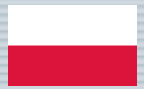
Barriers to CSIRTs cooperation. Challenge in practice – the CLOSER Project

Krzysztof Silicki

Mirosław Maj

NASK / CERT Polska



20th FIRST Annual Conference, Vancouver

SENSE OF TELECOMMUNICATION NASK

Introduction

- **Base material for this presentation**
  - CERT Polska experiences
  - International cooperation initiatives
  - The CLOSER project

- **Big part of the paper is a part of document issued by European Network and Information Security Agency (ENISA) – "CERT Cooperation and its further facilitation by relevant stakeholders < http://www.enisa.europa.eu/cert_cooperation> as authors of this paper were involved in preparation of ENISA document.**

How to improve a cooperation – FOCUS ON IMPROVING SERVICES!

PRACTICAL ASPECT

We believe that different observations on CSIRTs cooperation and recommendations resulting from those observations can be very practical and can be used in other initiatives. One concrete example is a CLOSER project which is generally about building and enhancing cooperation of CSIRTs.

Benefits of cooperation

- **Since there is no doubt that cooperation is beneficial in CSIRT community the main areas of cooperation may include:**
  - Incident handling
  - Project conducting
  - Information sharing
  - Networking

Benefits related to common incident handling

- Since incidents reported to CSIRTs are international, a good cooperation in incident handling is critical
- An important thing is that an information exchanged during the incident handling process is very often sensitive (activity of internet underground groups, successfully attacked organizations, plans of internet criminals, detailed analysis of malicious code, electronic evidence etc.)
- Long term and effective exchanging of incident data can result in the setting up of a regular exchange of incidents data related to the constituencies of cooperating CSIRTs.
- It gives a big improvement of the quality of the incident handling process and significant reduction of workload of CSIRTs

Benefits related to common project conducting

- A cooperation between CSIRTs gives them the capability for better recognition of their common areas of interest:
  - their competence,
  - their goals and also
  - a chance of building trust.
- Based on this recognition some teams have embarked on closer cooperation.
  - eCSIRT.net (http://www.ecsirt.net/) project.
    - European CSIRT teams
    - TERENA TF-CSIRT
    - Accredited Teams within Trusted Introducer Initiative
    - national level.
  - HoneySpider Project
    - GOVCERT.NL / surfCERT / CERT Polska initiative
- There are also examples of not strictly formalized cooperation. Teams work together on similar problems related to their projects. They exchange ideas, solutions or even source code.

Benefits related to information sharing

- **Information sharing - probably one of the most effective ways of cooperation**
  - sometimes used as a synonymous term for cooperation
  - should be applied to concrete tasks, initiatives and projects
  - good to relate information sharing to the particular kind of resources and services provided by CSIRTs.

- **Different kinds of resources which can be shared and benefits related to them ("information sharing" treated very widely)**
  - Knowledge and experience sharing – regular, formal or informal, exchange of information about issues related to IT security.
  - Staff exchange – a method of exchanging information and experience by exchange of personnel.
    - Also a method of mentoring new teams of organizations which just started to establish a CSIRT
    - Benefit: Team staff can learn in detail about methods of daily work, procedures and techniques
  - Technology sharing – by technology sharing CSIRTs
    - give an opportunity of direct usage of concrete technical solutions which can improve the quality of the services .
    - A good examples:
      - Request Tracker for Incident Response as the enhanced version of Request Tracker, made available by JANET CERT , or the CHIHT – Clearing House for Incident Handling Tools – where different teams share their knowledge and software which they use daily - http://chiht.dfn-cert.de/)
      - joint development of new tools (e.g. RTIR group within TF-CSIRT - http://www.terena.nl/activities/tf-csirt/rtir.html).
    - Benefits of technology sharing include:
      - access to well developed and verified incident handling and security tools,
      - support in the resolving of a technology related problems,
      - support in technical analysis of incidents (especially malicious code analysis).

Benefits related to networking

- Networking is a crucial factor for building trusted relationships between CSIRTs
- Planned meetings, workshops, conferences, regular exchange of information (e.g mailing lists), working groups
  - great benefit resulting from the simple fact that people gather in one place and have an opportunity to talk to each other and to get know each other better
  - in effect, they learn about business more and more and they find the most convenient and effective way areas of common interest.
- Very often - a first step to a closer and more formal cooperation between teams.

Barriers – another side of the story

- Cooperation results then in many positive effects for parties involved
- Unfortunately there are also some barriers which can limit or even make cooperation impossible
- Some of them, identified as probably most important, are listed further:
  - Lack of standards
  - Finanancing barriers
  - Lack of agreed level of service (SLA)
  - Differences in legal systems
  - Insufficient organizational and political support

- Questions:
  - Obstacles, when identified: can they be resolved?
  - What is worth to concentrate on to facilitate CSIRT cooperation?

Lack of standards

- Although the first CSIRT team was established 20 years ago (1988) today still there is no well developed standard of CSIRT operation (although there are some best practices like e.g. RFC 2350 "Expectations for Computer Security Incident Response"). This drawback is very important from the point of view of developing the cooperation.

Barriers to CSIRTs cooperation. Challenge in practice – the CLOSER Project

Missing standard	*Consequences*
Incident classification (IODEF – Incident Object Description and Exchange Format)	*Lack of common statistics* *Ambiguous threat assessment* *Impossibility of phenomena assessment scale*
Data Exchange Format (IDMEF – Intrusion Detection Message Exchange Format)	*Delayed exchange of significant data* *Automatic incident data processing and handling more difficult*
Incident handling process	*Unknown reaction time* *Unknown resolving problem time* *Unknown procedure sequence tracking*
Set of incident related data record	*Lack of some data important for problem resolution*
Format advisory (EISPP Common Advisory Format Description) (VEDEF - Vulnerability and Exploit Description and Exchange Format)	*Additional overhead in preparing own versions of advisories instead of using existing ones* *Delayed reaction to threats*
Threat assessment (CVSS – Common Vulnerability Scoring System)	*Change management decision is difficult* *No change in the solution configuration when needed*

Finance

- Closer levels of cooperation lead to larger financial expenses.
- Only the very basic cooperation activities like common mailing lists or some information sharing electronic platform are a very low cost issue (but even they are usually consequences of earlier meetings, workshops, conferences and so on).
- Building a valuable level cooperation is therefore also a money issue.

Thus money can be a barrier in building cooperation.

Lack of Service Level Agreements (SLA) between cooperating CERTs

- Especially concerns the team-team model of cooperation
- It is not a barrier which completely blocks cooperation between teams but it can slow down the process.
- The incident handling process is the most afflicted (especially request-response sequence.
  - In the CERT world there is no culture of establishing strict rules of reaction and the time of the problem resolution. Such a situation is not conducive to development of cooperation.
- As SLA can be recognized as a too strong model of a commitment for CERT cooperation – we propose Declared Level of Service solution
- this barrier is very much related to other ones like *Differences in Legal Systems* or general *Lack of standards*.

Differences in Legal Systems

- Different CSIRTs work in different environments.
  - must to fulfill the requirements and operate in accordance with the legal system of the country they function in.
- Obvious issue that has consequences in the way of providing services.
  - it impacts how, when and to whom they can make available data which CSIRTs process (same with exchanging them).
  - particular kinds of network attacks can be differently treated in different countries – this concerns international cooperation but not only.
- Even in the same country legal rules may not be the same for the collaborating parties. Affiliation to a specific sector may force adherence to specific regulations.
  - E.g. regulations for Internet Service Providers concerning provider data retention requirements.
- Internal regulations of organizations where CSIRTs operate
  - General regulations,
  - more detailed, such as security policies,

  can include rules for dealing with information and other organizations' data.
- Concerns information sensitive sectors like finances or public administration.

Insufficient organizational and political support

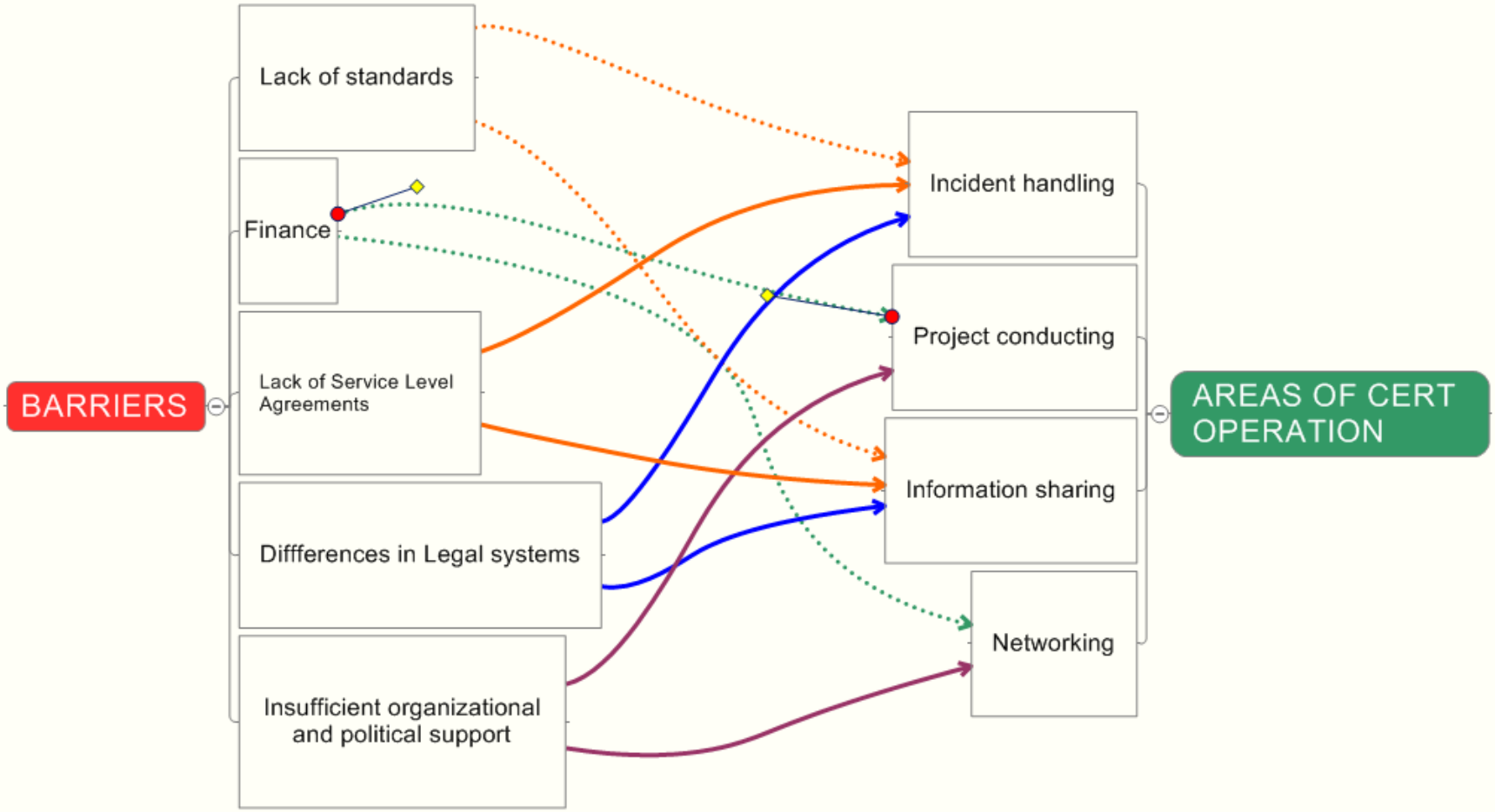
- Usually CSIRTs are from a formal point of view part of bigger organisations like universities, corporations, public administration bodies etc,
- Their role may often not be seen as "mission critical" from organisation point of view,
- This may result in not enough support from the management. This can have negative impact on CSIRT cooperation.
  - the management of a parent institution either may not understand the benefits resulting from supporting IRT capability or considers cooperation impossible because of competition issues,
  - but cooperation among CSIRTs of competing companies may work very well on this level, for example in FIRST, TF-CSIRT, the German CERT-Verbund, Polish Abuse forum. So this specific barrier is probably only virtual and can be abolished quite easy.
  - important task for CSIRT teams: to brief their higher management about the necessity of CSIRT cooperation and the resulting benefits to the organisation.
- One of the interesting initiatives that potentially could lower this barrier is the Corporate Executive Programme (CEP) initiated by FIRST..

POLISH ABUSE FORUM

- One of the ideas of improving incident handling, within the teams operating in the same geographical region
  - informal group of teams which meet regularly and discuss methods of cooperation
    - Germany,
    - The Netherlands,
    - Austria,
    - Poland

- Polish case
  - The forum was initialized by Research and Academic Computer Network in Poland (NASK) and operating within NASK – CERT Polska team.
  - The forum meets quarterly and regularly more then 10 members are present.
  - The main topics of discussion and activities are:
    - Cooperation between forum teams and LEAs in Poland
    - Exchanging of experiences between the teams, especially related to the operation of a team within their company organizational structure and methods of contacting and cooperating with the teams' constituencies.
    - The undertaking of technical actions in the teams' networks, with the goal of improving the security of the teams' parental organizations, as well as their customers (e.g. blackholing project).

Barriers to CSIRTs cooperation. Challenge in practice – the CLOSER Project



Influence of cooperation on CSIRT's services improvement

Matrix presents the relation between a set of services and the influence of cooperation on their better performance and improvement. The list of services is based on the list provided by CERT Coordination Center (http://www.cert.org./csirts/services.html). This list is shortened by merging some categories and representing them by one which relates to the cooperation issues the most (e.g *technology watch* represents also *announcements* and *security-related information dissemination*).

Barriers to CSIRTs cooperation. Challenge in practice – the CLOSER Project

Services / influence of cooperation	Low	Medium	High
Alerts and Warnings			√
Incident Handling			√
Vulnerability Handling		√	
Artifact Handling		√	
Technology Watch [1]			√
Configuration and Maintenance of Security Tools	√		
Development of Security Tools		√	
Intrusion Detection Services [2]		√	
Risk Analysis	√		
Awareness Building		√	
Education/Training		√	
Product Evaluation and Certification		√	

Recommendation: Declared Level of Service (DLoS)

This recommendation especially concerns the team-team model of cooperation.

- In the CSIRT world there is no culture of establishing strict rules of reaction and the time of the problem resolution.
- Also there are no generally known examples of collaboration in accordance to an agreed upon service level agreement (SLA).
- Lack of DLoS does not completely block cooperation between teams but it can slow down the process.
  - One specific problem concerns the incident handling process and especially request-response sequence.
- DLoS: declared procedure and timeframe of response or particular action to be taken by CSIRT – should exist.
  - this is important not only in cooperation between CSIRTs but also in communication with their constituency.

INHOPE case

Good example of cooperation between response teams is INHOPE organization which was established in 1999 under the European Commission Safer Internet Action Plan <*http://ec.europa.eu/information_society/activities/sip/index_en.htm*>.

INHOPE *http://www.inhope.org* is an international association of internet hotlines which the main area of operation is fighting with illegal content in the internet.

- This kind of security (or rather safety) response team is much younger then the CSIRT concept
- After few years of operation community of hotlines was able to develope own standard of reaction, exchanging of information and even statistics, what is still not always possible within CSIRT teams.
- It is worth to analyze methods of cooperation within INHOPE and implement the best practices in CSIRT's world.

Recommendation: Information Handling Improvement

- During the incident handling process as well as other IT security related activities, CSIRTs have contact with very sensitive information.
- Processing of such a data is very often regulated by law.
  - regulations impose many limits on the exchanging of information and its usage for different purposes (especially in international cooperation).
  - teams may be not allowed to share sensitive and important information with other teams.
  - in such case they can produce abridged information
  - in case of collecting incident related evidence – a workaround could be the protection of sensitive data before appropriate parties (e.g. LEA) turn to CSIRT for requested data.

Recommendation: Mentoring schema, filling the gaps

- The idea is to build a good, long-term operational relationship between experienced teams and the new ones
  - This process can be active, facilitated by various relevant stakeholders (e.g. TERENA TF-CSIRT, CEENet and ENISA).
  - It could be based on a plan how to fill the existing gaps on the map of CSIRT services, constituencies and geographical areas
  - The practical example of such activity is the CLOSER project
- Who should be contacted?
  - Ideally, there should be a single point of contact in each country, keeping current network of local contacts.
    - In order not to repeat the co-ordinational and hierarchical approach from not working, past initiative EuroCERT, the national point of contact should not be a point to report an incident, it should just direct the reporter to appropriate contact. The point of contact could be established by a national CSIRT or as an institution not affiliated with any CSIRT in particular e.g. by a telecommunication regulatory authority.

CLOSER Project

Funded by NATO Public Diplomacy Division, Network Infrastructure Grant #983081

- CERT Polska
- AzNET-CERT / GRENA CERT

Assistance

- CEENet
- SURFnet CERT

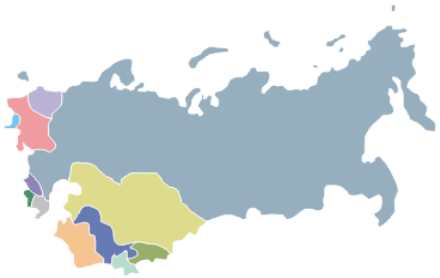
CLOSER Participants

Belarus
Ukraine*
Moldova*
Georgia*
Azerbaijan*
Armenia*

Kazakhstan
Uzbekistan
Kyrgyzstan
Turkmenistan
Tajikistan

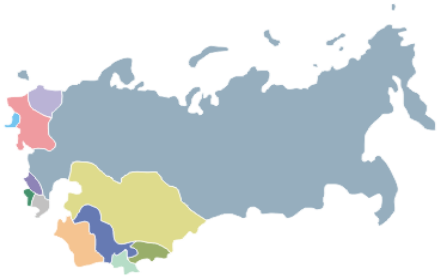
11 National Research Education Networks from CIS

CLOSER Goals



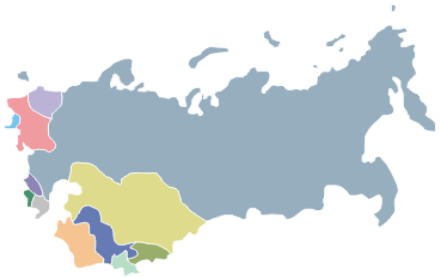
- **Organization of the cooperation among CEENet members with newly established CSIRT**
- **Developing infrastructure for providing well developed CSIRT services**
- **Assistance in joining international CSIRTs forums**

CLOSER Tools



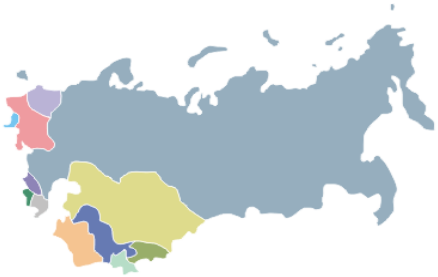
- Coaching the new teams
- Operational cooperation on daily basis
- Conferences
- Trainings

CLOSER Steps



- Information dissemination
- Survey based on the ENISA "A step-by-step approach on how to set up a CSIRT"
- Development of projects website
- Setting up constituency
- Setting up a "network"

CLOSER Targets



- Ready technical infrastructure for CERTs work
- Ready procedures and ongoing daily cooperation within network
- At least 10 well developed CERT teams in CIS
- 5 new members of FIRST
- 20-30 trained CERT officers

CSIRT cooperation improvement and CLOSER project

- Establishing the same of similar procedure of incident handling. This gives a chance to build the same of similar method of operation by different CSIRTs (maybe some SLA framework)
- Building information sharing infrastructure, like IRC channels and mailing lists, which are used for regular exchange of information
- Contacting with management of organizations where the new teams are established to explain the role, benefits and importance of CSIRT concept. This gives a support for CSIRT members
- Convincing new teams to build in proper way, from the very beginning of their operation, relationship with their constituencies and other security and response team in their countries
- Promoting a common statistics

Upgraded concept of CSIRT cooperation.

- We can consider the network of CSIRT collaboration of today as a basic "version 1" with some "sub-releases" featuring a set of enhanced functions (version 1.x) – eg. in case of cooperation between members of regional initiative or sector cooperation
- There is a need to "upgrade" this network to version 2 ("Next Generation CSIRTs") This could include ideas presented and other obvious ones:
  - DLS (Declared level of Service)
  - IHI (Information handling Improvement)
  - Implementation of common standards and tools
  - Active participation in deployment of network of contacts and international cooperation
  - Mentorship programs
  - Involvement in awareness raising

DLS (Declared Level of Service)

- As a basis for DLS the set of CSIRT services should be defined by each team and published.
- It is recommended that when the set of services is defined for a particular team:
  - relation between the most important services (e.g. Incident Handling, Vulnerability Handling, Alerts and Warnings),
  - declared procedure and timeframe of response or particular action to be taken by CSIRT – should exist.
- This is important not only in cooperation between CSIRTs but also in communication with their constituency.

IHI - Information Handling Improvement (or Enhancement).

- Various kinds of information is exchanged among CSIRTs and between CSIRTs and their constituencies.
- If parties agree on some protocol or scheme of sharing information there is less hesitation in sharing in concrete situations.
- It is recommended to classify information and to attribute particular labels to every piece of information (mail, alert, advisory) which clearly shows how it is to be handled by a CSIRT (or other party).
  - some information should be encrypted,
  - some are of limited distribution,
  - others are dedicated only for internal use.
- The "next generation CSIRT" should have policy of handling information which is known to peer parties and also should expect the same from cooperating teams.

COMMON STANDARDS

- The possibility of implementing common standards is currently limited by their availability.
- In order to allow for easy and effective sharing of incident related data, clearly some standardization is needed that would facilitate handling of incident related data, proper prioritization and comparison of trends and statistics between different teams.
- Along with the standards, tools supporting them need to be developed. In the future, CSIRTs should be able to use common set of tools for everyday incident handling.

CSIRTs v.2

- Participation of CSIRTs in regional or international initiatives seems to be one of the most successful means to build a network of live contacts which supports the increase of trust between teams as well as sharing expertise.
- These initiatives could be:
  - joint research projects,
  - negotiating common standards deployment (working groups),
  - workshops or teleconferences.
- Participation in various initiatives can also be an opportunity for engaging in mentorship process with new teams, and such mentorship should be a role for CSIRTs v.2 as mature and experienced teams.

And… awareness raising!

- Awareness raising programs
  - hopefully growing in most European countries
  - good opportunity for CSIRTs to communicate their role in local community
  - an idea can be establishing relation between CSIRTs and "Safer Internet" program in every country.
    - There is an example of such cooperation in Poland between CERT Polska and Saferinternet.pl (http://saferinternet.pl/) program initiated and being carried out as the parent organization (NASK) is involved in both projects.

Thank you for your attention!

Questions?

Krzysztof.Silicki@nask.pl
Miroslaw.Maj@cert.pl