

The information and views set out in this document are those of the members of the network and information security (NIS) Platform and do not necessarily reflect the official opinion of the European Commission or the European Network and Information Security Agency (ENISA).

NISP WG2 Plenary Report

Information Sharing and Incident Notification

DRAFT V3 (22.4.2014)

[Editor's note –

1. This document is the product of collaborative work done to date and it is the view of NISP contributors that there is more work to be done.
2. This document does not address risk management or cybersecurity controls for risk mitigation, which are the responsibility of NISP WG1.]

Introduction

The European Union (EU) Commission is developing the Network Information Security (NIS) Directive to support the EU Cyber Security Strategy. Alongside the on-going legislative deliberation on the Directive, the Commission has established the NIS Platform (NISP) to “develop incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally.” The NISP comprises three working groups of governments and industry. WGs 1 and 2 were tasked to complete their final contributions by late April 14, with WG3 by Sep. Well over 350 people were involved.

- WG1 – Risk Management – is conducting a separate survey, which includes the identification and review of risk management methods, frameworks and capability maturity models.
- WG2 - Incident Notification & Information Sharing - has established three sub-groups (SG1 – Existing Initiatives; SG2 – Incident Notification & Information Management; SG3 – Protocols). WG2 SG1 and SG2 sponsored this survey.
- WG3 – Research and Innovation is separate.

Going forward, the EU Commission recognises that industry and public sector participation will need to continue beyond NISP into 2015, building on NISP activities and using the recommendations and information in this document.

Purpose

The purpose of this document is to make initial recommendations by the EU NISP for collaborative action to enable the goals of NISP to be met, particularly regarding information sharing and incident notification.

NISP

The details of the NIS Directive (NISD) will remain undecided and unclear for many months. Until then, the NISP's work will remain relatively decoupled from the NISD and focused instead on articulating an increasingly detailed and structured set of observations, recommendations and guidance for successful information sharing and incident notification. The NISP work will seek to address industry issues and perspectives, in particular, as most of the organisations, the activities and relevant information exist in industry. This is where the NISP offers wider benefit in its own right. It is this much bigger, real-world industry environment of users and suppliers that underpins and enables the NISD's scope of regulators and incident notification.

Disclaimer – Legal Notice

Notice must be taken that this publication represents the views and interpretations of the NISP Working Group 2, unless stated otherwise. This publication does not represent the views of any individual organisation or person.

Third-party sources are quoted as appropriate. The participants of NISP WG2 are not responsible for the content of external sources, including external websites referenced in this publication.

Neither NISP WG2 nor any participant is responsible for the use that might be made of the information contained in this publication.

Primary Recommendations

Many recommendations have been made and more could have been made. However, the overwhelming consensus view was that further work was required to shape, structure and justify a more mature family of recommendations, which could be considered as a whole and in part. Consequently, six primary recommendations are made now, in priority order, that should be addressed, if NISP is to continue and be successful. They are:

1. For NISP to have the necessary collaborative governance to progress, by establishing new NISP working groups under a collaborative, balanced and neutral Steering Group with clear objectives and resources.
 - a. The Steering Group members should include the Commission, industry and governments, and be supported by adequate project management, communication and administrative resources.
 - b. This governance should be based on, and encourage, much wider active participation, particularly from law enforcement and national cybersecurity organisations.
2. To develop a set of collaborative objectives and tasks, based on the work already done, which could provide the basis for future work.
3. To leverage the existing work, including the spreadsheet of information sharing schemes, the survey responses, the experiences and the reference documents. The content needs to become richer and more representative, to provide the evidence to support a set of future recommendations.
4. To distribute widely a communication with a set of questions for organisations to ask

themselves regarding their need to be more aware, to share information and to belong to a relevant community of trust and mutual support.

5. To create a catalogue of information sharing schemes, with support from ENISA.
6. To give feedback to those that have already participated or provided information, to encourage their further participation and a greater level of engagement, feeding into a future catalogue of collaborative requirements.

Approach

The approach has been to provide a context with supporting information, then to gather information, analyse the information, draw deductions and make recommendations. This approach has been successful in producing some initial recommendations. However, its success was limited for several reasons:

- The majority of organisations either did not respond or participate, or considered themselves unable to participate, either because they were not mature enough to provide answers or did not have sufficient resources.
- Some felt that there were too many questions, others that there were not enough or they were not sufficiently specific or too informal. This range of opinions and views was expected but the Working Group knew from the outset that there could be no “one-size-fits-all” approach. With more time and resources it should be possible to have a family of surveys, each targeted at specific groups and sectors.

More work is required to gather and analyse more information, and to improve the recommendations and guidance, which will require the encouragement of more and better participation, and also help for organisations to form their own views.

Context

Cybersecurity, incident notification and information sharing maturity across cybersecurity communities are evolving fast. The survey was supported by a re-usable context of definitions, realities, standards and best practices that is relevant for all - just starting or very experienced. See Annex A.

Information Sources

The current work gathered information from several sources:

- Informal information from organisations and individuals participating in NISP;
- Formal qualitative information from a survey of organisations;
- Formal quantitative data from a survey of information sharing scheme operators;
- The identification of reference documents and standards.

Participation

Over 100 NISP participants, from the public and private sectors, contributed at the beginning,

mostly in meetings. Over time, this reduced to about 35 individuals.

The Commission, via the European Member States Forum, distributed the surveys to 32 governments. Industry distributed the surveys to sixty trade associations.

Surveys

Surveys

There were two formal surveys:

- A qualitative survey of 20 questions for organisations, under three headings – General information; incident notification; information sharing. The questions are repeated in the results section below.
- A quantitative survey in a spreadsheet of 50 questions for information sharing schemes. These focused on scheme basics, scheme membership, scheme assurance & resilience, sharing operations, sharing security, sharing automation and physical meetings of scheme members.

Responses to the Surveys

The majority of recipients of the surveys did not respond. Enquiries suggested that the most common reason for not responding was a combination of caution, a lack of support for the draft Directive, uncertainty about NISP itself or a lack of time. If the situation were clearer and they could be supportive, then they would be more willing to complete surveys in the future.

Of those that replied without giving information:

- Many said there was insufficient time to respond or to respond properly.
- Several said that they were not the right people in their government or organisation to respond, that they did not know who should respond or that their government/organisation's cybersecurity situation was not in a position for a response to be given.

Survey Results – Quantitative Survey

The results of the quantitative survey are given at Annex A, which describes the approach, the analysis, the primary observations and the recommendations.

Quantitative data on 31 information sharing schemes was received, using the data capture spreadsheet. These included schemes from governments, EU and industry sectors – energy, nuclear, water, healthcare, financial, managed service providers, harbour, airport and telecommunications.

Annex A is a significant document and an important contribution to the NISP work. The underlying data and supporting information are not publicly available for reasons of confidentiality. However, they will be available as important input for future NISP work. There is a clear demand, from the surveys, for such NISP work to continue.

Here are the major deductions, bearing in mind that the responses were from a small sample across the EU.

- The majority of schemes are national, sector-based schemes with discretionary

participation (coordination to establish regional sector based schemes is more complex and hence more costly to implement).

- Simple sharing mechanisms, such as email and phone communication play a significant part in current information sharing scheme operation (these are cheap to operate using commonly available infrastructure).
- Schemes offering automation capabilities are currently limited to the maturer schemes with larger numbers of participants, with access to funding capabilities.
- The higher proportion of existing schemes, captured to date, involves information sharing schemes, with informal facility to also report incident related intelligence. Only one example of a mandatory incident reporting schemes has so far been captured, but is noted that they are emerging as requirements e.g. national financial regulators.
- The vast majority of schemes are currently free to access, with subscriptions required for only those schemes in private sector requiring infrastructure to support automation of significant communities e.g. >200. State created schemes, or those smaller communities only using basic infrastructure have not required further complexities of financial subscription.
- Where schemes participants have face-to-face meetings the majority appear to meet more than twice per year. Regular face to face meetings have assisted in building the trust required to share threat and vulnerability information in a non-competitive manner.
- The majority of schemes operate within a formal sharing protocol, but there is currently insufficient data to illustrate the areas of commonality, e.g. utilising a traffic light protocol, anonymity of submissions. Basic protocols assist in the formulation of trust between community participants.
- A significant proportion of schemes have a website which details the scope of the scheme and provides information on how to join the scheme. Access to such details could provide for further basic data gathering from public domain information.
- New sectoral schemes are still emerging, as well as plans for EU region-wide schemes. As further interest in sharing cyber situational awareness, there will be an increase in demand for a central repository detailing planned schemes.

Survey Results – Qualitative Survey

Five organisations responded to the qualitative survey of 20 questions:

- Three government organisations from Finland, Germany and Switzerland.
- One non-government organisation from Luxembourg
- Two international technology-provider companies

Some respondents included a preamble to their answers. The key points included the following.

- Opposition to open-ended government requests for information about customers; requirement for incident response, reporting and notification not to circumvent law enforcement or data protection obligations.

- Technology providers are concerned with threats to, and vulnerabilities in, their products and services. They are not so concerned with threats and vulnerabilities to, or caused by, the user, which are outside the technology providers' control.
- End-user organisations are concerned with threats to, and vulnerabilities of their systems, particularly as it affects their business operations and risks to sensitive information.
- Formal incident notification is not an end in itself. Existing and emerging notification and reporting schemes serve other purposes and need to be scoped to achieve public policy goals and directly beneficial objectives rather than (unintentionally) raising costs and risks.
- Central to the success of such efforts is developing the right incentives and motivations for information sharing and collaborative risk management between and among public and private entities and across international borders.
- More collaborative work needs to be done on the consistent development of controls that are re-usable for protecting sensitive information, including for incident notification. These should build on developments in technology, policy and markets, and include greater collaboration with the private sector on cybersecurity, cloud and critical infrastructure protection. They should also leverage existing international information sharing initiatives.
- Governments should invest in building the requisite expertise to analyse, coordinate, and act upon the data received. They need to do this in close cooperation with industry and with each other. This will take time, resources and sustained executive commitment. One way to boost the development of such capabilities would be to include public administrations in the scope of key emerging policy and regulatory frameworks such as the NISD and related directives/regulations.
- There is a strong requirement for collaborative dialogue across all organisations – the whole EU Commission, governments and industry. This should also leverage existing international information sharing initiatives.

General

Question 1 – Contact details

Question 2

Describe the nature of your organisation's business, its number of employees (>5000, <5000, <250, <50, <10) and the nature of its external interactions – e.g. business community or sector, supply chain, partner organisations, government customers as well as your role in the organization.

Answer 2 – Key points. Responses ranged from small government agencies and research organisations with <250 employees through to major companies with many more than 5,000 employees, including industry operating globally in most developed nations. These companies provide services and products to governments, all industry sectors and to consumers. There were no responses from end-user companies, at this stage.

Four responders supported the protection of critical infrastructures with a range of external interactions, providing information on incidents and threats, as well as supporting technical and non-technical information. All responders were involved in assessing situations,

recognising attacks and incidents, handling incidents, evaluating their implications and analysing malware. The degree to which they carried out these functions varied in scale and detail. At the high end, one organisation collects and disseminates information about information security incidents and threats of relevance to their country. The domestic information sharing partners include operators of critical infrastructure such as telecommunications operators, energy companies, financial institutions, users of industrial control systems and defence industry, as well as central government and national leadership. It is also actively engaging with the CERT community and interacts with security researchers.

It would be helpful for newcomer organisations to be able to discover communities that they might be able to join.

Recommendation 2

- a. Create an EU register of information sharing communities
- b. For each information sharing community to have an accessible register of members, who are willing to be known.

Question 3

Outline the main risks faced by your organisation and its primary regulatory and voluntary requirements for incident notification and incident management.

Answer 3 – Key points

The main business risks associated with cybersecurity concern the risks of regulatory violation, data loss and reputational damage, leading to potential financial losses and a reduction in competitive advantage. These legal requirements include regional, national and local regulations for privacy, civil liberty, sensitive personal data, financial regulations, payment industry regulations, health regulations and export control regulations. In addition, there are contractual requirements from governments and industry, to protect commercially sensitive information and intellectual property. Finally, there is the additional, non-specific need to protect sensitive information whose loss could lead to reputational damage of governments, companies or persons – there is no regulation or contract for this, which makes risk assessment and prediction particularly difficult.

The requirements for incident notification vary in several ways. There is wide variation in what constitutes an incident, whether it needs to be notified and the method for notification. Within governments, incident notification is mainly mandatory, but for critical infrastructures, it is mainly voluntary today but is increasingly becoming mandatory. The roles and responsibilities of the organisations receiving the incident notifications also vary; some were regulators, but others were only a management focus for providing the information to other government organisations.

As the requirements for mandatory and voluntary incident reporting and incident notification (to regulators) increases, there could be new potential risks associated with incident notification, mainly relating to inappropriate data protection and data incident handling.

These risks to information sharing include:

- The value and quality of information received from various channels decreases:
 - voluntary data donors stop sharing information (for fear of liability issues, as a consequence of cost-cutting efforts, after having felt frustration over what they get in return) or put "paywalls" around the information they consider proprietary;

- obligatory reporters limit the reporting to legal minimum (in fear of legal liabilities or as a protest against regulatory oversight);
- the data donors or reporters attempt to "poison" the data by introducing inaccurate data (in effort to cause disruption in the networks or in effort to undermine the trust between actors that participate in data sharing schemes).
- The data sharing dries up or the amount of data offered exceeds the ability to process it:
 - there's a distinction between "raw" event level data and information about incidents;
 - in order for the information about an incident to lead into action, the notification has to travel after the original detection (from the 'discoverer') to the actual owner of the affected assets ('victim') in due time, in compatible format and with enough verifiable information;
 - the information travels through one or more intermediaries (clearing-houses or brokers), who may only have a partial interest in passing the information to the 'next hop';
 - some of the intermediaries handle terabytes' worth of raw information daily, which turns into condensed reports to the network owners;
 - if the high volume intermediaries would cease to operate or share (for economic reasons, trust issues, technical incompatibilities, legal and liability issues), many information sharing schemes would either cause a spill-over of raw data to the 'next hop' or the sharing would simply dry up.
- Sharing of data becomes impossible or too complicated due to:
 - security classification requirements or issues with the sensitivity of the information;
 - liability issues;
 - legal issues regarding traffic data or personally identifiable information.

Much more work is required to be done to catalogue and address these shared risks.

Recommendation 3

1. For future work to capture, analyse and address these risks and associated requirements for their mitigation.

Incident Notification

Question 4

Describe your approach for incident notification resulting from events within the organisation.

Answer 4 – Key points

Most responders consider incident reporting to be part of incident management, which can occur during the incident, and usually does so. Incident notification (as defined by the NISD) is considered to be after the fact or incident has occurred, and uses some information derived from internal and shared information sources. The responders' information sharing approach is driven by the requirements for incident management – how to mitigate a threat, how to protect against a vulnerability by installing an update or taking a specific action, or providing

other guidance to be more secure.

Incidents arise from security events that result from detections. These detections are usually prioritised against a set of rules – for example, one set concerns the importance of sources

1. Primary sources: the detection systems owned or operated by the organisation.
2. Secondary sources: detection systems owned and operated by third parties that are willing to share details about how and where the detections are being made (technology, configuration, location in the network topology)
3. Tertiary sources: 'black box' detection systems owned and operated by third parties that can only be evaluated based on the information being shared, not by evaluating the tools and processes used to obtain the information.

The detection systems in this context are intrusion detection systems, netflow monitors, antivirus engines, honeynets etc.

As the volume of secondary and tertiary source information increases, so there is an increasing need for automation and greater standardisation of taxonomies and some parts of the analytical processes that generate shared data.

Formal incident notification information is provided to the General Counsel or equivalent, as they involve regulatory compliance, where decisions are made on what kind of notification is required, to which regulatory authority and when.

Recommendations 4

- Incident notification information formats should be specified in such a way that they can reuse (under control) incident reporting information, and the processes, taxonomies and automation that is increasingly necessary for information sharing and collaborative cyber defence.
- Future work should involve general counsels and their legal staff.

Question 5

Describe your approach for incident notification resulting from events in your external community (e.g. partners, supply chain) that present a risk to your organisation. This should include any collaborative arrangements to ensure a consistent and comparable approach across a community.

Answer 5 – Key points

None of the responses addressed the issue of collaboration on incident notification to regulators. They only mentioned incident reporting.

The global IT companies and governments do collaborate on incident reporting and incident management where relevant. The breadth and depth of that collaboration vary in maturity, and all are experiencing a gradual increase in breadth (more organisations) and depth (more information). Global technology companies, such as Microsoft, McAfee (Intel), Cisco and others, have response centres and Computer Emergency Response Teams (CERTs), backed by considerable data and data analysis resources. All of these capabilities are made available as appropriate through partners to customers, and also through cooperative arrangements with governments.

Major companies increasingly have policy compliance teams, linked to general counsels, to ensure that suppliers are compliant with policies and standards related to legal, regulatory

contractual and statutory obligations.

Where governments have collaborative relationships with companies, this tends to be limited to critical infrastructure organisations under a public private partnership. This does not include the vast majority of companies whose needs and vulnerabilities are not addressed.

The incident reports from external sources provide a valuable addition to internal sources. The external reports may be more difficult to use due to incompatibilities with data formats and means of transport. It is difficult to exert SLA requirements on the volume, completeness, timeliness and continuity of the data. There are also trust issues and - in some cases - even not-invented-here attitudes involved. Many organisations are poorly prepared to accept external incident reports.

To overcome these barriers, leading nations have set up information sharing schemes. Here is an example.

A national example

One leading scheme automatically collects 3rd party incident reports about incidents affecting the national internet space from dozens of sources ('data donors'), breaks the material apart, anonymises it if necessary, repackages the data into batches reports and forwards the material to the network administrators in the expectation that they take corrective actions to secure their own or their customers' assets.

The recipients include operators of all national AS numbers (over two hundred) and in certain cases, owners of individual IP netblocks. In 2013, this system processed over 600.000 notifications indicating incidents in over thirty different categories, most notably malware infections, denial of services attacks, web server intrusions, command and control servers, malware distribution and phishing sites.

The telecommunications operators cannot 'opt-out' from this national scheme but they can delegate the actual handling of incidents to their customers' and partners' security teams. Individual network-connected organisations can, however, opt-in to receive reports for their own IP netblocks (or AS numbers, if they run a multi-homed network).

The information is provided 'as-is' but the national scheme operator exercises care before introducing new data sources and notification categories as the quality and consistency of the data is valued among recipients. Due to partial anonymisation of the data, the recipients cannot go "upstream" and ask the original source for more details, but rather they either have to trust the scheme's assessment or ask the scheme to relay information requests to the original source. If the quality of the data is in doubt, the national scheme operator removes the data feed or the source from the system.

The scheme not only collects and shares the data, but it also reformats the notifications in a common format and provides a single transport channel to deliver the reports to the actual recipients. The scheme also aims to be format and transport agnostic in the way it receives data from the sources.

The scheme supports basically any text based data formats that can be parsed through automated means. Originally, Team Cymru's IP2ASN format was the de-facto format supported by most high volume sources. The scheme also supports standardised formats such as IODEF and has successfully turned into parsing more proprietary formats and scraping information from web pages. The reports are sent out in "human readable" format similar to IP2ASN. Also XML and CSV are supported but not widely used by the recipients.

The incoming data is obtained by both GET and PUT methods over XMPP, e-mail, FTP and HTTP. The supported output transports are e-mail and XMPP. Both of these can support federated trust in a manner that supports partial anonymity.

The system supports batch processing of notifications and AS-IT-HAPPENS reporting. In practice, most data sources prefer to prepare a batch report that they release in agreed-upon schedule. Conversely, most recipients prefer to be informed in batch. Batch processing has a tendency to introduce added latency times between the detection and resolution. On the other hand, the most important thing is that the notifications are processed in the first place, instead of them flowing through without causing action.

This national scheme has been operational since the end of 2005. Since that, the national networks have been repeatedly deemed one of the 'least infected' in the world, with the word infection being used as a reference to malware infections.

The legacy core engine was upgraded in 2011.

Recommendations 5

- More work is required to establish the requirements of SMEs and supply chains, and their service providers.
- More work is required to build on the experience and capabilities of leading scheme operators.
- The EU should establish collaborative arrangements to leverage international and de facto standards for information sharing, particularly for high assurance federated trust, for partial and full anonymity, for access controls, for taxonomies to support data interoperability, for transport mechanisms to support security automation, for basic rulesets for data analysis and triage.
- The EU should establish collaborative governance arrangements to support the operationalization and adoption of information sharing and incident reporting. This should include scheme assurance, testing and serious gaming.
- The EU should establish collaborative capabilities to enable much improved communication, backed by training and awareness.

Question 6

Outline examples of possible incident notifications that are important to your organisation.

Answer 6 – Key points

Incident notification – what happened, after the fact, how we mitigated – the overwhelming majority of those types of notifications are in the public domain and generally well understood.

The types of incidents of interest for notification (to a regulator) and for reporting generally vary and their range continues to grow. However, incident reporting and management has a much wider scope than incident notification. They may be categorised by their impact, the user communities or the technologies. Incident notifications mainly focus on data breaches and denial of service. Looking deeper, incident reports can include technical safety issues, software vulnerability reporting, privacy, civil liberties, ethics, fraud, phishing, defacement, foreign corrupt practices, sabotage, espionage, etc. They impact critical national infrastructures, banking, financial, health & life sciences, aerospace, aviation, transport and several other sectors.

All information can be important to someone, but it takes time and maturity for an organisation to begin contributing or posting information for two reasons. When joining a community, organisations are reluctant to provide information and they don't know what others require. They don't have the maturity to be able to generate and provide information that is useful to others.

Any large provider of IT services to customers worldwide relies on receiving information from its service providers of products and services to mitigate any threats to it or its customer. Security bulletins provide detailed information to help customers protect themselves.

At this time of change, information about new and novel threats is of great interest to global IT providers. These are hard to come by and often held by governments or private sector entities that use such information as a part of a service they provide to their customers.

Learning about more sensitive incidents (the type that if known broadly or publicly would cause harm to the computing ecosystem), those are the types of incidents that would be of significant interest. Sharing such data is extremely risky, and merits strong access controls due to the risk of exploit and the rapid and pervasive nature of security exploits. How much to share such information is a challenging balance, but one faced routinely in intelligence, aerospace, defence and law enforcement. Some aspects of NISP will need to go into these areas if NISP is to be successful.

It is also important to underscore that in addition to controls for protecting the incident notification data, governments must also invest in building the requisite expertise to analyse, coordinate, and act up on the data received. This is not a small investment. To successfully develop capabilities governments need to ensure that they have also have internal reporting processes across their infrastructures so that they can (1) better protect themselves, and (2) develop the "hands on operational" expertise to be able to effectively engage with technical and operational experts from the reporting entities in the private sector. Most challenging of all, governments need to develop the analytical capabilities necessary to evaluate, synthesize multiple reports, and provide actionable and useful insights for relevant public and private sector entities. Building capabilities takes time, resources, and sustained executive commitment.

An example view

Leading national schemes consider that any sign of an information security anomaly that a national network or organisation experiences is of value and possibly worth sharing. However, in order for the reporting to be useful to the ultimate recipient, the data contained in it has to be 'actionable'. This means that the report has to include (or point to) enough information for the ultimate recipient to be able to determine whether the "claim" is plausible and to identify the ICT system that is experiencing the security anomaly in question. Concrete examples of currently active types of incident notifications processed by a national scheme tool include (among other) instances of Zero Access malware and compromised web sites in national networks.

Below is an example notification ("human readable format"), from the scheme tool, about Zero Access malware in a broadband subscriber's computer:

*16086/188.67.xxx.xxx/2014-03-15 xx:xx:18
+0000/xxx.bb.dnainternet.fi/FI/Bot/784945/Datasource: B, Malware type: ZeroAccess, C&C:
70.175.xxx.xxx/16471, AS: 22773, DNS name: xxx.no.cox.net*

Another example is about a compromised web server that has been turned into malware

distribution platform:

719/194.136.xxx.xxx/2014-03-15 xx:xx:47 +0000/|FI|Bot/784927/Datasource: B, Malware type: hacked-webserver-stealrat-t1, C&C: 194.136.xxx.xxx, AS: 719, C&C url: backup/rssQVA6.php, DNS name: www.xxx.fi

Chances are that neither of the asset owners had noticed anything peculiar with their systems on their own. There is also a high probability that the ISP (or a hosting service provider) was unaware of the incidents until they received a fresh batch of notifications about their network.

Experience has shown that there is an urgent need for schemes that leverage the existing incident detection capabilities of various third parties and seek to bridge the gap between the 'discoverers' and the 'victims'.

Recommendations 6

- Further work is required to establish how incident reporting and incident management could support incident notification and to address the issues of confidentiality and consent with regard to the use of incident notification information.

Question 7

Describe any challenges you have identified about incident notification that need to be addressed in any implementation system and supporting guidance.

Answer 7 – Key points

A small but increasing number of governments and global IT organisations have established effective approaches to incident notification and reporting both internally and with the external communities of security researchers, CERTs, partners and allied governments. Below are some of the many challenges.

Major challenges exist in the following domains:

1. Building the motivation to share. The motivation to share needs to be nurtured:
 - a. A surprising number of organisations collect observations about incidents and even investigate them on their own. While the primary impetus is to gain knowledge about security threats affecting one's own business, the process often reveals incidents affecting other organisations as well. These findings are usually kept internally and not shared with the other potential victims. Ways to motivate organisations to share information that may (or may not) be of help to complete strangers or even competitors are needed.
 - b. There is a fundamental requirement for a legal environment where sharing of incident notifications is encouraged or mandated (as in the USA). In this context, the quality and richness of data depends on the liability aspects - organisations will not share self-incriminating data (unless everyone is forced to do so – as in the USA) and will not risk sharing data that could subsequently be deemed too sensitive or not okay to be shared.
 - c. There needs to be a way to align the sharing of data with the business interests of the organisation. If there is not 'added value' in sharing, business organisations opt to not share. The scheme must reward the participants in ways not possible to achieve elsewhere. Establishing mutual or collective benefit is key. The more reciprocal the information exchange is, the more it

rewards both the data donors and the recipients. Data brokers must also find a business case in forwarding third parties' data.

- d. Organisations vary in their ability to handle securely information that is shared with them. These differences are hard to observe, so organisations are reluctant to share information due to fears that the recipient's network may be breached.
 - e. Build trust among participants. Strengthening relationships, managing expectations and establishing a common cause are all key.
2. Deciding what to share. There is no single model for sharing or for building the trust and relationships on which sharing depends.
- a. Sharing public or discernable information about routine tactics or techniques regarding phishing, malware, fraud and abuse does not help the service providers who support significant percentages of the market. Decisions need to be made about whether the scope of information sharing is for the top end market providers, all market providers, or for customers (enterprises, smaller businesses, etc.) because the information sharing needs of each of those communities, and their ability to act on that information, differ dramatically by group. Narrowing down the scope of sharing and getting crisper on the reason for it is paramount.
 - b. Moreover, sharing information that is meaningful and not meant for broad and public consumption requires a mechanism to allow the sharer / owner of that information to assess and manage risk. Most routinely, this is done through contracts. Many information sharing efforts are done bilaterally, under a non-disclosure agreement or some other legal arrangement that allows parties to manage the risk of sharing, or multi-laterally, through some sort of program agreement. It is critical that these informal, very valuable information-sharing channels are preserved against the backdrop of emerging regulatory-based incident notification regimes.
3. Problems of incident detection:
- a. A notification's content has to be of high quality to be worth sharing.
 - b. Some incidents are almost impossible to detect by the victims themselves but are easy for a third party to spot if they have access to key resources. A service provider can spot incidents affecting their customers, a security researcher can spot victims globally and law enforcement action can uncover wide-ranging breaches of security half a world away. The ability to detect must be coupled with the willingness to share.
 - c. Some incidents are sensitive in themselves or the circumstances in which they have been discovered are sensitive. There are encouraging signs of willingness to distinguish the differences in sensitivity between the 'context' of the incident and the 'indicators' of the incident. A sensitive detection capability or investigation can still produce less-sensitive indicators of compromise that are okay to be shared.
4. Identification of reporting points is messy and needs to be made easier:
- a. Victims are hard to reach on the internet. It may be next to impossible to

determine who operated a malware-ridden computer or whose responsibility it is to fix a web site that has been broken into. CERTs have long struggled with this problem and found ways to overcome it. Below is an example extract about an algorithm to find a proper reporting point. The method involves advancing the steps described below until a satisfactory combination of reporting points has been found:

- i. Names: identify hostnames, names of organisations and popular brands involved in the incident. → if security contacts for those entities can be found and can be expected to take action based on the information, send report
- ii. IP: identify IP addresses involved in the incident; resolve hostnames to numeric if necessary. → if security contacts can be found and are known to be capable enough to handle the incident, send report
- iii. AS: associate the IP addresses with the corresponding autonomous systems. → report the incident to the security contact of the autonomous system and request assistance in finding the ultimate contact
- iv. CC: determine in which country the autonomous system or the brand names are associated. → identify the national CSIRT or other "CSIRT of last resort" in that country and request assistance in finding the ultimate contact.
- v. Upstream: determine the network service providers responsible for the up- stream communications link. → report the incident to the security contact of the upstream provider and request assistance in finding the ultimate contact if appropriate.
- vi. Region: chart the geographic region neighbouring the country; observe geo- political and cultural nuances. → identify national CSIRTs or other trusted resources familiar with the culture and language and request assistance in finding the ultimate contact if appropriate.
- vii. Publicise: if no contacts can be found or no response have been received, widen the circulation or make the incident public in the hope of limiting collateral damage. If the primary victim cannot be helped, at least let secondary targets know about the incident
- viii. Drop case: if all options have already been exhausted, drop the case.

5. The role of the incident report brokers needs attention:

- a. As seen above, the incident reports in any nontrivial real life system flow through a number of intermediaries whose task it is to receive somebody else's incident reports, determine who might be in a position to either resolve the issue or know another entity with closer access to the victim, and then pass the information onwards. Without such intermediaries most incident reports would never reach their intended recipients.
- b. Intermediaries provide valuable contributions by correlating and normalising data originating from various sources before passing it to the final recipients.
- c. The intermediaries also serve to hide the originator's identities or other

sensitive information in instances where the sources wish to remain anonymous to the recipients.

- d. Given the invaluable role of the intermediaries, surprisingly little is being discussed about their role and expectations for a well-functioning intermediary.
- e. Is it okay for the intermediary to utilise the information that it passes to advance one's own gain? Whether it is business interests of a company, academic interest of a research, regulatory interest of a government agency?
- f. How should intermediaries be funded? Paid service, advertisement, subsidised or a governmental monopoly, or a mix of these?
- g. How can an intermediary prove one's trustworthiness? How does a participant in an information sharing scheme recognise a dishonest intermediary?
- h. Who owns the information? The intermediary, data donors, the victim? Does ownership matter?

6. Actionable information.

- a. Sharing information that is in a standardized format is of secondary interest to the higher priority of sharing actionable information that is not available in the public domain. Regardless of the mechanism that is selected for how information is shared, there are important decisions to be made about the scope of what is shared. The reality is that strong information security practices are in place in leading global IT companies because they need to meet their customers' needs.
- b. A challenge posed by incident notification is that by the time an incident is notified, if it is an attack against a product or service, it is already in the public domain by the time it is noticed. If it is related to a generic type of exploit or harm on the order of millions of times a month, then notification about best practices is also, for the most part, after the fact and not generally helpful.
- c. The full extent of an incident including important details on root cause often cannot be determined within aggressive reporting timelines which limits the usefulness of such notifications.

7. Recipients must be able to validate reports:

- a. Once the victim (or an upstream intermediary) receives the incident notification, there needs to be a certain amount of information available to determine, whether there is a genuine incident that needs to be resolved.
- b. In order for the report to be 'actionable', the recipient must be able to establish that a security incident has indeed taken place and that it affects systems and users within the recipients' domain of control. The report has to provide enough technical material to identify the affected network and nodes and to indicate the type of incident. Such Indicators of Compromise might include IP addresses or hostnames, timestamps, information about the type exploit or compromise.
- c. If the originator's identity is omitted, the chain of which the report was delivered must be trusted, or the report must contain enough information for the problem to be reconstructed.

8. Tools for information exchange need to become more available:
 - a. Up until recently, the information sharing schemes had to come up with a custom tools and dedicated data formats. Currently, a number of well-defined formats and transports have been introduced, but the practice of information sharing still suffers from incompatible implementations. Given the generally low motivation for sharing and the high reliance of the intermediaries, the tools should seek to be as interoperable and format agnostic as possible. The tools should not become a barrier to sharing.
 - b. Any practical scheme must be able to function in an environment where there are different amounts of trust between groups of actors. The information sharing tools must be designed and implemented in a way not to discriminate parties with only partial interest in the original problem statement or who are participants with a different or competing technological platform.
9. Emerging standards must continue to be improved and to be adopted.
 - a. Leading IT providers interpret incident handling in relation to their own products and services and there are standards for terminology in security response. However some of these standards are new (ISO 29147 & 30111) and others are broadly interpreted. This results in challenges of misinterpretation between different bodies and across the countries and regions of the world. Even in these documents, the terms Incident, Notification, Information and Sharing are not defined in absolute terms.
10. A pressing problem is about sharing advanced persistent threat (APT) related information (malware samples, command and control (botnet) servers, intrusion detection system fingerprints, checksums, behavioural clues, information about the campaigns, etc.). A strong law enforcement interest and foreign policy dimension will continue to ensure APT remains a challenge for information sharing schemes.

Recommendations 7

- A catalogue of collaborative requirements for information sharing and incident reporting should be developed as a priority deliverable of future work. These requirements should be derived from the challenges experienced by all public and private sector groups.

Information Sharing

Question 8

To what extent is information sharing important to your organisation and your community, to maximise your cyber security. This should include all major steps – Identify, Protect, Detect, Respond, Recover.

Answer 8 – Key points

Information sharing can and does play a key role in protecting organisations, and is seen as an imperative by an increasing number of governments and industry sectors. This is reflected in leading national cyber strategies. Most governments and sectors either have or are moving towards a model similar to – Identify, Protect, Detect, Respond, Recover – and contain the key functions for time-based security and business resilience. However, more work is required to connect the discoverer to the victim as rapidly as required.

There are some key principles that underpin successful information sharing efforts.

1. Sharing efforts should be outcome focused and designed to solve a particular problem. Open-ended sharing quickly breaks down, because there is no mutual benefit to sustain participation.
2. The information shared should be actionable and operationally relevant.
3. The information sharing efforts should be transparent, meaning that the existence, principles, and processes are known.
4. The efforts should be interactive and result in insightful and risk-based, feedback (if a recipient does not action on information, is it valuable and worth the risk & cost of sharing).

The most useful and actionable data comes from “voluntarily shared information” not from either being required to report or receiving derivative analysis from data required through other sources. For example, most vulnerabilities related to software, services and hardware are found and mitigated internally. Thus, information sharing is likely of interest for only the smallest subset of previously unseen or unknown vulnerabilities or tactics. For that most sensitive information, or for information shared about a new and critical vulnerability, Leading IT providers will trigger their incident response processes, which work across the “identify, protect, detect, respond, recover” cycle.

Information sharing from third parties is helpful, but is not a panacea for strong defence in depth processes that support the secure development and secure operation of services.

Leading global IT providers have developed procedures and capabilities for disclosing vulnerabilities to selected third parties, information security providers and customers for action, and also with research communities. They share information relating to the security of products and services, which includes bulletins, advisories and tools, through our security cooperation programmes with governments and some national CERTS around the world, as well as online. They also run communication events for external and internal researchers.

Recommendations 8

- These principles and functional requirements should be captured in the aforementioned collaborative catalogue of requirements.

Question 9

What are the key elements that an information sharing methodology should include in order to be used by any kind of organisation (from critical infrastructure operator to SMEs)? Please provide them in priority order.

Answer 9 – Key points

The key elements of information sharing methodologies and their priority will vary by context, purpose and membership however important requirements include:

1. Legal mechanisms to ensure that the information disclosure can understand and manage the risks associated with sharing the information;
2. A legal entity capable of taking disclosure responsibility for the information being shared, held and disseminated by it;
3. An Information Sharing Agreement (ISA) or contractual process to specify the policies, procedures and mechanisms for information sharing, which takes account of the

sensitivity and sharing conditions for information that is shared, the changes over time and the outcome for unsanctioned disclosures;

4. A known membership with means of control and representation to promote trust and management of risk with the participation of trusted individuals. This membership should include, where relevant, end-users, governments, policy makers, service providers and technology providers;
5. Potentially, if electronic means are considered, a method of automation with appropriate authentication, marking and control to receive, mark, control and disseminate information to only those parties or groups intended for each type of information, according to “obligation to share” and “need to know” principles;
6. A mix of mechanisms to support different requirements for information sharing e.g. an information hub, broadcast mechanisms, secure email, secure chat and discussion groups.
7. The building of repositories of information for in-depth analysis for trends and to support risk assessments.
8. An exception process for emergency situations where urgent ad-hoc response is required;
9. Multilingual capability.
10. A regular review process to ensure that all constructs and processes of the method are relevant to the prevailing security environment. This should include a roadmap of future developments to meet changing needs;
11. A collaborative governance mechanism that manages the community’s information sharing requirements, develops the policies, procedures and mechanisms for information sharing, and also ensures the compliance of members.

Recommendations 9

- These principles and functional requirements should be captured in the aforementioned collaborative catalogue of requirements.

Question 10

What collaborative or shared information capabilities do you believe need to be developed either internationally, nationally, across your industry or community?

Answer 10 – Key points

Many governments, national organisations, like CERTs, and some international organisations have established information sharing initiatives. These provide information sharing in some depth for some parts of the world and breadth across other parts the world. For large service providers, information shared by CERTs is generally at the level of public information.

However, the dated mindset of information ownership remains a major challenge. This creates a lack of transparency, which is a big problem. This lack of transparency stems from a fundamental misunderstanding by legal, sales and public relations people, who have not yet understood that sharing information is crucial for everyone. In the case of governmental organisations, often wrongly (over-)classified information is the main reason that information is not openly shared.

A way must be found to balance the transparency of information exchange and, at the same

time, to make sure that the knowledge of the existing security gaps are not being exploited and used to build attack vectors.

A way is needed to share incident information in a distributed and non-hierarchical manner.

The range of sensitive information should include at least, threats, vulnerabilities, attack vectors, and the status of members' cyber defences. All too often, an organisation will identify a vulnerability or failure in another organisation, before that organisation is aware – it needs to know.

The issues of limited trust have a tendency to limit the usefulness of schemes where a single entity can control the flow of information – these trust, access control and anonymity issues have to be addressed.

The role of intermediaries (see above in Question 7) is complicated needs to be addressed and capabilities put in place.

The legitimate roles of nations, organisations, originators and victims should be recognised. There should be a common legal frameworks for international data transfer providing adequate protections for consent, confidentiality, integrity, availability, accountability, destruction.

Recommendations 10

- These capability requirements should be captured in the aforementioned collaborative catalogue of requirements.

Question 11

What kinds of information would you wish to share, to receive and to submit, and what concerns need to be overcome to ensure success?

Answer 11 – Key points

The scope of the information that could be shared should include all types of information to support Identify, Protect, Detect, Respond, Recover. The kinds of information should include technical information (IOCs, Indicators of Compromise), requests whether another organisation has seen similar attacks and much more – see above.

Information should always be transmitted in a format based on international standards. This allows the automated transmission, interpretation and handling of information.

Sharing information that is meaningful and not meant for broad and public consumption requires a mechanism to allow the sharer / owner of that information to assess and manage risk. Many information sharing efforts are done bilaterally, under a non-disclosure agreement or some other legal arrangement that allows parties to manage the risk of sharing, or multi-laterally, through some sort of programme agreement.

It is critical that these informal, very valuable information-sharing channels are preserved against the backdrop of emerging regulatory-based incident notification regimes. Sharing public or discernable information about routine tactics or techniques regarding phishing, malware, fraud and abuse does not help the service providers who support significant percentages of the market. Decisions need to be made about whether the scope of information sharing is for the top end market providers, all market providers, or for customers (enterprises, smaller businesses, etc.) because the information sharing needs of each of those communities, and their ability to act on that information, differs dramatically by group. Narrowing down the scope of sharing and getting crisper on the reason for it is paramount.

Currently, governments choose to limit the automated collection of incident-related information in cases where the victims appear to be outside their country. Cross-border information sharing could enable a more collaborative approach and mutually beneficial approach, with the victim being the ultimate beneficiary.

The ability to share information about another country with that country faces practical challenges on where to submit foreign data and how to help foreign CERTs receive such data.

Recommendation 11

- Further work is required to identify the types of information that are required to be shared by most organisations, by sectors, by technology and service providers, and other communities.

Question 12

What are your concerns about information quality and timeliness, and the management of the information itself – for the information you provide to others and the information they provide to you?

Answer 12 – Key points

Here is the heart of the challenge for EU policy makers in Brussels and in Member States. Creating an incident notification regime is, in many respects, an outpaced approach to network security. Generally an attack against a product or service is already in the public domain by the time it is “notified” to a government entity. If there is a rapid timeline required for notification the national competent authority will not receive a great deal of actionable data for itself, for other infrastructures, or the general public that is unique and not public. In addition, the shorter the required reporting time the less likely the initial report will be accurate. Specifically, the full extent of an incident including important details on root cause often cannot be determined within aggressive reporting timelines which limits the usefulness of such notifications. In addition, organisations vary in their ability to securely handle information that is shared with them, and these differences are hard to observe, so organisations are reluctant to share information due to fears that the recipient’s network may be breached.

Ideally, security event information should be shared as rapidly as possible, but at the same time, inaccurate information and reports of false-positives undermine the value of information sharing. Each report should be assigned a confidence level that can be upgraded or downgraded as more information comes to light. With such a system, those who are focused on cutting-edge research can see early data, but more conservative organisations can focus on security event information that has been better scrutinised.

Currently, it would seem that national schemes choose to limit the automated collection of incident-related information in cases where the victims appear to be outside that nation.

The information has to be either 'actionable' or 'of historical value'. 'Actionable information' is such that it contains sufficient data for the technical staff to determine whose responsibility the incident is, how to find the affected systems and what other clues to look for in the network. Both information quality and timeliness are very important. The actual set of information required depends on the type of an incident.

- For instance, IP address and (accurate!) timestamps are an absolute necessity for the telecommunications providers to determine the identity of their broadband or mobile subscriber. However, in order for the operator to determine whether they are legally

allowed to identify the subscriber, there needs to be plausible information about the type of security incident that the holder of the IP address at a given time has been involved in. The assertion needs to be backed with verifiable information ('proof') that the operator or a network administrator uses to determine the validity of the claim. In case of a known malware merely a name of the malware may help to run a series of tests to determine whether the claim holds.

- Some Indicators of Compromise do not give out the identities of the victims but rather provide clues on what signs of network or system activity to look for in case an incident is actively taking place. They can be treated as fingerprints and behavioural clues that must be complemented with access to primary sources of information (see answer to question #4 for more information about the primary sources).

Information that is 'of historical value' may be used to correlate and enrich past incidents, and to provide statistical references.

Recommendations 12

- Collaborative requirements for information timeliness and quality need to be detailed and captured, to support future implementations.

Question 13

Do you have a set of Critical or Priority Information Requirements for security event and incident management, and how many of them depend upon information sharing? Please provide examples.

Answer 13 – Key points

Most organisations were reluctant to admit whether or not they possess or use a set of Critical or Priority Information Requirements (CIRs/PIRs) to help guide security event and incident management. In some cases, such sets are proprietary, in other cases they don't exist. Experience suggests that CIRs and PIRs do help to guide forward planning and early detection.

Global IT providers have security incident management processes that are commercially confidential except where it is described above in terms of criticality or exploitability for the benefit of all of their customers, often in the context of a bulletin. The supporting information sharing requirements with partner organisations are equally confidential to the sharing agreements for collaborative programmes.

Recommendations 13

- A baseline set of CIRs and PIRs should be developed and made available for communities to develop further. This should leverage existing CIRs and PIRs already available elsewhere.

Question 14

Do you think that publicly available information regarding incidents could be useful? What risks exist for the provider in making information publicly available?

Answer 14 – Key points

Opinions are divided on this. A minority is concerned that organisations, which publish information more frequently than others, could be considered to be less secure and so could lose customers. The majority view is below.

Currently for hardware and software products, all vendors publish vulnerabilities with related patches and workarounds. Customers generally perceive this as a good practice. Sharing some incident information, particularly regarding intrusions, carries significant reputational and legal risk. It is likely that organisations would feel more comfortable sharing information about certain types of security events if anonymity were guaranteed. Organisations are also likely to be reluctant to share information as “fact” until after a thorough investigation. One way to ease that concern is to allow shared information to be qualified with a confidence rating.

Regarding incident information, IOCs can be made available to the public on a technical level without saying who has been affected and when. If an incident threatens a group of persons/organisations that cannot be contacted directly, the incident must be disclosed. Otherwise, it is left to the discretion of the organisation, but being transparent is seldom wrong. However, if an incident is still going on, a press release can destroy analysis and information gathering, so any information must be coordinated with the Security Incident Response team first. Again, in this process transparency is vital.

Most governments and sectors actively use OSINT information and consider it beneficial, such as information gleaned from CLEAN-MX database, Zone-H and Malwaredomains.com. The fact that data has been made publicly available doesn't necessarily mean that the actual victims become aware of the incidents. Most national and sector schemes take publicly available information and make it 'actionable' by passing it to the responsible network administrators.

A variant of 'publicly available' information is LIMITED circulation information that can be exchanged in public networks but must not be shared with those without need-to-know. This requires the existence a federated identity and access management model.

Recommendations 14

- Further work is required to capture these information sharing requirements and to maximise the use of OSINT information sources.

Question 15

Do you have an information release procedure, such as a Traffic Light Protocol? If so, please describe its use.

Answer 15 – Key points

Most responding organisations use a Traffic Light Protocol to support information release. The larger, more sophisticated organisations may have additional information release procedures or taxonomies, however there is acknowledgement that the simplicity of a TLP approach allows for scale and interoperability. One major responding organisation treats all its information as AMBER.

The important point is that in any instance where an organisation is choosing to share information, it assesses the risks of sharing and if needed, ensures appropriate protections are in place to help protect our information or prevent its disclosure. It can then apply its own processes to decide what it chooses to disseminate broadly, and what it shares under contract, such as through one of its information sharing programs.

Experience has highlighted that some organisations use a TLP instead of an access control regime. This should be avoided as a release mechanism is completely different from an access control regime, and could lead to access control violations.

Recommendations 15

- To establish and capture use cases for TLPs, for variations in the use of TLPs and best practices for augmenting TLPs with other taxonomies.

Question 16

What recognised information sharing mechanisms (see Annex B) does your organisation use?

Answer 16 – Key points

The major IT companies and governments use many different types of sharing mechanisms, including many of those in Annex B. The selection of mechanisms for use depends on the principles that the specific information sharing requires. The agreed purpose and principles are foundational, and absent a clearly articulated problem or common goal, no mechanism will likely be successful.

The same organisations belong to various relevant collaborative communities or groups, such as the European Government CERTs Group, the Nordic National CERTs Cooperation, the International Watch and Warning Network, FIRST, FS-ISAC, NCSC-FI Autoreporter, NSIAM, the Shadowserver Foundation and more. Some governments and companies also belong to non-public schemes.

Recommendations 16

- To identify what is required to make greater use of the leading, more widely-used information sharing mechanisms, to support greater trust, interoperability, information re-use and shared benefits. This should include the mechanisms themselves, the taxonomies and protocols, the information repositories they need to use, and the policies and procedures to enable greater use.

Question 17

What is your experience? How effective are these sharing mechanisms and cyber controls standards/frameworks for meeting your organisation's and community's requirements?

Answer 17 – Key points

See previous comments.

Particularly note the key principles for successful information sharing efforts, which are repeated here:

1. Sharing efforts should be outcome focused and designed to solve a particular problem. Open-ended sharing quickly breaks down, because there is no mutual benefit to sustain participation.
2. The information shared should be actionable and operationally relevant.
3. The information sharing efforts should be transparent, meaning that the existence, principles, and processes are known.
4. The efforts should be interactive and result in insightful and risk-based, feedback (if a recipient does not action on information, is it valuable and worth the risk & cost of sharing).

The information obtained from active and professional information sharing mechanisms provides access to Indicators of Compromise and incident data, which it is not possible to obtain otherwise. They augment other primary sources of information.

Leading organisations have consistently found that, due to the variety of circumstances,

combining standard mechanisms is more effective than adhering to a single standard.

Sharing on a personal and technical level is very effective. The time factor is very important and speed is essential for effectiveness. Anything that hinders the flow of information should be avoided, as the damage done is often bigger than the benefit of keeping it secret. Using an appropriate TLP is effective and must be followed by anyone receiving information. It should be clear that if someone distributes an information report as TLP RED, everyone must adhere to it and not distribute it, if the community members are to trust each other; this requires enforcement by the community.

Recommendations 17

- To identify the different types of existing sharing mechanisms, to articulate their similar and different characteristics, including the behavioural and trust elements that have to exist if the community is to function confidently.

Question 18

What gaps exist and what improvements need to be made to these mechanisms and standards/frameworks to improve information sharing?

Answer 18 – Key points

The challenges of information sharing and incident reporting as they are envisioned in the EU Cybersecurity Strategy and the Network and Information Security Directive will not be resolved alone with improved standards and protocols. A key aspect will be that EU Institutions and Member States build internal cybersecurity risk management and incident reporting capabilities commensurate with the threats they face and can engage with private sector as partners against common challenges.

Information sharing tends to be addressed at technologies that suit the commercial organisations rather than building the subject's/customer's trust. Information sharing programs need to be sensitive and transparent to people's concerns over the handling of their personal information. This also applies to organisations.

An emerging problem is that there are too many different information sharing mechanisms that cannot be readily applied across sectors, many of which are destined to fail because they cannot evolve to support wider interoperability (obligation to share) yet remain sufficiently secure for the sharing of sensitive information (need to know). A twofold approach is needed: on the one hand we need common mechanisms that guarantee a basic protection, and on the other hand sector-specific mechanisms for individual IT systems (for example banks need different standards than the energy sector).

Recommendations 18

- To conduct a gap analysis that would inform a future catalogue of collaborative requirements.

Question 19

Describe any potential or perceived barriers to the adoption of best practices for information sharing, particularly in support of the EU Cyber Security Strategy, which you believe need to be addressed. If possible, please provide examples of what you consider effective motivators to encourage more information sharing.

Answer 19 – Key points

The first big motivator that the private sector would like to see is the EU Institutions and

Public Administrations (particularly at the Federal level) demonstrate a sustained commitment to cybersecurity by establishing information security requirements, regular audits, and incident reporting for government entities. These entities serve the public good and they face both common threats (phishing, malware, etc) and operational challenges (training, configuration, patching etc) that are faced by the private sector. In addition, they face unique, persistent and targeted threats to their data and operations. The more that these institutions understand and share these operational and analytical perspectives, including with the private sector, the more effective collaboration with the private sector will become.

In establishing national competent authorities, they must be competent. They must have strengthened operational expertise, appropriate resources and the capability for analysis. This, in turn, would enable collaboration in a meaningful way with the private sector, creating and enhancing benefits for the EU and its Member States.

Information sharing can and does play a key role in protecting organisations but their success depends on the aforementioned key principles.

Sharing information that is meaningful and not meant for broad and public consumption requires a mechanism to allow the sharer / owner of that information to assess and manage risk. Many information sharing efforts are done bilaterally, under a non-disclosure agreement or some other legal arrangement that allows parties to manage the risk of sharing, or multi-laterally, through some sort of program agreement. It is critical that these informal, very valuable information-sharing channels are preserved against the backdrop of emerging regulatory-based incident notification regimes.

Information sharing requires significant dedication of resources. Wide adoption of information sharing programs will require a clear demonstration of the return on investment of those resources. There should be clear benefits in participating, including rewards and incentives, rather than punishment for opting out. Organisations of a certain size should probably be required to contribute if they wish to receive information shared by others; it should be expected that smaller organisations will more likely be consumers of information, rather than suppliers.

Practical and potential barriers will need to be addressed, particularly around trust and interoperability. This also includes language and cultural differences and the cost and complication of awareness building, particularly at the executive and leadership levels.

Another motivator is reputation. Reputation and perception matter, and they have to be managed. Monitoring and security aspects should be included from the outset to ensure confidentiality, mutual exchange and transparency. It is not sufficient for an organisation to be trusted. It also needs to be seen to be trusted and to be an active participant in the community, otherwise its trustworthiness and reputation in the community is likely to suffer.

Recommendations 19

- To capture these motivators and community behavioural requirements in a document that could support a future catalogue of collaborative requirements.

Question 20

Please list any important reference documents and standards that your organisation uses to support incident notification and information sharing.

Answer 20 – Key points

The responses highlighted national and company specific documents, but were sparse when it

came to international and technical standards. Further work is required to develop an adequate initial list that could be mapped to the major information sharing functions.

Recommendations 20

- To build a repository of reference documents, including policies, best practices, guidance and standards.

Annex A - Existing Schemes for Information Sharing and Incident Notification

Introduction

This section of the report focuses on existing information sharing and incident notification schemes. It aims, where provided scheme operator data supports, to illustrate some basic analysis of common features, insights and differences, as well as experiential observations and considerations of today's key challenges.

A survey exercise has been undertaken within the NIS Platform Working Group 2, to document the type and characteristics of the incident notification and cyber situational awareness (CSA) sharing schemes in operation across EU Member States. The survey recognised the potential for schemes in critical national infrastructure sectors, as well as specialist schemes for sharing intelligence about particular cyber threat vectors e.g. malware, botnet. The survey separated characteristics in terms of "scheme basics" from "scheme details" pertaining to information and attributes associated with more mature schemes. The results from the survey have been compiled into a simple index of schemes to support the observations and recommendations contained below.

Approach

Three separate channels were sought to harvest details of existing schemes. The first was to request registered members of WG2 to submit details of schemes or operators they were directly aware of. The second was a formal request for input via DG CONNECT and thirdly, specifically for the Finance Sector, members of the EU FI-ISAC were requested to contribute.

Surveys

A spreadsheet data-gathering tool was developed to capture scheme attributes; the number and format of questions changed over the period and consequently earlier providers of scheme data include less detail. A significant number of attributes were identified, ranging from the very basic e.g. scheme name, scheme operator and the sector or EU Member State associated with the scheme, to the more technically detailed for more mature schemes. The resulting responses have now been combined into a single spreadsheet comprising a simple index, illustrating the potential scope of the information sharing scheme landscape, and then individual tabs inserted for each of the scheme responses. This Annex summarises the analysed results from the spreadsheet data and supporting information. They are not available for public publication for reasons of confidentiality. However, both the spreadsheet data and supporting information will be made available for future NISP work.

Analysis

A1. The full scope of the EU Member States and defined sectors creates a potential matrix of over 900 schemes (28 Member States, plus Norway and Switzerland, and 30 sectors). Responses have been received to date from 27 (<3%) scheme operators, which include a number of pan-European schemes, as well as those which share successful practice but not operational cyber intelligence. With this small a sample of scheme data it is considered inappropriate to draw too wider conclusions at this stage.

A2. Individual sectors strongly represented from the sample include Energy (Electricity) and Finance, whilst at a national level member state contributions are observed only from eight out of thirty (Austria, Finland, Germany, Luxembourg, Netherlands, Norway, Spain, and the UK); a number of pan-European schemes were also illustrated, including the European Electronic Crimes Task Force, which brings a further important dimension to schemes emerging or in operation.

A3. Feedback throughout the data gathering period illustrated the need for more specific information, and it has become clear that others might also be important, e.g. language of operation, whether the scheme operates a Traffic Light Protocol (TLP). There is need to agree upon a common set of scheme attributes sufficient to illustrate commonalities and successful practice.

A4. Schemes under analysis (31) have been illustrated via the simple table of characteristics below. These statistics have been drawn from data in the Data Analysis worksheet of the spreadsheet.

	Distribution 1	Distribution 2	Distribution 3
1	National (71%)	Regional Multinational (25%)	International (1 scheme)
2	Single Sector (75%)	Cross Sector (25%)	
3	Mandatory Participation (7%)	Discretionary Participation (93%)	
4	Free to Access Scheme (86%)	Subscription Required to Access Scheme (14%)	Both (Of the subscribing services some subset of services are free based on specific criteria) 3 Schemes
5	Information Sharing Schemes (27)	Pure Incident Notification Schemes (1)	Providing for both Incident Notification and Information Sharing (17)
6	Formal Sharing Protocol incorporated (64%)	Informal Sharing / Notification Protocol incorporated (43%)	
7	<20 Participating Organisations (43%)	>20 <40 Participating Organisations (18%)	>40 Participating Organisations (29%)
8	Email Communications Supported (57%)	Portal Sharing Platform (25%)	Support for Automated Exchange of Information & indicators (25%)
9	Scheme Operating >1 <3 years (4)	Scheme Operating >3 years < 5 years (3)	Scheme Operating > 5 years (7)
10	Scheme has No Physical Community Meetings	Scheme has Community Meetings between 1-2 time per year (1)	Scheme has Community Meetings more than 2 time per year (11)
11	Website in place for Scheme (68%)	No Website in place	

A5. Attributes captured to date are provided from a scheme operator perspective, rather than that of scheme participants. This is an important distinction, as within the Finance sector it is clear that organisations become participants of multiple schemes, and there is no attempt made to illustrate preference for one scheme over another, or what features are deemed to be most important.

Deductions (those derived solely from data provided by scheme operators and contacts)

Recognising the relatively small sample of schemes captured, we can draw some deductions:

D1. The majority of schemes are national, sector-based schemes with discretionary participation (coordination to establish regional sector based schemes is more complex and hence more costly to

implement).

D2. Simple sharing mechanisms, such as email and phone communication play a significant part in current information sharing scheme operation (these are cheap to operate using commonly available infrastructure).

D3. Schemes offering automation capabilities are currently limited to the maturer schemes with larger numbers of participants, with access to funding capabilities.

D4. The higher proportion of existing schemes, captured to date, involves information sharing schemes, with informal facility to also report incident related intelligence. Only one example of a mandatory incident reporting schemes has so far been captured, but is noted that they are emerging as requirements e.g. national financial regulators.

D5. The vast majority of schemes are currently free to access, with subscriptions required for only those schemes in private sector requiring infrastructure to support automation of significant communities e.g. >200. State created schemes, or those smaller communities only using basic infrastructure have not required further complexities of financial subscription.

D6. Where schemes participants have face-to-face meetings, the majority appear to meet more than twice per year. Regular face-to-face meetings have assisted in building the trust required to share threat and vulnerability information in a non-competitive manner.

D7. The majority of schemes operate within a formal sharing protocol, but there is currently insufficient data to illustrate the areas of commonality, e.g. utilising a traffic light protocol, anonymity of submissions. Basic protocols assist in the formulation of trust between community participants.

D8. A significant proportion of schemes have a website which details the scope of the scheme and provides information on how to join the scheme. Access to such details could provide demand for further basic data gathering from public domain information.

D9. New sectorial schemes are still emerging, as well as plans for EU region-wide schemes. As further interest in sharing cyber situational awareness grows, there will be an increase in demand for a central repository detailing planned schemes.

Observations (including input made directly by WG2 participants in association with their participation with existing schemes)



Observation 1

Whilst most of the existing schemes have discretionary participation, new mandatory requirements are emerging in certain industry sectors. Such a shift could affect businesses ability to transact digitally across the Member States and there is currently no single “go to” place to identify the current / future state of mandatory scheme notification and participation requirements. **Impact:** *organisations may inadvertently fail to plan for, or comply with, such mandatory participation, leaving themselves open to sanctions.*

Suggestion 1a:

Create and maintain a reference list of legal and regulatory requirements by Member State and Sector, illustrating the mandatory schemes requiring participation, what must be notified and shared (including any criteria for materiality), and the timeframes with which reporting must be achieved.



Observation 2

At the date of this draft report there are many apparent gaps in survey responses and or scheme

capabilities across Member States and sectors (albeit some may have just not replied to the survey, or considered such information confidential and not contributed on grounds of national security). Certain Member States illustrate mature schemes that have been operating for over five years, e.g. Finland, Norway, and the Finance Sector appears to be particularly well served. **Impact:** *organisations seeking to participate in schemes have no point of reference to identify schemes compatible with their interests, or are faced with creating potentially competing schemes within their industry sector.*

Suggestion 2a:

Define a formal statement of requirements for an online catalogue of schemes and seek funding / resourcing to develop and maintain it as an acknowledged point of reference for all such schemes going forward.

Suggestion 2b:

Create and maintain an initial basic catalogue / register of existing (and future planned) schemes based on the content gathered to-date, with contact points for joining them and any costs associated to subscribe. Subsequently publish / communicate how the register can be more widely accessed.

Given the potential demands for organisations to engage in relevant sharing schemes with their peers, suggestions 2c and 2d are positioned to satisfy both latent demand and assist in sharing the learning of more mature schemes that have been engaged in sharing for some time.

Suggestion 2c:

Create a mechanism for registering an organisation's interest in creating / joining a sector based information sharing scheme, such that like-minded organisations can collaborate to create new circles of trust (whilst avoiding the potential of duplicating the work of existing schemes).

Suggestion 2d:

Create a Circle of Trust starter-kit to support organisations wishing to create a new scheme to support their interests. The kit could include reference to the basics around governance and protocols for operation, drawn from successful practices of more mature established schemes. Such a starter kit might also be utilised by existing schemes to assess their operations against a suggested benchmark.



Observation 3

Existing schemes have often begun as small local social gatherings of trusted peers (often sharing anecdotal information about incidents, but have grown with basic agreement (often undocumented) to utilise accessible technology (e.g. email listservs) for unstructured sharing of information. This has been helpful in creating schemes with low barriers to entry (many are free to participate in, with largely unstructured reporting requirements). **Impact:** *Access to such schemes has often limited participation to a particular geography or peer group, without either wider consideration of the liabilities they are facing in sharing information, or longer term governance and operational challenges as volumes of information and interested participants grow.*

Suggestion 3a:

Define a statement / manual of successful practices and tools for incident notification and information sharing schemes, in order to support scheme coordinators develop a roadmap to enhance scheme capabilities.



Suggestion 4

Schemes cite the successful practice of slowly building trust amongst scheme members through provision of anonymous (or partially anonymous) intelligence sharing and sponsoring of new members where peer-level trust is already in place. Maintaining trust is seen as critical as scheme participation and sharing levels grows to more industrial levels. **Impact:** Schemes that cannot exhibit basic governance over their membership may suffer lower levels of timely actionable intelligence sharing.

Suggestion 4a:

Schemes captured within the proposed register are required to clearly publicise how scheme participation governance operates, the criteria for eligibility and any validation activities undertaken before new member organisations and individual participants are permitted to join.

Suggestion 4b:

Schemes publish the current average level of sharing between members and any expectations concerning new members and what behaviour is expected of them within the sharing community, e.g. adherence to a strict traffic-light protocol.



Suggestion 5

Beyond the requirement for a basic catalogue of schemes currently in operation (or planned), there is no agreed model of scheme attributes to assist organisations assess and select the schemes which most closely aligned with their current threat profile or organisational response capabilities. **Impact:** *Organisations cannot adequately assess or differentiate the capabilities and benefits of available schemes, potentially wasting resources engaging with schemes that they would fail to benefit from.*

Suggestion 5a:

Define and agree a basic data model / attribute list associated with incident notification and information sharing schemes, with guidance as to what and how information should be structured and captured, from simple yes or no, to descriptive narrative.

Suggestion 5b:

Design a simple scheme of icons to denote a scheme's focus and capabilities, enabling a rapid perusal of scheme benefits / constraints. This could be used in a fashion similar to garment care labelling and facilitate identification of schemes meeting / not meeting needs, e.g. those transacted in a particular language; those specific to a particular cyber threat vector; those free to join versus paid subscription.

Suggestion 5c:

Plan and execute a more formal and comprehensive data gathering exercise to populate a widely accessible online catalogue of incident notification and information sharing schemes (see Recommendation 2a)

Suggestion 5d:

Define and agree a technology strategy for storing, analysing and enquiring on available information sharing and incident notification schemes and services.



Suggestion 6

The impacts of national privacy legislation are not currently transparent in terms of the way the schemes operate, or the implication for certain data shared or reported e.g. IP Addresses, location of the repository holding the information. **Impact:** *Legislation may constrain sharing between scheme participants; attract sanctions if certain information is shared unwittingly; lead to inadequate protection of personal*

information held.

Suggestion 6a:

Clarify via examples and use cases the information that can be legitimately shared in the context of the Cyber Security Directive, the proposed General Data Protection Regulation and existing national data privacy legislation.

Suggestion 6b:

Define a general purpose privacy risk assessment for incident notification and information sharing schemes, sufficient to create a baseline security controls model for the protection of information held by the schemes. This should be based on international standards.



Observation 7

More mature information sharing schemes are experiencing growing concerns over the cost and ability of their participants to analyse and consume the high volumes of actionable intelligence being shared.

Impact: *Without automation and effective and coordinated triage of information shared, it may not be possible for organisations to prioritise their security mitigations effectively.*

There is also significant variation in scheme operating protocols and data standards, with little sense of the need for or benefit of future inter-scheme sharing or interoperability for the benefit of multiple sectors or geographies. **Impact:** *Whilst cyber threats appear to know no geographic or sector boundaries, the specific schemes tend largely to operate as islands of intelligence with benefits restricted to discrete participants.*

Suggestion 7a:

Scheme coordinators are made aware of the growing momentum to store and transfer bulk threat indicator data in a consistent manner.

Suggestion 7b:

The European Commission, via ENISA and industry, should provide guidance on the overarching strategy and potential standards necessary to support future scheme interoperability.



Observation 8

There is recognition that as scheme sharing volumes grow further there is greater potential for increased numbers of false-positive reporting and need for speedy retraction mechanisms. **Impact:** *Legitimate organisations with uncompromised infrastructure at the centre of false positive assertions will experience unintended downtime of their Internet services.*

Suggestion 8a:

Define and agree consistent protocols and expectations for scheme coordinators to alert and retract indicators found to have been shared incorrectly.



Observation 9

Scheme maturity varies considerably from, face to face meetings limited to a few participants, to multi-national schemes with many participants, already supporting aspects of automation. There is no reference model to depict the scale or sensitivity of information reported in schemes, and the risks represented, e.g. potential lack of scheme resilience, loss of data integrity, loss of confidentiality. **Impact:** *As trust and*

reliance upon such sharing schemes grow, inadequate provisions are made for the continuity of scheme operations and or alternatives to be used should a scheme denial of service occur.

Suggestion 9a:

Define a general purpose threat and risk assessment for incident notification and information sharing schemes, sufficient to create a baseline security controls model for the protection of information held by the schemes.



Observation 10

Certain organisations are engaged with, and connected to, multiple circles of trust and intelligence sharing schemes, without an ability to determine which schemes provide greatest value, or distinguish multiple reports of the same incident (echoes) versus multiple organisations being impacted by the same. **Impact:** analysis efforts can be duplicated leading to greater costs associated with on-going cyber security protection.

Suggestion 10a:

Schemes are recommended to include specific references to the way they handle multiple sources of intelligence and how they assess the overall impact and or remove observed duplicates.



Observation 11

There is evidence of communications disruption during concerted cyber-attacks against either specific regions or sectors. **Impact:** Organisations will need real-time information about changes in attack profiles being witnessed or effective mitigation strategies. Consumers will also potentially require more granular information.

Suggestion 11a:

Schemes develop crisis communications capabilities over and above their normal channels for sharing.

Recommendations

R1. Those that provided information to support WG2, which is associated with existing schemes, should be provided with a copy of the analysis and kindly requested to complete any missing information, now we have a richer base of attributes and completion guidelines.

R2. Further, systematic data gathering is performed to fill as many of the gaps as possible, and the EU Commission consider a suggestion of providing a self-maintenance platform to maintain attributes and allow new schemes to register.

Considerations for Future Work

In completing this phase of the Existing Schemes' assessment, it is apparent that only a small percentage of the schemes known to exist have provided the data needed to inform our analysis. The EU Commission should consider whether more should now be done to operationalise and enable on-going maintenance of scheme information, as well as share successful practices across less mature schemes.

The following content is not intended to form part of Annex A, but is included to illustrate how, by painting a particular backdrop for the Annex, we can continue to develop and meet the interests of a wider audience.

Preface:

The focus for existing schemes in this report has been constructed principally on the basis of information provided from scheme operators with no emphasis on the challenges faced by organisations starting out on their sharing journey. Based upon limited discussions with organisations either currently disenfranchised from schemes aligned to protection of critical national infrastructure, or just new to sharing situational awareness, a picture might be painted of the facts new participants may need to make informed decisions on engaging in available sharing schemes.

A possible narrative to depict the challenges faced by technology managers in SMEs

Pierre and Greta are peer technology managers in SME's (Critical National Infrastructure relevant suppliers) faced with emerging cyber threats, and are concerned about the growing need to incorporate Cyber Situational Awareness (CSA) within their organisation's security strategies. They have not previously engaged regularly with circles of trust, and outside the ad hoc networking they engage in at conferences and training events, they do not know where to start, or fully understand what the implications are. In addition, there is speculation about the potential requirement for mandatory sharing and incident notification at a regional, national and sector level, which would require Board level engagement, organisational resource positioning and potentially new policy creation.

Pierre and Greta have brainstormed the following list of questions, as part of their agreement to collaborate together, to better position their organisation's cyber security capability. The questions have been grouped into three sections to illustrate how their interests will change in accordance with the growing exposure to circles of trust and scheme engagement:

Section 1 - What must I know and what liabilities do I need to consider before participating?

1. What are the legal, regulatory and contractual requirements to notify incidents and or share cyber situational awareness? What are the consequences of not complying, in terms of financial and other sanctions and who is accountable in their respective organisations?
2. What types of incidents and security alert fall within interests of reporting requirements?
3. What information are they currently able to gather from within their organisations, and who has access to the information? How quickly can it be made ready for sharing?
4. What types of information and intelligence are they interested in receiving, given their cyber threat profile and the incidents befalling their organisations?
5. What schemes are available for them to join within their industry sector (and who provides the intelligence shared to scheme participants)? If there are no apparent schemes, how do they reach out to their peers to create a new circle of trust?
6. Do members of the relevant schemes meet regularly face to face, and what language do they converse in? What type of roles do people in the community share e.g. network defence?
7. How is information actually shared / notified, e.g. by paper report, telephone, email, online portal or a combination of these? What about in an emergency situation?
8. What terms and conditions / protocols do scheme members (most likely all competitors) follow in sharing and reporting information, e.g. do they operate a traffic light protocol associated with the way they expect information shared to be treated?

9. How do they find out what can and cannot be shared and notified, as they are aware certain information may be prohibited from sharing based on national and regional laws, e.g. General Data Privacy Regulation?
10. How are new members wishing to join the sharing community vetted / validated?
11. How many member organisations and participants take part in the schemes and how widely is the information shared? Can the information be shared anonymously?
12. Under what circumstances might information divulged to the scheme be accessible by state agencies or regulators?

Section 2 - How do we get the most from our participation?

The following questions and issues were also determined by Pierre and Greta to be relevant but would likely to require further investigation, once they begin participating in a relevant scheme:

1. What skills and knowledge are required to analyse and process the information shared, and do such personnel require particular levels of security vetting / clearance?
2. Is there any triage / centralised impact assessment performed on the information shared before it is communicated to scheme participants?
3. What security measures are used to protect the information being notified and shared?
4. What process is followed if false-positives are identified?
5. What is the volume of intelligence provided by such schemes and what capacity is typical required to fully participate (consume and publish)?
6. How do they assess which schemes provide greatest value (coverage, timeliness, actionability) and what is the cost of participation? This also needs to be considered in the light of commercial security and threat intelligence service offerings.
7. What will it cost to cover any gaps in information required and what will it take to put the tools and procedures in place?

Section 3 – How do we optimise and safeguard the value gained from participation?

1. How is shared data to be structured or organised, conforming to recognised industry standards and norms?
2. Is it possible to receive feeds of actionable intelligence in machine-readable form, in order to integrate with their existing security control tools?
3. How are duplicate intelligence reports dealt with?
4. Has the capacity and resilience of the scheme infrastructure and operations been risk assessed and appropriate controls and capabilities been implemented and tested?
5. How is the future operation of the scheme safeguarded e.g. has future resourcing of the scheme's continuity been considered?
6. Has the scheme infrastructure been designed and implemented to recognised architectural standards?

Annex B – Context

NISP's approach is to develop a balanced view based on the following context:

- Definitions. Organisations experience cyber security events on a daily basis. Such events may have no impact, such as monitoring a particular threat. Some events may result in a security incident where immediate mitigating action is required, usually to increase Protection or to Respond – this is incident response. Some security incidents may become notifiable by the organisation to one, or more, National Regulatory Authority (NRA) in a Member State (MS).
- The incident notification requirements of the NIS Directive as proposed by the Commission share characteristics with other breach notification legislation including the proposals on the Data Protection Regulation and Electronic Identification and other trust services. Many NRAs for the NIS Directive could also be the NRA for other regulations. Cyber security organisations are involved in providing information for all incident notifications, using the same systems and resources, to all NRAs, so their information sharing has to take this into account.
- Incident Notification
 - ENISA view. Incident notification differs from incident response.
 - It:
 - Is after the fact;
 - assesses the total impact;
 - identifies root causes;
 - documents the actions taken; and
 - describes lessons learnt
 - It is to share experiences with the rest of sector/other sectors and with other government bodies/abroad.
 - It is to exchange, discuss security measures and best practices.
 - It is to inform policy makers, the public and industry so they can assess the risks (i.e. frequency, impact).
 - MS NRAs are free to establish thresholds for incident notification as they please. However, the majority of MS are aligning to the ENISA Technical Guideline on Incident Reporting¹ in Article 13a.
 - Some MS have more stringent notification thresholds than ENISA recommends. Where organisations notify to multiple NRAs (e.g. telcos), this lack of harmonization is an issue.
 - A notifiable incident may result when:
 - There is a service disruption caused by a network or physical infrastructure failure, a natural event, a physical attack or a cyber attack. This includes cyber attacks on physical infrastructures.

¹ <https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0>

- Sensitive information belonging to an organisation is disclosed intentionally or unintentionally in violation of previously agreed or contractual policies or legislation for the storage, use and sharing of such information.
 - Sensitive or privacy information, or personally identifiable information (PII) belonging to a person is disclosed intentionally or unintentionally.
- The identification of events and incidents is based upon:
 - The use of cyber controls frameworks to provide a structured basis for normal operation and also for the detection of abnormalities. These abnormalities are events and may become incidents.
 - A consistent approach to:
 - **Identify** potential risks, threats and vulnerabilities;
 - **Protect** against abnormalities occurring;
 - **Detect** them when they occur;
 - **Respond** to the abnormality (or threat) and enable key business functions to continue operating; and
 - **Recover** to a normal operating state and learn lessons.
- As time marches on, so incident notification is becoming less one-way and more two-way as NRAs see the benefits of information sharing and companies respond by becoming more proactive.
- For most organisations, the same cybersecurity information management systems are used to support information sharing, event management, incident management and incident notification. Better incident notification increasingly depends on better information sharing.
- Information sharing
 - The benefits of information sharing have been proved many times. Most outliers and non-collaborating organisations are at greater risk. The challenge is to increase capacity and re-usable capability across communities and down supply chains, wherever sensitive information exists.
 - Cybersecurity information sharing is increasing to enable collaborative cyber security – one organisation's response can be another organisation's protection. Information sharing enables collaborative cyber situational awareness on which collaborative cyber security depends.
 - Standards-based methods and frameworks are increasingly being used to support collaborative risk management and mitigation of both internal/enterprise risks and external/supply chain/community /shared risks. They also address both static and dynamic risks. This helps provide a shared baseline of 'What is Good' or 'Normality' against which abnormalities and suspicious behaviour are easier to detect.
 - Information protection requires access control. Access control requires authentication and authorisation. Across multiple organisations, this requires federation, based on common policy. For federation to scale requires use of international standards.

- Federation is where multiple authorities work together in a collaborative governance arrangement to develop a Common Policy for trust and interoperability across the community. Trust and interoperability are the foundations for information sharing.
 - Common policy describes the policies, procedures and mechanisms by which the community agrees to collaborate.
 - Inter-federation enables different communities of trust to interoperate.
- Within a successful information sharing community, access control and sharing mechanisms should balance “Need to know” vs “Obligation to share”. Obligation to share is the duty of an organisation to share information for the good of other organisations within the community for collective cybersecurity. This differs from mandatory requirements, which are defined by legislation, regulation or contract, and for which there would be a compliance regime.
- Cross-community relevance. A number of attacks and events impacting the Finance Sector will be relevant to other sectors, e.g. defence, telco.
- Key principles affecting the willingness of an organisation to post information include:
 - Anonymity. There is no information about the posting organisation, the source or the victim.
 - Partial-anonymity is where there is no visible information about the posting organisation, the source or the victim. However, some accountability information is held by a trusted intermediary, who assures the provenance of the information. (See ISO 19191). This helps to protect reputations.
 - Duplication prevention. Sufficient metadata is required to prevent duplicate reports of the same event becoming confused and resulting in the reports being interpreted as many, separate events. Preventing duplication requires, at least, partial-anonymity.
 - Information redaction or filtering. The ability to remove varying degrees of sensitive information in a report for recipients with different access rights, based on Need to Know.
 - Report redaction or withdrawal. The ability for an organisation to withdraw a report that was posted in error or is incorrect, without undue consequences or liability.
- A successful information sharing system should become more resilient as it grows in capacity, capability and functionality. It may mature from initial project > minor support > major support > operational capability for incident management > core capability for cyber security & incident management operations (similar to a command & control system).
- As it grows and becomes more valuable, its attack surface will increase and greater protection will be required.
- Security automation is an increasing requirement to reduce costs, manage more transactions and to reduce error.
- Information sharing methods should be adaptable to manage changing requirements and risks presented by new technologies, including mobile and cloud computing.
- Ownership. It should become possible to fuse proprietary and non-proprietary information, particularly threat intelligence information, whilst protecting the commercial interests of proprietary information providers.

- A liability model(s) should be available to protect the interests of relevant parties in a way that is balanced with achieving community benefit from sharing information.
- General
 - There will be multiple standards and/or specifications for information sharing. This is not a competition; the issue is about interoperability and re-use.
 - Successful national methods or standards can be, or become, internationally recognised and adopted.
 - Analysis will be use-case driven. Successful communities will understand their primary use cases before selecting any framework for information sharing.
 - The requirements of communities (e.g. supply chains, alliances), not individual enterprises, will increasingly drive development and adoption.
 - Methods, standards or framework documents that are freely available at no cost or minimal cost are more likely to have widespread adoption.

Annex B – Standards & Frameworks

Cyber Controls Frameworks

The main risk mitigation frameworks of international interest include the following because they specify cyber controls:

- Internationally recognised and significantly interoperable:
 - ISO/IEC 27002 and 27006 controls. Other ISO 27xxx and 29xxx in support.
 - Australian Top 35 Mitigations
 - US SP800-53 R4
 - SANS 20 Critical Controls – CAG-4
- Other national or industry specific risk mitigation frameworks or standard
 - COBIT 5
 - German BSI 100 series
 - Spanish Magerit

Information Sharing Mechanisms

The mechanisms of interest to the survey include taxonomies and associated transport mechanisms, with a special interest on their ability to support automation.

The main mechanisms of interest include:

Taxonomy

- CIF – Collective Intelligence Framework
- IODEF – Information Operations Description Exchange Format
- OpenIOC – Open Indicators of Compromise
- STIX – Structured Threat Information Expression
- Veris – Vocabulary for Event Recording and Incident Sharing

Transport

- CIF Protocol
- RID – Real-time Inter-network Defense
- TAXII – Trusted Automated Exchange of Indicator Information
- XMPP – Extensible Messaging and Presence Protocol