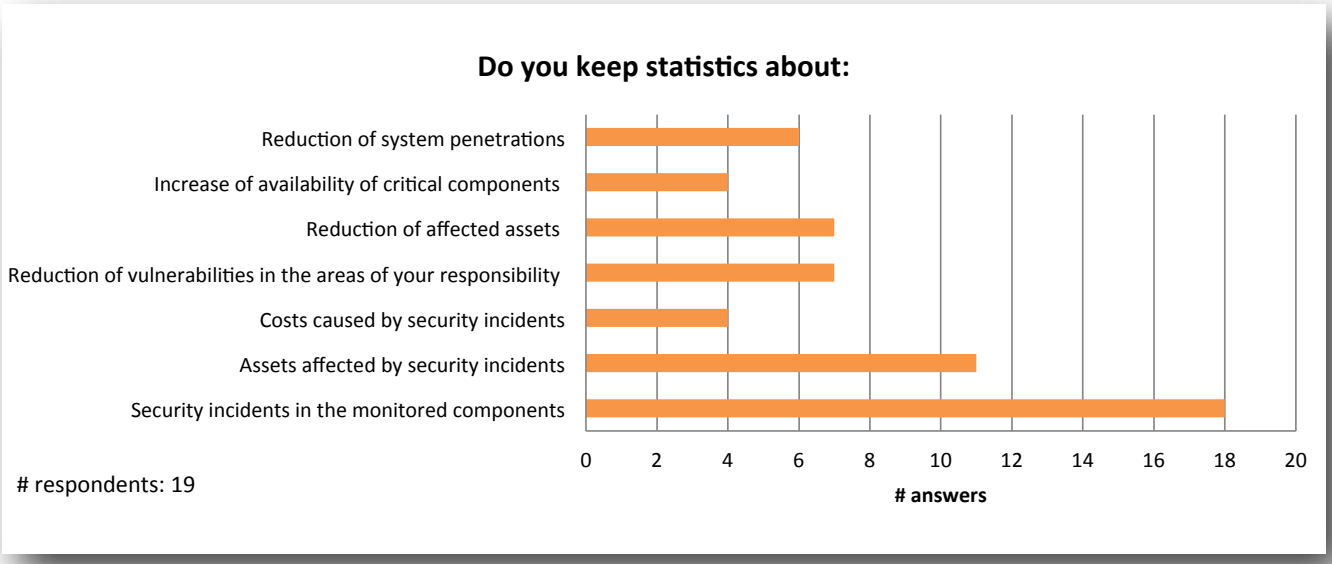


Figure 9: Topics on which data are kept

Another activity that needs to be considered to achieve efficiency is 'Establish feedback loops with all types of stakeholders concerned (e.g. participating organisations, regulation authorities, government agencies, law enforcement agencies).' The level of feedback loops was tested in the survey. Although 90% of the SIESs establish feedback loops with recipients of notifications to measure the effects of notifications, feedback loops with other stakeholders are not frequently found:

- Only 26% of the SIESs establish feedback loops with other SIESs.
- Only 26% of the SIESs establish feedback loops with regulation authorities.
- Only 21% of the SIESs establish feedback loops with national security agencies.
- Only 21% of the SIESs establish feedback loops with government agencies.
- Only 21% of the SIESs establish feedback loops with law enforcement agencies.

These results are shown in Figure 10.

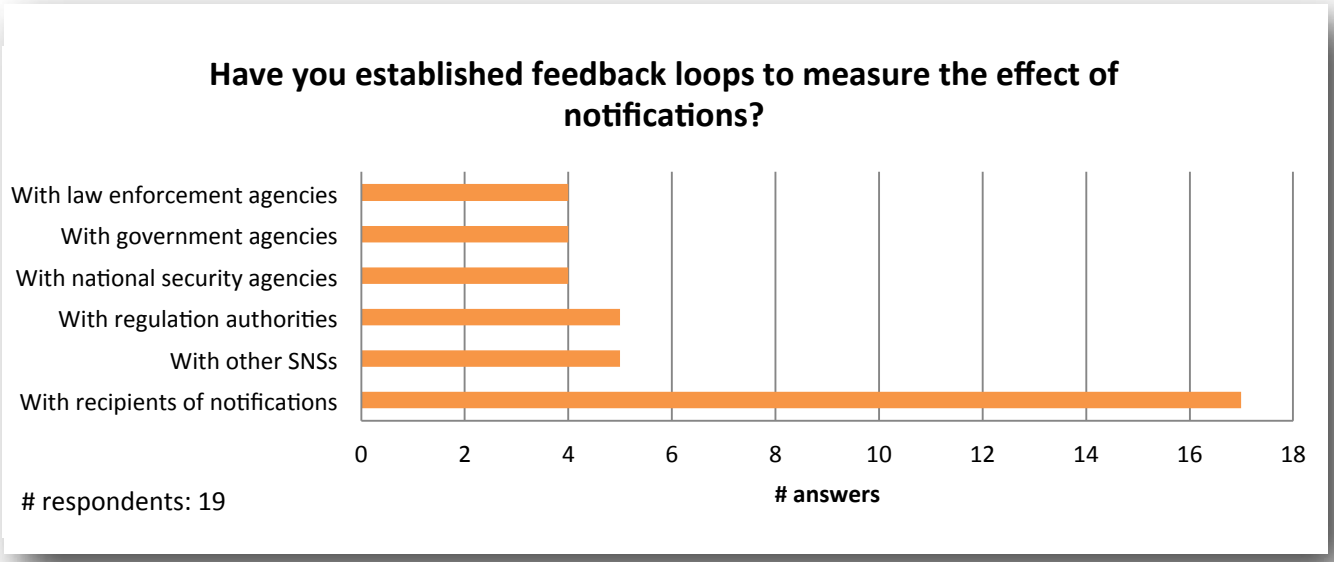


Figure 10: Parties with which feedback loops are kept

Furthermore, the following actions were underlined: 'Take into account the economic perspective when establishing the security breach notification', and 'Take into account the economic impact and economic return of offered services (for all types of participating organisations)'.

In 74% of the SIESs, the economic perspective was not considered during the establishment phase. In only 16% of the SIESs were economic assumptions taken into account prior to the deployment of services. In only 5% were economic assumptions taken into account dynamically to ensure the rightsizing of deployment and to adapt the offered services. In another 5%, the assumptions were validated after the deployment of services. These results are shown in Figure 11.

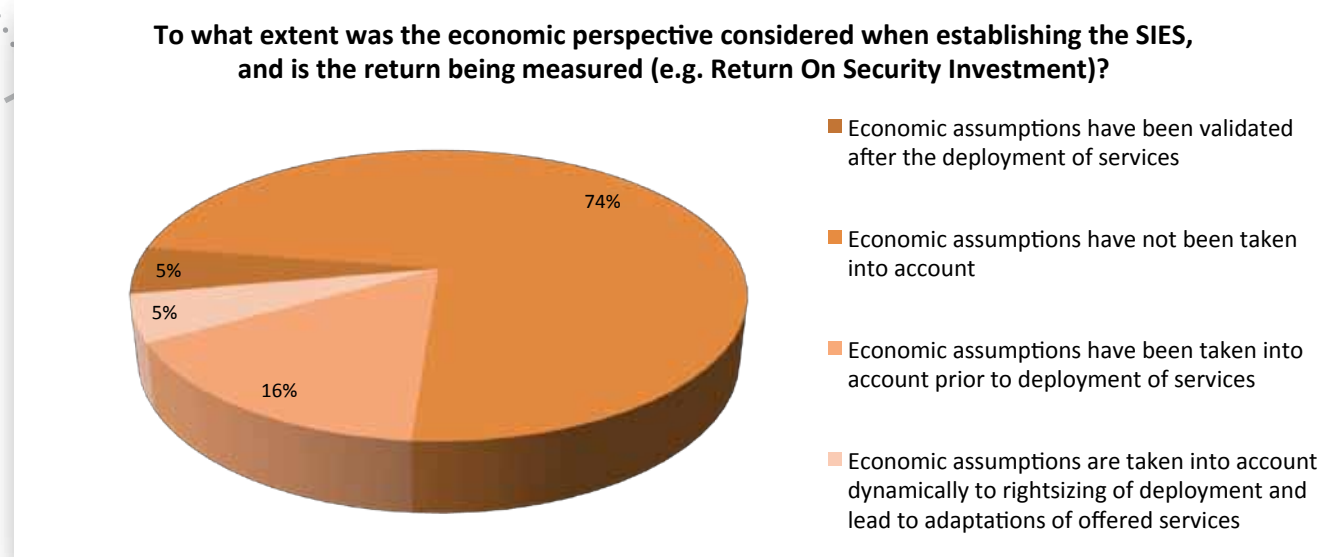


Figure 11: Extent to which economic perspective considered when establishing a SIES

The economic impact or return of services offered was not measured in 79% of the SIESs. Where it was measured, no negative economic impact was identified. In 21% of the SIESs, the economic impact was measured as positive. This can be seen in Figure 12.

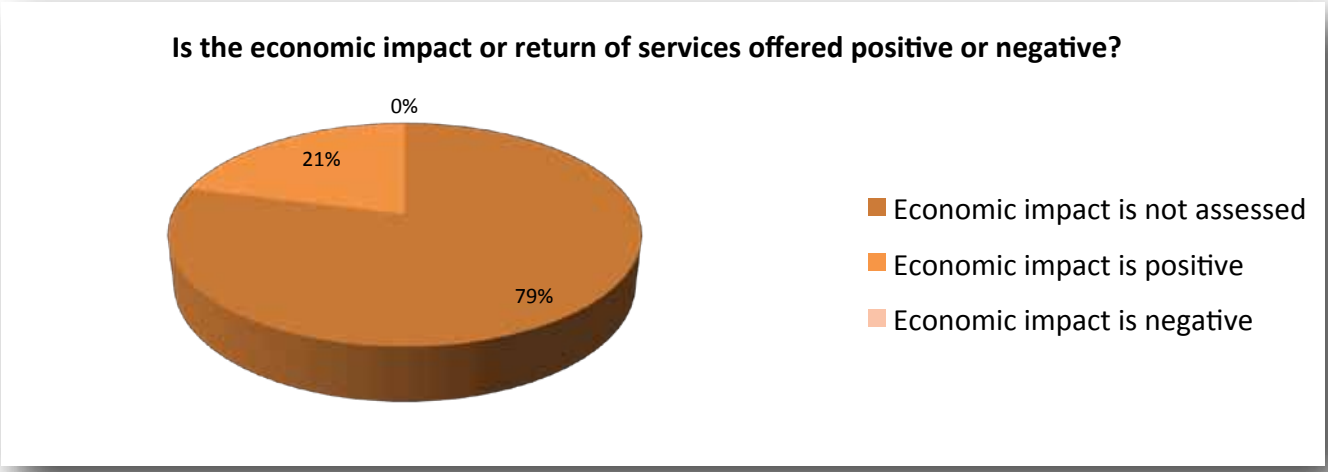


Figure 12: Positive economic impact

Furthermore, as shown in Figure 13, in 68% of the SIESs the economic impact/perspective is not based on feedback (including the notification of security breaches) from notified organisations. Feedback from recipients on breaches and incidents is used in 21% of cases, and feedback from recipients is being validated with a view to be used in the future in 11% of the SIESs.

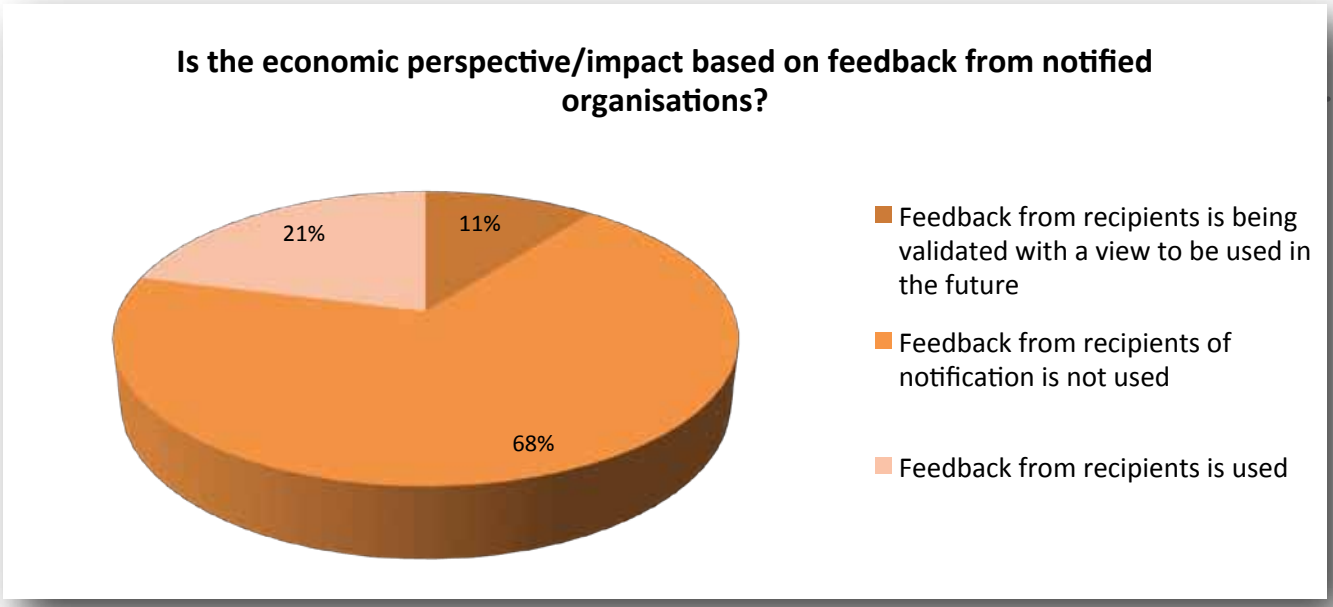


Figure 13: Economic impact based on feedback

7.3.4 Barriers and benefits of information related to security breaches

`Respondents are convinced that SIESs have considerable benefits, such as:

- Quality, value and use of information shared (58%)
- Improved time to react to (or even to anticipate) incidents (89%)
- Potential to influence government policy (and avoid the introduction of misplaced regulation) (26%)
- Discourage cybercrime (42%)
- Creation of awareness about seriousness of security incidents (74%)
- Cost savings (10%)

These results are depicted graphically in Figure 14.

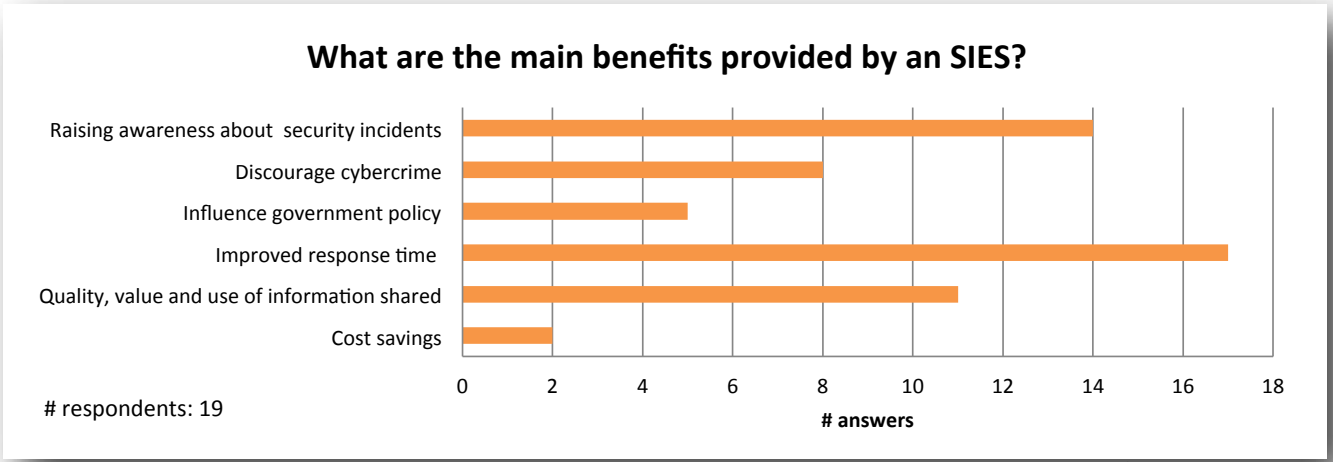


Figure 14: Benefits provided by SIES

The respondents also report some problems, however:

- 10% of the respondents consider market conditions and trust to be a barrier for the SIES
- 36% of the respondents indicate that poor management of SIESs constitutes a barrier to its success
- 47% of the respondents are convinced that regulatory and political factors are a constraint for the SIES
- 20% of the respondents think that technological factors are a constraint for the SIES
- 37% of the respondents indicate privacy concerns as a barrier
- 63% of the respondents indicate social factors such as resistance to use a SIES as a barrier
- 16% of the respondents see misaligned economic incentives stemming from reputational risks as a barrier
- Other barriers identified are trust about the provider and the willingness to cooperate.

These results are shown in Figure 15.

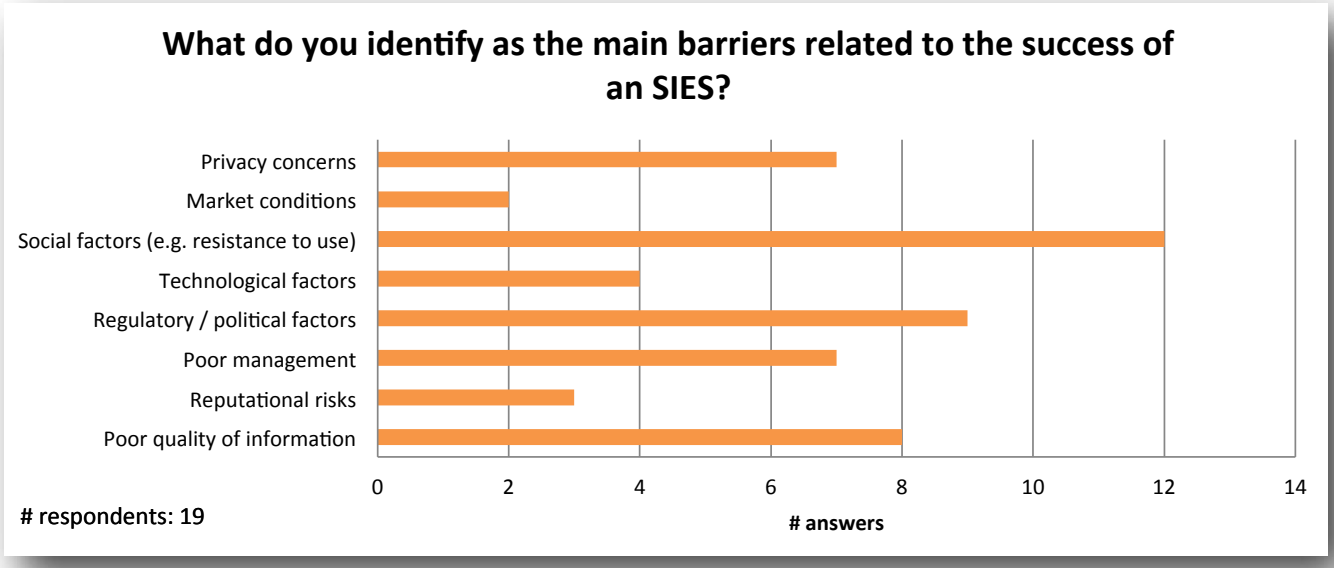


Figure 15: Barriers to SIES success

Respondents identified how they think these barriers can be reduced. The following answers were provided:

- Take appropriate measures (organisational, technical and legislative) in order to pay more attention to, and acknowledge the importance of, the question of cyber security.

- Develop trust. If the source of information is not trusted, the information will never be used.
- Political drive and political players must be willing to change the situation.
- Regulation should understand SIESs and especially the role of CERTs. If needed, exception in law is required.
- A common European legislation and framework are required.
- Education, training and raising of awareness of IT security is required.

Respondents are convinced that participation could be increased by making all SIES services free of charge (84%), by nudging (data assimilation, 26%) or by adjusting the form of notification to the profile of the recipient (37%). One respondent furthermore identified 'Quality of information and demonstration of business value' as a technique to increase participation.

8. SWOT analysis

8.1 Introduction, scope of the analysis

In this chapter, the results of the survey are analysed and conclusions are drawn about the strengths, weaknesses, opportunities and threats. The results of this assessment serve as the basis to for the recommendations in this document on all issues related to security breach notification and the practices currently followed in SIES. To this extent, this chapter elaborates on the 'lessons learned' from the performance characteristics of the SIES that participated in the questionnaire. As such, this chapter comprises the analytic part of this study, while Chapter 9, referring to the recommendations, is the synthetic part of this work.

The performance of a SIES is first of all dependent on the scheme's strengths and weaknesses. These strengths and weaknesses will result from a number of factors – especially the ones that are directly related to security breach notification.

The first two subsections in the SWOT analysis deal with 'Strengths' and 'Weaknesses'. For those two subsections, we first identify the factors influencing the strength or weakness of a SIES with regard to aspects related to security breach notification. After these factors have been identified, the organisations participating in security breach and security incident notification are analysed.

The focal point is not the performance of a particular SIES in terms of every single factor influencing its strength (or weakness) with regard to security breach notification. It is more interesting to understand the performance of the whole set of factors influencing the strength (or weakness) and to compare this performance with the overall performance of all participating actors. This is the starting point for drawing up conclusions/ recommendations leading to more efficient security breach notification, in particular regarding economic factors. In this way, we identified an over-

all state of play for the assessed SIES, with a view to identifying trends and proposing ways to achieve better efficiency. It should be noted that it is advisable to *gradually* enhance average efficiency of notification in general and breach notification in particular. This is due to the borderless nature of information security breach notification: existing SIESs need to jointly increase their efficiency, as the existence of weak links may jeopardise the rest of the community involved in security breach notification.

The last two subsections of the SWOT analysis deal with 'Opportunities' and 'Threats'. These are characteristics of the SIES that are derived from their individual organisation, structure and business models. Opportunities and threats can be conceived as environment variables and, as such, are to some extent beyond the control of the organisations themselves. SIES should, however, try to take advantage of the opportunities and protect themselves against exposure to potential threats.

An overview of the factors influencing the strength or weakness of a security breach notification scheme is presented below. These factors make up the framework for the analysis in this chapter. Furthermore, this information can be used by interested organisations as a benchmark to assess their efficiency even beyond the scope of the present study.

8.2 Strengths

Strengths are characteristics that position SIESs more favourably. We distinguish various factors that strengthen the position of a SIES with regard to security breach notification.

We identified the following factors as strong positive contributors to the economic efficiency of security breach notification:

- *Assessment and brokerage of a broad range of information related to potential breaches (i.e. on vulnerabilities and threats)*, together with the analysis of possible effects on the related assets, is one of the strengths of existing security breach notification. Current SIESs possess large amounts of information in these areas and there are very effective mechanisms in place to collect and disseminate such information to the participating organisations. Examples of such information are:
  - Technical/logical **vulnerabilities of relevant assets:** a weakness that leaves a system open to exploitation, thereby resulting in a risk related to confidentiality, integrity or availability that can potentially be materialised by means of a security breach. An example of a technical vulnerability is buffer overflows that can be exploited by malicious code or known worms/viruses;
  - **Information on physical attacks.** Such attacks include Tempest passive attacks where information is eavesdropped using emissions of electromagnetic radiation (EMR). They also include active attacks where such information is then used in replay scenarios or where EMR pulses are generated to physically disable ICT systems.

- *Quantification of frequency of security incidents potentially impacting asset value.* As depicted in Figure 9, almost all of the responding SIESs in the survey keep statistics about security incidents in the monitored components. By further analysing these statistics, trends can be understood and can help inform the decision-making process on where to involve extra resources, i.e. how to better understand the impact of security breaches resulting in attacks to the infrastructure of participating organisations (see also corresponding weaknesses and recommendations, below);
- *Identification and prioritisation of improvement areas for security controls,* enabled by feedback loops with recipients of security breach and incident notifications. Feedback can be provided on a regular basis or case-driven. Several parties are involved in the feedback mechanism:
  - Law enforcement agencies
  - Government agencies
  - National security agencies
  - Regulation authorities
  - Other SIESs
  - Recipients of security breach notifications

  As demonstrated in Figure 10, the feedback of recipients is commonly used;
- *Establishment of benchmarking based on the assessment of a broad range of information* Benchmarking can help in understanding trends, identifying areas for improvement, suggesting further refinements, sharing experience with proposed solutions, etc.

8.3 Weaknesses

Weaknesses are characteristics that place the scheme at a disadvantage. We identified the following negative issues regarding the efficiency of SIES in relation to security breach notification:

- *Economic impact is not always measured.* The economic impact or return of services offered is not measured in 79% of the organisations involved in the survey. However, measuring the economic impact of a SIES is one key element in the

life cycle of such a service and security breaches are the basis for such measurements. Apart from increasing the acceptance among potential participating organisations, assessing economic impact is a key element in right-sizing the service portfolio of the SIES. Furthermore, measuring economic impact is fundamental for better maturity of the offered security protection;

- *Focus is on dissemination of information, and it is hard for the SIES to reach all involved stakeholders and agents.* However, in the event that a security breach has taken place, the SIES could go further in facilitating the finding and implementation of solutions. By using a layered approach, i.e. the combination of detective as well as preventive controls, the overall security level can be increased. SIES could make use of a proposed repository of information about tools,[13] including the following:
  - Gathering evidence from the information related to the security breach;
  - Investigating existing evidence of a security breach;
  - Developing supportive tools for handling evidence related to security breaches;
  - Supporting participating organisations in system recovery after an incident;
  - Implementing well documented (and eventually standardised) operational procedures;
  - Using detection/audit tools to proactively manage vulnerabilities and prevent security breaches;
- *Lack of specialisation in particular areas of vulnerabilities, threats, assets and controls.* There does not seem to be a consistent approach for defining who covers which types of security breaches. Instead of having many SIESs coping with a wide range of information, it might be more efficient to have SIESs with specialised capabilities towards specific kinds of security breaches. The following weakness is a consequence of this one.

13 http://www.enisa.europa.eu/act/cert/support/chiht

- *There seems to be an overlap in the coverage of different SIESs.* The overlap needs to be analysed, discussed and negotiated to find a compromise. This topic has also been identified in the ENISA report 'Good Practice Guide for Incident Management'[14];
- *Need to improve management of SIESs.* Besides the survey answers (see Figure 15), we have assessed this weakness as a combination of a variety of factors, such as the need for improvements in the service provision (see weaknesses above), potential to enhance communication with participating organisations, need to enhance statistics – just to mention the more important ones. All these factors point to a lower maturity of SIESs with regard to management of security breaches, thus implying that better management should be in place. The same conclusion, albeit under slightly different working assumptions, was also drawn in the ENISA report 'Incentives and Challenges for Information Sharing in the Context of Network and Information Security'.[15]
- *Need to intensify exchange of information.* Exchanging information among SIESs themselves, among SIESs and participating organisations and also among participating organisations themselves seems to be a measure that will increase efficiency. This is because of the variations in the maturity levels of all these players. An information exchange is seen as a measure to identify gaps, to exchange good practices and share information about all kinds of controls needed to mitigate identified and materialised risks.
- *Need to broaden the use of statistics with incident information from participating organisations (including information on security breaches).* The use of statistics from security breaches and their consequences is fundamental for the evaluation of the efficiency of controls used. Besides improvement of feedback loops, the need to include breach notification has been identified, especially because companies as well as public entities are particularly reluctant to publish this data. Eventually, notifications from organisations on security breaches and incidents and their effects need to broaden in order to cover the ones that are outside the circle of those connected to a particular SIES. On the other hand, this information needs to be fed to an as-

14 http://www.enisa.europa.eu/act/cert/support/incident-management

15 http://www.enisa.europa.eu/media/news-items/enisa-analyses-the-incentives-and-challenges-to-public-2013-private-information-sharing

sessment process in order to identify precisely the causes and effects of incidents (see also weaknesses above).

Now that we have identified the factors influencing the strength or weakness of SIESs, we give an overview of the opportunities and threats that they face. Opportunities are external chances to improve performance of the scheme. Threats are external elements in the environment that could endanger the scheme.

8.4 Opportunities

Opportunities offer possibilities for existing SIESs to capitalise on their capabilities in order to improve the efficiency of all aspects related to security breaches. The assessed opportunities have been extracted from available effectiveness parameters (see Chapter 4) extrapolated with a view to using them more effectively in order to fulfil upcoming market trends:

- *Improve awareness towards larger user communities and wider spectrum of ICT devices and services.* The further proliferation of smart devices and the 'IOT – Internet of Things' means ICT will be embedded in even more business processes as well as products such as end-consumer devices, both simple and complex (e.g. from low end processing capability tokens up to household devices and cars). The go-live of Galileo, for example, will spur a range of new applications and devices. Some of these are already taking shape, e.g. the next generation of EU digital tachograph and the EETS (European Electronic Tolling System, i.e. road pricing). For this kind of ICT application, the notification of security breaches will be of key importance and has to be communicated to end users.

- *Integrate better into various Member States/EU initiatives.* The arrival of Stuxnet and its successors such as DuQu has demonstrated that threats can indeed have a serious impact on critical infrastructure and might become issues of national security. SIESs should be lined up with various national and international CIP (Critical Infrastructure Protection) initiatives in the Member States. Again, security breach notification has to be part of the strategies/approaches developed in all areas and particularly in critical infrastructures and services.

- *Based on existing experience, achieve greater influence on government policy regarding security breach notification.* By building up valuable expertise through proper analysis of security breaches and actions to be taken, the SIESs can share their knowledge with regulators and other relevant national bodies to ensure that policies and regulations are aligned with the actual threat situation.

- *SIESs should take advantage of favourable market conditions to continue their growth.* Market conditions are favourable for the growth of SIESs, in particular regarding information security and breach/incident management. The growth needs to be aligned to a number of economic challenges which make it even more important that investments follow today's market trends (see also economic challenges in the report 'Economics of Security: Facing the Challenges'[16]).

8.5 Threats

Threats are events or situations with the potential to jeopardise the operations of SIESs and thus adversely affect security breach notification.

We identified the following threats to the overall EU situation that relate to security breach notification and posture of SIES:

- *Failure to generate economics of scale.* SIESs targeting closed user groups such as Financial Services work well but only within their own community. In such organisations, security breach notification has good penetration.[17] Given the current financial crisis, such a specialised approach might not be economically efficient in the long term. SIESs should therefore try to obtain good coverage within their sectors/specialty in order to generate economies of scale and secure their long-term existence.
- *Excessive dependence on knowledge outside the EU.* As many of the ICT providers and the dedicated security solution providers are US-based and given that emerging economies play a significant role in ICT, Europe needs to be vigilant to build up and maintain its own independent knowledge tanks in detection, incident management and response capabilities.
- *Underestimation of potential threats to vital ICT components.* Experience from the last decade or so has revealed the catastrophic impact of events that were considered to be of low probability (e.g. 9/11, Fukushima, cyber-attacks in the EU, cyber fraud etc.). Cyber incidents, e.g. in CIP, for which risk mitigation strategies were either suboptimal or underlying risks have been accepted, may

16 Link to the EoS Working Group report to be added upon availability.

17 Aftermath of a Data Breach Study, January 2012, http://www.google.co.uk/url?sa=t&rct=j&q=aftermath%20of%20a%20data%20breach%20study&source=web&cd=2&ved=0CEMQFjAB&url=http%3A%2F%2Fwww.experian.com%2Fassets%2Fdata-breach%2Fbrochures%2Fponemon-aftermath-study.pdf&ei=HuEvT_WjBpKk0AXg7diuCA&usg=AFQjCNG85-ZboAopv3itZc-8Ewqb2GAI4w

have increasingly strong impacts. Security breach notification requirements have to be applied to a wider range of ICT components, especially those related to CI, as they play an important role for cyber-security.

- *Poor balance between privacy and security prevention legislation might affect efficiency of response.* Too tight (privacy) regulations may cause the schemes to operate in a less efficient way. If critical information may not be shared, this will make it more difficult for the relevant entities to respond to security breaches and to properly assess their impact. Misaligned privacy and security regulations may lead to inadequate implementation of security controls.
- *Misaligned incentives among SIES themselves and among participating organisations to share security breach and incident related information.* It is currently considered more interesting to take advantage of the benefits of using the information shared in a scheme, than to contribute to the sharing scheme with information emanating from own security breaches and incidents. It takes an effort to communicate the right information and some members may be reluctant to share information due to privacy concerns. The current situation of information sharing can thus be characterised as 'asymmetric' (i.e. trying to profit from experience of others while keeping own contribution as low as possible).
- *Aversion of potential users to use available capabilities.* Economic, social and privacy factors may reduce the impact of the security breach notification. Creating awareness is an important factor to help overcoming these matters.

9. Recommendations

Based on the results of the survey, we conclude this report with some recommendations to make Security Information Exchange Schemes (SIESs) more successful in the implementation of security breach notification.

However, before listing the recommendations, we would like to stress that SIESs **should capitalise on the four opportunities identified and in presented in the SWOT analysis above** (see section 8.4). We see these opportunities as a first step towards increasing efficiency and effectiveness. In this section, for each recommendation we also discuss the stakeholders that are primarily concerned with the actions that need to be undertaken. These stakeholders are also listed in Table 1.

Recommendation	Key Stakeholders					
	SIES	Regulators	EU Commission	ENISA	PPP	Industry
1. Improve value chain	X				X	X
2. Consistency	X	X			X	
3. Economies of scale	X		X			
4. Improve international cooperation			X	X		
5. Improve actual econ. impact	X			X		
6. Sustainable measurement	X	X				

Table 1: Recommendations by key stakeholders involved

Recommendation 1: Role of security breach notification in the value chain of the SIES, including further guidance for participating organisations

We recommend reflecting on the scope of the target value chain of the SIES. Being informed of security breaches is highly valuable in itself; however, it has been observed that in practice many organisations would benefit from help in restoring the 'back to normal' situation. If an organisation is aware that there is a computer virus outbreak, prevention can help to limit the infection. However, if some computers nevertheless fall victim to the virus and are, for example, caught in a botnet, what is required is a tool that allows recovering from damage and thus hindering other collateral, even more severe, security breaches.

This implies, that SIESs and participating organisations need to enter into a dialogue/cooperation that allows them to quickly identify weaknesses and effects of a possible security breach or incident; issues such as level of exposure to a threat, vulnerabilities, controls used, impacts from materialised threats, etc., need to be elaborated both by SIESs and the respective participating organisation.

In order to enable the partners involved to obtain this material, an approach needs to be developed that includes both ex-ante and ex-post activities. Initially an identification of risks, the protected assets, the implemented controls, the threats to be

encountered and the potential impact of security breaches has to take place. After the security breach an analysis has to be performed of the impact, of the threat materialisation, of the recovery options and replacement. In order to do all this, knowledge transfer between the SIES and the owner of the infrastructure has to take place. It will also be necessary to involve service providers that could facilitate this transfer.

Such an approach would help in:

- Justifying the organisations' investments in ICT security preparedness;
- Preparing for the worst, including back-up preparation/test and reinstallation from trusted media as well as risk awareness raising;
- Performing a risk analysis of the organisation's responsibilities and liabilities from the legal perspective;
- Gathering evidence prior to a security breach;
- Gathering evidence on breach-related information;
- Gathering evidence and providing guidance on tools to support involved parties;
- Implementing restore and 'back to normal' operations by recovering from the security breach;
- Performing post-factum analysis and law enforcement interaction.

Given the variety of players involved in such processing of security breaches, we consider public–private partnerships as an instrument to address this issue. At the same time, an agreed approach to risk management, information sharing and coordination of actions in case of incidents needs to be developed.

Stakeholders: It is considered that the **industry** stakeholders with particular emphasis on software and hardware developers are primarily concerned with the actions to be taken. In this context an initiative could be encouraged by any of these parties, given their in-depth knowledge and experience in the field. **SIESs** should develop corresponding services for both protection and support of participants before and after the notification of a security breach.

Recommendation 2: SIESs should follow a consistent approach in covering all relevant areas of ICT

As the field of ICT security aspects will only continue to grow, from the point of view of both technology and service availability, and as countries, regions and organisations tend to differentiate and specialise, we recommend establishing a SIES ap-

proach that would ensure that all relevant topics are addressed. Such an approach would increase the efficiency of the EU-wide SIESs, as it would create sector and technology specialties.

We recommend establishing an approach that distinguishes between upstream, core and downstream aspects regarding the management of security incidents and security breaches:

- Upstream aspects include monitoring the activities that could lead to security breaches and security incidents. These include monitoring Internet fora for malware, viruses, botnet, credit card numbers, etc. These fora give insight in what might be the next generation of attack vectors (i.e. emerging trends).
- Core aspects include real-time sensing, data capturing and extraction, filtering and analysis. Own core capabilities should be enriched by international information exchange and cooperation.
- Downstream activities should then disseminate the information collected, filtered, and enriched during the core processing of the security breaches notified.

This information should be made available in a format that is structured according to the life-cycle of a SIES. Combined with the previous recommendation (recommendation 1), this approach would boost the effectiveness of the SIES, while reducing duplication of work at various levels of the SIES value chain. Such an approach would help advance sector and national risk management and preparedness capabilities.[18]

Stakeholders: The above recommendation entails an activity that requires deep knowledge in terms of content but a wider effort in terms of coordination. Therefore it is one of the recommendations that would best be served by standardisation or by a **public–private partnership** scheme. In addition, in order to ensure that such an initiative would materialise, it is recommended that the PPP originates from **national competent authorities.**

Recommendation 3: Improvements in efficiency and effectiveness via economies of scale

Information sharing and data collection is positively influenced by economies of scale. These economies of scale can be achieved by increasing the number of participating members, but also by improved sharing of information between SIESs. Taking into consideration the prevailing landscape in the European Union, we recommend a model that is distributed in nature but well coordinated, rather than an overly centralised model that will have difficulty in accommodating regional and cultural diversity in maturity of approaches, technology use and service provisioning.

In order to achieve efficient but also effective coordination regimes, it is necessary to initiate a dialogue for unifying approaches followed by various SIESs (see

18 "http://www.enisa.europa.eu/act/rm/files/deliverables/WG%202010%20NRMP/view

also recommendation 2). This includes agreed information collection and dissemination processes, information sharing practices, approaches to identify, understand and monitor the needs of participating organisations, dialogue to national and international bodies, models of public private partnerships, etc.

Stakeholders: The ability to improve efficiency and effectiveness via economies of scale requires continuous collection of accurate data via the actors involved. Such data concern vulnerabilities, threat exposure, intrusion detection, incidents and breaches. They should be gathered by the **established SIESs** and other relevant undertakings with the support of participating organisations. EU coordination needs to be achieved in this area in order to maximise the data collection and the respective processing. An active role for the European Commission would enhance the EU-wide coordination required.

Recommendation 4: Improve international cooperation to improve security breach notification

In a world where both national and international economies are interdependent, a reliable global information sharing infrastructure does make sense. Countries face common threats, and defence should be well organised, even across borders. As resources are and will always be limited, cooperation should be sought across borders with organisations such as the US IT-ISAC (Information Technology – Information Sharing and Analysis Centre). International SIESs' cooperation should capitalise on information that is globally available, and filter EU-relevant information. It should also make sure that important sources of information, such as from OWASP, are factored in. In this case particularly the annually updated OWASP Top 10,[19] the OWASP Mobile Top 10 risks,[20] the SANS Top Se-

19 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

20 https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks

curity Risks[21] and the suggested countermeasures should be included in the EU SIESs' /EISAS framework. Similar information from other players should be consolidated, validated and put at the disposal of interested stakeholders. ENISA foresees relevant work via its 2012 Work Programme and in particular within the Work Stream 1: Emerging Risks. As security breach and incident notifications are already part of existing SIES practices, their role has to be transposed to all relevant areas of application.

Stakeholders: The above recommendation is considered to be instrumental in the effort to deploy security breach notification and raise the level of information security preparedness in Europe. The need for the EU and in particular ENISA to further intensify its efforts to support and complement the activities of the **European Commission** becomes apparent. In the area of security breach notification in particular **ENISA** is in a unique position to propose possible approaches, due to its particular competences and expertise.

Recommendation 5: Improvements in measuring the actual economic impact of the SIESs

Continuous improvement of the SIESs can be stimulated by measuring the economic impact of the scheme. Organisations that do not measure their own return on services do not know how they are performing. Those organisations that do measure their own return on services will be aware of the economic impact and, as such, they are in a better position to adapt their activities in order to increase efficiency.

The results in the survey have shown that only a minority of SIESs measure their economic impact. We observed in the survey that at present, measuring the economic impact is not a common practice for SIESs. We recommend including this more explicitly in the future.

21 *http://www.sans.org/top-cyber-security-risks/

We recommend capturing leading and lagging indicators. By 'leading' we mean the quantification of investments made in SIESs, in terms of Capital Expenditures (CapEx) and Operational Expenditure (OpEx), as well as the level of commitment attributed.

By 'lagging' we mean the reporting of security breaches and incidents through police and law enforcement (e.g. Europol and Member State Cybercrime police departments). Information on both actual losses as well as operational law enforcement cost should be obtained from these bodies.

We believe that by considering the proposals of recommendations 1, and 3, issues of leading and lagging indicators can be effectively addressed.

An additional issue that is worth noting with regard to this recommendation is that SIESs and their participating organisations should use/enforce externalisation controls; that is, externalise the impacts for a number of risks. Major instruments for this purpose are insurance policies. Information on payments made through insurance claims should be taken into account when trying to increase economic efficiency (while some insurance companies have long been active in cyber insurance, this control is not widely used). Finally, the Eurostat statistics on Information Society could be expanded to include measurements on losses with regard to security incidents by including data from data breach notification, when available.

Stakeholders: Many stakeholders see economic impact as a factor isolated from other relevant considerations, which may explain why so little attention has been paid so far to the measurement of economic impact. Such a perception might be misleading, however. In the absence of such a measurement we are not in a position to establish the efficiency of such schemes. Therefore the **SIESs** have a prime role and interest in the collection of security breach information that would further support a proper assessment of effectiveness in due consideration of the efficiency variables. Moreover we see the need for EU-wide coordination on the matter; **ENISA** would be capable of doing this.

Recommendation 6: Elaboration of sustainable measurement instruments

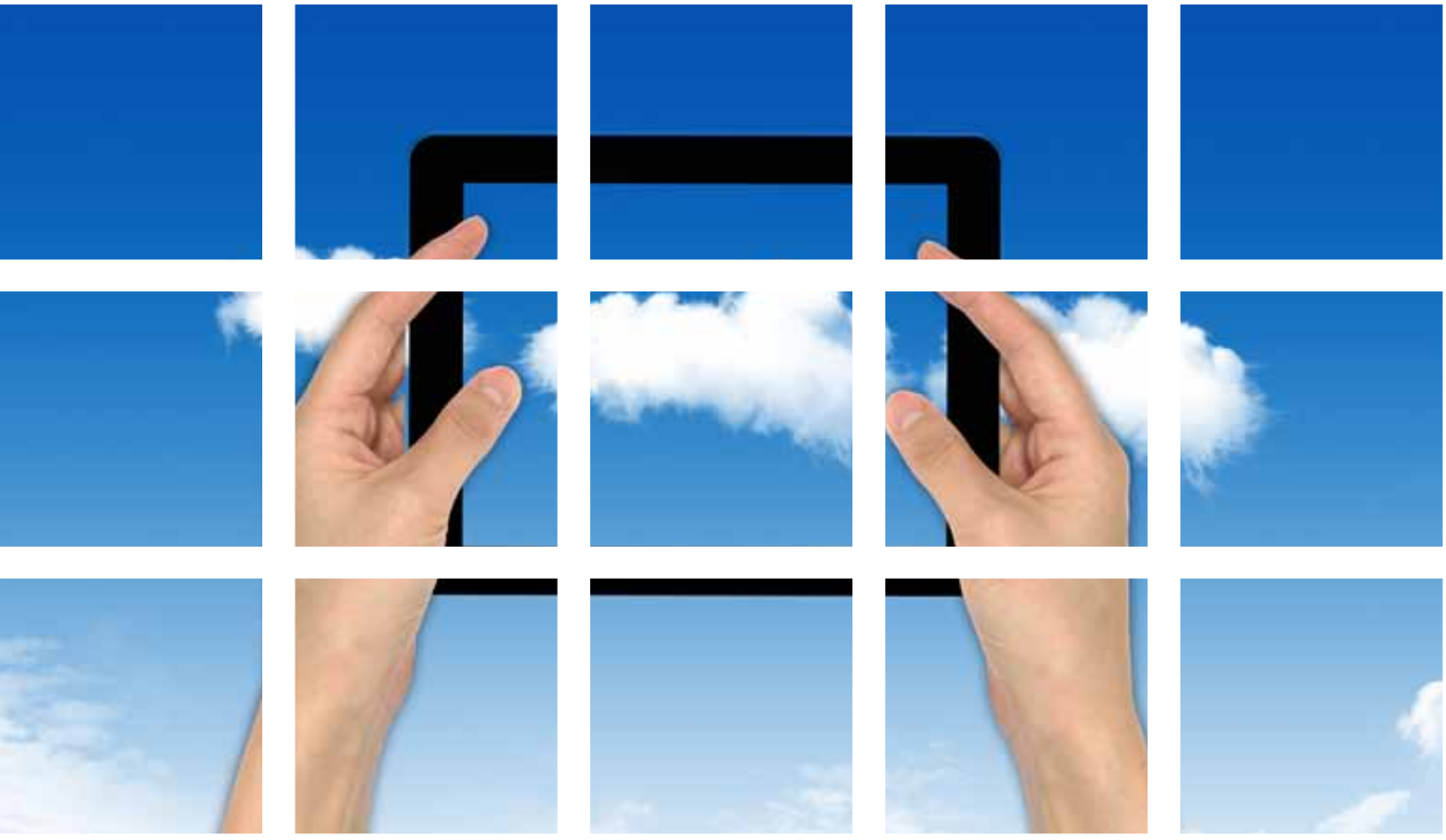
We observed that there are only limited measuring instruments with regard to the definition and operations of SIESs, not only in terms of thresholds for security breaches and incidents but also for the performance of the scheme.

To establish thresholds regarding the characterisation of a security breach or a security incident, sector-oriented views need to be developed linking the level of expected damage to the severity of a security incident or a breach. To do this, discussions need to be initiated within the relevent fora and committees.

For the performance of SIESs we recommend the establishment of a Balanced Scorecard or comparable KPIs (Key Performance Indicators). Balanced Scorecards 'articulate the links between leading inputs (human and physical), processes, and lagging outcomes and focus

on the importance of managing these components to achieve the organisation's strategic priorities'.[22] Such instruments help translate the security protection target into operational goals and contribute to the measurability of security services. Security breaches and security incidents are basic parameters that flow into this. Based on the improvements proposed in the preceding paragraphs, estimates should be made of how much SIESs contributed by preventing resources being spent on inappropriate measures. We believe that the definition of KPIs and a Balanced Scorecard, together with recommendations 1, 2, and 5 will provide a proper basis to improve the efficiency and effectiveness of SIESs.

Stakeholders: In elaborating on sustainable measurement instruments it is necessary for the competent actors and industry stakeholders to take the lead if this goal is to be achieved. Such an initiative should be motivated by their vested interest in economic efficiencies – a factor that is a driving force in every market. In this respect elaboration on the measurement instruments could be coordinated at national level by **competent authorities** or services. Grounds for the bilateral collaboration may be found in the mutual interest in establishing a meaningful benchmark. Such a benchmark would on the one hand facilitate the relevant economic efficiency evaluation for the interested constituents while on the other hand it would provide the national authorities with adequate data to assess the effectiveness of the **SIESs** established on their soil.



22 Abernethy, M.A., Horne, M.H., Lillis, A.M., Malina, M.A. and Selto, F.H., 2005, 'A multi-method approach to building causal performance maps from expert knowledge', p. 136.

10. Conclusions

Concluding this study, we would like to stress that the recommendations made in this document constitute a basis for a dialogue within SIESs in Member States and within the committees and bodies of the EU.

The purpose of this dialogue is to assess the feasibility of the implementation of these recommendations in order to enhance security breach notification, to prioritise them according to planned initiatives and to channel necessary detailed discussions in the relevant committees, stakeholder groups and communities. As such, this work the can serve as preparatory material for potential upcoming consultations at the levels of Member States and the EU as a whole.

Furthermore, material developed for the purpose of the analysis, i.e. parameters for the efficiency of security breach notification and SWOT-analysis results, can inform current and future assessments that might be deemed necessary in the ongoing attempt to improve security breach notification, both in Europe and worldwide.

Finally, this report will serve as input for the ENISA work to be carried out in 2012, in particular in the areas of security breach notification and Economics of Security.

European Network and Information Security Agency

Economic Efficiency of Security Breach Notification Analysis and Recommendations

Luxembourg: Publications Office of the European Union, 2012

ISBN: 978-92-9204-059-8

doi: 10.2824/23654

Catalogue Number: TP-32-12-112-EN-N

TP-32-12-112-EN-N

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu

doi: 10.2824/23654
Catalogue Number: TP-32-12-112-EN-N