

# NISP WG2 – Information Sharing and Incident Notification

Chair - Waldemar Grudzien - [waldemar.grudzien@bdb.de](mailto:waldemar.grudzien@bdb.de)

(Chair – Wil Semple until March 2014)

SG 1 – Alan Stockey - [astockey@fsisac.eu](mailto:astockey@fsisac.eu)

SG 2 – Patrick Curry – [patrick.curry@federatedbusiness.org](mailto:patrick.curry@federatedbusiness.org)

SG 3 – Claire Vishik - [claire.vishik@intel.com](mailto:claire.vishik@intel.com)

# Overview of Phase 1

- 250+ organisations signed up, 50+ initially active, tailing off to ~20. All volunteers. Insufficient support for admin and communications.
- Requirements for incident notification not defined. Treated as a subset of information sharing, driven by wider needs, not just the NISD.
- Confusing direction – what needs to be done vs guidance for SMEs? (Can't have the second without the first)
- Single initial survey with two parts:
  - Qualitative for organisations
  - Quantitative for information sharing schemes
- Finding - Information sharing is a hot topic
- Phase 1 has been a reconnaissance – much more could and should be done
- WG2 report:
  - Describes the current situation and organisations' views
  - Recommends what needs to be done
  - Provides a set of questions to help organisations form sharing communities

# Initial Findings from Surveys and Experience

- Different levels of maturity and understanding – industry and governments.
- Industry well ahead of governments
- Immature strategic collaborative situation. Requires collaborative leadership and coordination of multiple stakeholder interests.
- Nations depend on industry. Governments behaviour is to control not collaborate with industry. Industry needs to see this change. Consumer, industry and government scopes are highly interwoven due to the reality of more data being shared more widely by more organisations.
- Communities share information. Progress is by communities that could benefit NISP. The focus should be on sharing communities.
- Other strategic drivers and initiatives are relevant to NISP
- 8 major responses to the qualitative survey
- 32 information sharing schemes responded to the quantitative survey
- Major comments
  - Lack of time to respond – need more time
  - Not in a position to respond
  - Wrong people engaged in the organisation or don't know who to ask
- Organisations want to engage with NISP if it is going to help them. Need for confidence.

# Organisational Survey – 20 Questions

## **Organisational info**

1. Contact info for follow ups
2. Nature of the business
3. Major risks and challenges

## **Incident Notification**

1. Incident notification approach
2. Incident notification with partners
3. Examples of important incident notifications
4. Challenges for incident notification

## **Information Sharing**

1. Importance of info sharing: Identify, Protect, Detect, Respond Recover
2. Key elements for info sharing
3. Collaborative capabilities required
4. Kinds of info to share, and concerns
5. Concerns about info management and quality
6. Critical and Priority Information Requirements and sharing
7. Publicising incident information
8. Information release procedures and TLP
9. Use of recognised information sharing schemes and cyber controls frameworks
10. Experience of schemes and cyber controls frameworks
11. Gaps and improvements
12. Barriers to adoption of best practices, particularly in support of EU Cyber Security Strategy
13. Provide reference documents

# Organisational Survey

- Barriers to Entry
  - Suspicion and lack of understanding
  - Lack of a community behaviour or a community to join
  - Duplicate reporting
  - Quality of one scheme's information vs another's
  - Reputational damage
  - Liability
  - Clear value to the organisation
- Challenges to growth and benefit include:
  - Trust
    - Based on Authentication, Authorisation and Assurance (AAA)
    - Need to know vs Obligation to share
    - Different levels of collaboration and trust
    - Partial Anonymity and Anonymity. Requirement for a trusted intermediary
    - Liability and ability to retract posted data without impact
  - Interoperability
    - Policy and data interoperability
    - Baseline for interoperability and reuse. Key - cybercontrols frameworks and assessment tools based on ITIL → **Normality**.
  - Implementation issues. Point solutions don't scale. Requirements for:
    - Federated trust at high assurance (ISO 29115)
    - Interoperability – Taxonomies (IODEF, STIX, OpenIOC, Veris, CIF) and protocols (CIF, RID, TAXII, XMPP)
    - Security automation
    - Detection and decision support
- Also
  - Major differences in maturity
  - Other initiatives are further ahead, sharing is growing. Standards and best practices exist but are only being used by a few leaders
  - Organisations spending money on point solutions and reinvention, which can't scale

# Scheme Surveys - Questions

- What exists today / tomorrow?
  - How might the scheme landscape be sized and characterised?
- What are the most common scheme features?
- Who can provide us with qualified data about existing schemes?
- What direction are the more mature schemes heading in?

Points of interest:

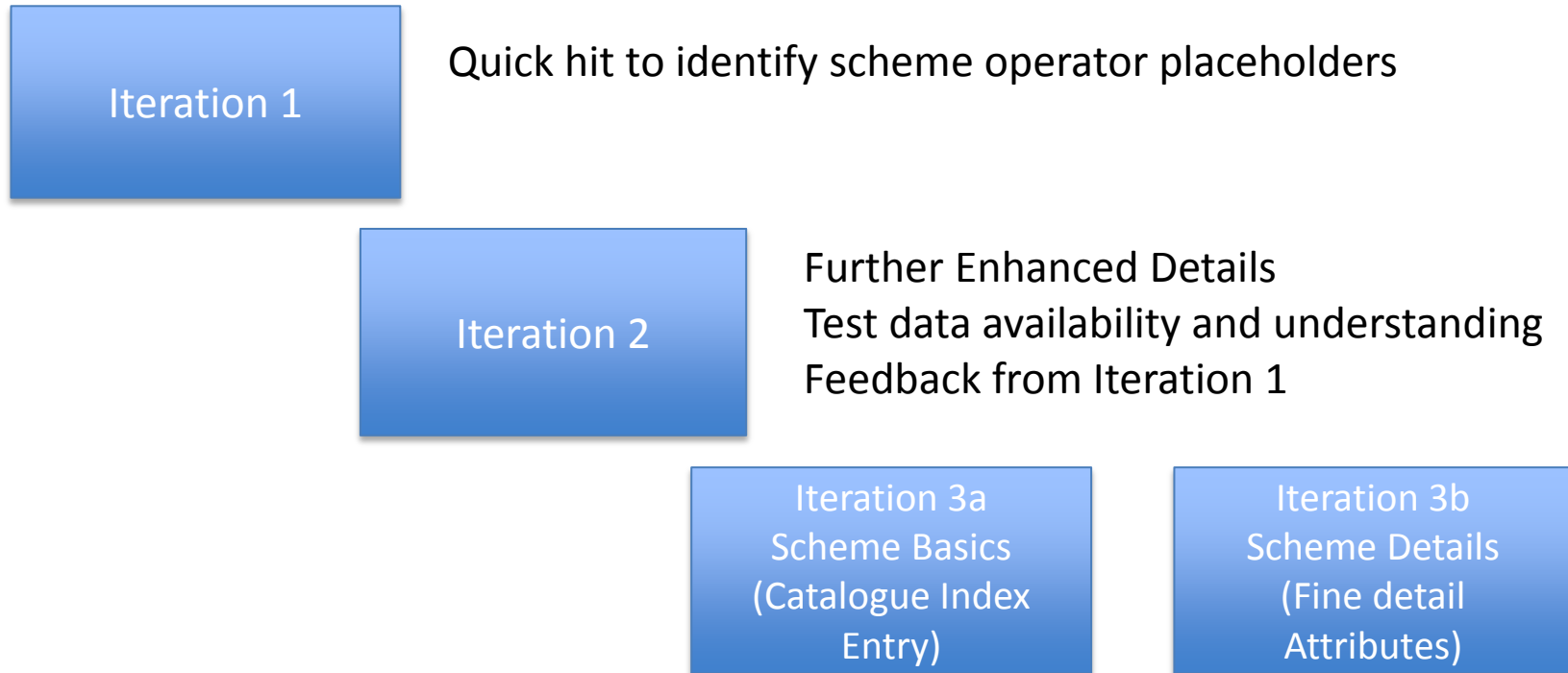
- Potential size of scheme landscape
- Some schemes don't want to publicise
- More than just CERTs

*All from a scheme operator, rather than scheme participant perspective!*

## Summary of 32 Scheme Responses

	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	

# Existing Scheme Data



Potential Scheme Landscape: 28 Member States+2 x 30 Sectors = 900 Schemes  
(comparison ENISA reports: 42 CERTs in 2010 – 220+ CERTs in 2013)

- Plus regional and international schemes
- Plus breakout of Information Sharing Schemes from dedicated Incident

Schemes

***So far we have received data from approx 30. schemes, <3% of possible landscape***



# Scheme Data -> Basic Analysis

## Iteration 3a Scheme Basics (Catalogue Index Entry)

## Iteration 3b Scheme Details (Standards & Attributes)

### *Example:*

Scheme Name:	FS-ISAC
Scheme Operator:	FS-ISAC Inc.
Scheme Origination:	1999
Scheme Website:	www.fsisac.com
Scheme Geography:	International
Sector Relevance:	Finance Sector
Incident or Sharing:	Information Sharing
Free / Subscription:	Subscription*
Scheme Participation:	Discretionary
Sharing Protocol:	Formal – TLP
Attribution:	Anonymous+
Scheme Participants:	Threat Intel. / Network Defender
#Scheme Members:	4500
Scheme Technology:	Portal / Email / Phone
Physical Meetings:	Yes - English
Automation Support:	Yes
Scheme Maturity:	3->4 / 5

### Detail sub-headings:

- Scheme Membership & Governance
- Scheme Assurance & Resilience
- Sharing Operations
- Scheme Infrastructure
- Sharing Automation
- Scheme Security
- Scheme Meetings & Interest Groups

***A standardised data model of key attributes and a recognised maturity scale beneficial***

# Report Recommendations

1. Establish **NISP collaborative governance** for progress with **adequate dedicated resources to maintain momentum and navigate wider NISP bureaucracy**
  1. Neutral collaborative The Steering Group - Commission, industry and governments + support
  2. Dedicated Working Groups
  3. Encourage wider active participation, particularly from law enforcement and national cybersecurity organisations.
2. To develop a **set of collaborative objectives and tasks in an Outline Plan**, based on the work already done
3. To leverage the existing work, including the spreadsheet of information sharing schemes, the survey responses, the experiences and the reference documents
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 and maintain 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**.

# NISP Plenary meeting, 30 April 2014

## WG2–Chair's thoughts

# My thoughts as the convener – the “tenth man”

- What if, instead of carrying on doing “business as usual” – i.e. highly focused, with a rigid hierarchy, hard targets and challenging tasks – we tried taking a longer view?
- What do we want?
  - Transparency and control or
  - Trust and responsibility?
- What does the European Commission want?
- What does the European business community want?

# Experience with a national NISP since 2006 – #1

- Business community and state start off in a spirit of cooperation in 2006.
- Genuine trust is established between the two (we're talking about a process which kicked off at the beginning of 2006 and takes time).
- A few industries, most of which aren't involved in the NISP, pay no attention to the state's objectives.
- State responds with IT Security Bill draft (same objectives as NISD). This will apply to everyone, including NISP participants. Transparency and control arrive.
- Business community is annoyed. Cooperation stalls.

# Experience with a national NISP since 2006 – #2

- Draft legislation intends to introduce
  - incident messages (transparency) and
  - minimum security standards (control)
- IT-based businesses normally have adequate security standards in place already. The first point is causing more headaches (among other things, no thresholds are envisaged).
- I can now see history repeating itself at European level.
- By the way, I've been head of the German NISP since 2008.

# What do we want? #1

- “Transparency and control” or “trust and responsibility”?
- Is it possible to have trust and responsibility despite transparency and control?
- What does the European Commission want?
- What does the European business community want?
- As I see it, businesses currently feel coerced into working on something they can no longer change.
- Transparency and control are being forced on them.
- This is no basis for mutual trust. Nor, in my view, for long-term success.

# What do we want? #2

- Why has this happened?
  - Have businesses not defended themselves successfully against all possible threats to their IT and their customers?
  - What is the state doing to help businesses cope with threats which are too much for even the biggest company or sector?
- The business community needs to decide to what extent it's prepared to carry on as before.
- The state needs to decide whether transparency and control is really the best approach.