Cybersecurity Incident Taxonomy

CG Publication 04/2018

NIS Cooperation Group

July 2018

ABOUT

This document has been drafted and endorsed by the NIS Cooperation Group members.

The Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), has been established by Article 11 of the Directive (EU) 2016/1148 'concerning measures for a high common level of security of network and information systems across the Union' (NIS Directive). It facilitates strategic cooperation between the Member States regarding the security of network and information systems.

Contents

1 Introduction

This document proposes a common, simple and high-level taxonomy to classify cyber security incidents at the strategic and political level.

This document is developed by NIS Cooperation Group (NIS CG) work stream 7 on Large scale cybersecurity incidents, which is led by experts from Bulgaria, supported by experts from ENISA and involving the European Commission. It consolidates input and comments from all members of the NIS Cooperation group.

1.1 Target audience

This document targets members of the NIS Cooperation group, experts from national and sectorial authorities, CSIRTs, and EU Institutions who are involved with (large-scale) cyber security incidents.

1.2 Goal

The goal of this document is to offer a common taxonomy for large scale cybersecurity incidents, as mentioned in the Commission Recommendation of 13 September 2017, also known as the blueprint. This taxonomy has been welcomed by the General Affairs Council in its conclusions on '*EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*'[1].

This taxonomy is to be used for the purpose of incident response coordination activities at Union level carried out in the framework of the Integrated Political Crisis Response (IPCR) arrangements. The scope of this taxonomy is cybersecurity incidents in general, for the sake of completeness.

This taxonomy could be useful also for information sharing across borders, annual summary reporting under the NIS directive, and international collaboration and information sharing.

It is important to underline here that this taxonomy addresses only the 'naming' of cybersecurity incidents, and it does not address the 'processes' for example for notifying or escalating incidents. Moreover, this incident classification does not exclude the use of additional taxonomies, such as sectorial taxonomies, in case a more specific classification is needed.

1.3 Versions and changes

This is a living document and may be updated by the NIS Cooperation Group, periodically, when necessary.

Note that compared to earlier draft versions, several passages and sections (with information about processes like IPCR, more detailed technical concepts and background) have been moved to a separate accompanying document with reference material, to provide a basis for further work by the NIS cooperation group.

[1] Council conclusions 10086/18, adopted by the General Affairs Council at its 3629th meeting held on 26 June 2018.

2 Policy context

2.1 Legal reference

For the sake of reference, we report verbatim the relevant parts of the Recommendation (blue print).

2.1.1 Recital

(20) Awareness and understanding of the real-time situation, risk posture, and threats gained through reporting, assessments, research, investigation, and analysis, is vital to enable well-informed decisions This 'situational awareness' - by all relevant stakeholders - is essential for an effective coordinated response. Situational awareness includes elements about the causes as well as the impact and origin of the incident.

2.1.2 Recommendation

(7) Member States, with the assistance of ENISA and building on previous work in this area, should cooperate in developing and adopting a common taxonomy and template for situational reports to describe the technical causes and impacts of cybersecurity incidents to further enhance their technical and operational cooperation during crises. In this regard, Member States should take into account the ongoing work within the Cooperation Group on incident notification guidelines and in particular aspects related to the format of national notifications.

3 Scope

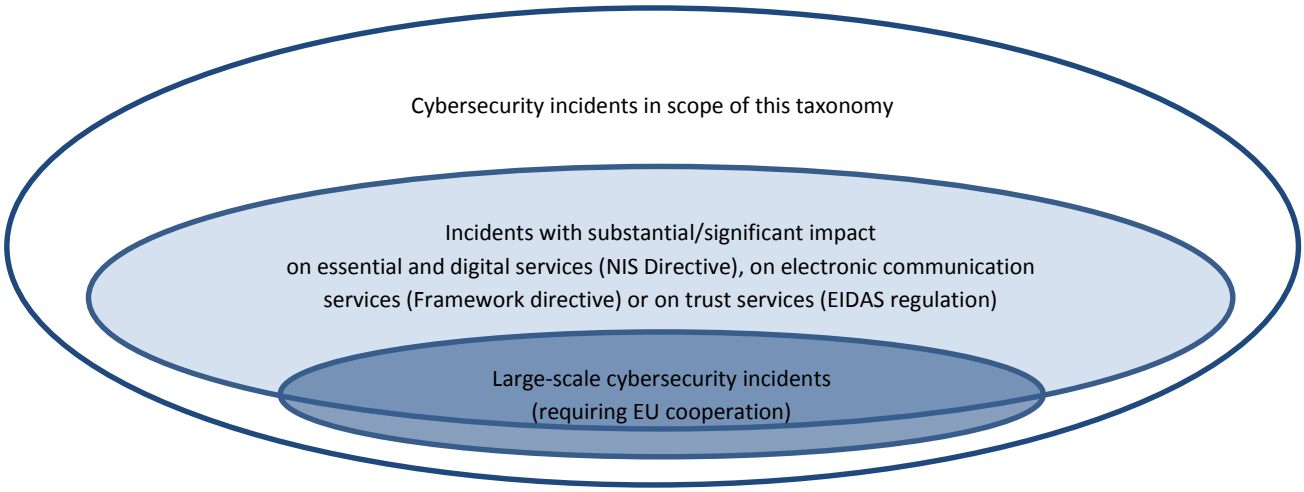
The scope of this taxonomy is defined as follows.

Incidents affecting the security of network and information systems, in any sector of society.

As mentioned, while the focus of this taxonomy is on large-scale cybersecurity incidents requiring EU cooperation, the scope of the taxonomy is broader. The scope for instance includes also,

- incidents with a substantial impact on essential and digital services, which have to be notified to national competent authorities under Article 14 and Article 16 of the NIS Directive,
- incidents with a significant impact on electronic communications, which have to be notified to national authorities under Article 13a of the Framework directive, and
- security breaches with a significant impact on trust and identification services, which have to be notified to supervisory bodies under Article 19 of the EIDAS regulation

The scope of the taxonomy is illustrated in the Venn diagram below.



4 Taxonomy

The taxonomy has two core parts: The nature of the incident, i.e. the underlying cause, that triggered the incident, and the impact of the incident, i.e. the impact on services, in which sector(s) of economy and society. The taxonomy is structured as follows.

1. **Nature**
    - **Root cause category**, i.e. what triggered the incident, see Section 5.1:
        - System failures
        - Natural phenomena
        - Human errors
        - Malicious actions
        - Third-party failures
    - **Severity of the threat**, see Section 5.2:
        - High
        - Medium
        - Low
2. **Impact**
    - **Sectors impacted**, i.e. where services are impacted by the incident, see Section 6.1:
        - Energy
        - Transport
        - Banking
        - Finance
        - Health
        - Drinking water
        - Digital infrastructure
        - Communications
        - Trust and identification services
        - Digital services
        - Government services
    - **Scale of the impact**, nationally, for economy and society, see Section 6.2
        - Red – very large impact
        - Yellow – large impact
        - Green – minor impact
        - White – no impact
    - **Outlook**, i.e. the prognosis, regarding the impact, for economy and society:
        - Improving
        - Stable
        - Worsening

Detailed semantics are explained in sections 5 and 6.

Optionally, both the nature and impact may be further specified, using labels, between parentheses. For example, a denial of service attack may be labeled as: malicious-action (availability, DDoS attack).

Impact on a payment gateway may be labeled as: finance (payment-gateway). In Section 7 we reference some commonly used terms and taxonomies for the purpose of this additional labelling.

To illustrate the taxonomy we give some examples.

- A large shipping firm is hit by malware, paralyzing its operations. Many workstations and lots of data is lost. It is not clear if the malware is sabotage or ransomware. It seems the software vulnerability that is exploited is quite old. All up-to-date software versions are not affected: **[malicious-actions (malicious code), medium; transport-maritime (port), red, stable]**

- A software update disabled core SCADA/ICS systems in a power plant, causing a major power blackout in the country. There are cascading effects in many critical sectors like telecoms and transport: **[system-failures (maintenance error), low; energy-electricity (power plant), red, worsening]**

- A major DDoS attack blocks a particular payment service in one country, severely disrupting daily life. The situation gets worse and worse in a few hours. More and more people have to walk back home from work because the public transport cards are not working: **[malicious-actions (availability, DDoS), high; finance (payment-gateway), red, worsening].**

- A fire caused by a broken fuse in a coffee machine completely destroys a major site of an IXP. Internet connectivity is slow across the north-west of Europe, and some major websites are hard to reach: **[system-failures (fire), medium; digital-infrastructure (IXP), yellow, stable].**

- There is a major power cut for hours in a large part of the country, causing outages of the mobile telephony network. Some base stations have diesel generators. Fixed lines connections are working normally, but mobile connectivity is impaired due to overload. There are cascading effects in many sectors: **[third-party-failures (power-cut), high; communications (mobile), yellow, worsening]**

5 Nature of the incident

The first part of the taxonomy is used to classify the nature of the incident, i.e. the type of threat that triggered the incident, the severity of that threat.

5.1 Root cause category

The Root cause category is used to indicate what type event or threat triggered the incident. Root cause categories are mutually exclusive. The taxonomy distinguishes 5 root cause categories:

- **System failures -** The incident is due to a failure of a system, i.e. without external causes. For example a hardware failure, software bug, a flaw in a procedure, etc. triggered the incident.
- **Natural phenomena -** The incident is due to a natural phenomenon. For example a storm, lightning, solar flare, flood, earthquake, wildfire, etc. triggered the incident.
- **Human errors -** The incident is due to a human error, i.e. system worked correctly, but was used wrong. For example, a mistake, or carelessness triggered the incident.
- **Malicious actions -** The incident is due to a malicious action. For example, a cyber-attack or physical attack, vandalism, sabotage, insider attack, theft, etc., triggered the incident.
- **Third party failures -** The incident is due to a disruption of a third party service, like a utility. For example a power cut, or an internet outage, etc. triggered the incident.

Note that in some situation the categorization of the root cause may change over time, as more is known about the incident. Something that seems at first a cyber-attack, may turn out to be a human error, and vice versa.

5.2 Severity of the threat

The severity of the threat is used to indicate, from a technical perspective, the potential impact, the risk associated with the threat. For example, the severity is high if an upcoming storm is exceptionally strong, if an observed DDoS attack is exceptionally powerful, or if a software vulnerability is easily exploited and present in many different systems. For example, in certain situations a critical software vulnerability would require concerted and urgent work by different organizations.

- **High** – High severity, potential impact is high.
- **Medium** – Medium severity, potential impact is medium.
- **Low** – Low severity, potential impact is low.

Factors to take into considerations when assessing the severity of the threat:

- Risks for organizations, taking into account likelihood and potential impact
- Amount of additional effort or costs needed to mitigate, protect or recover
- Potential damages for the organization, which could be caused by the threat
- Rate of spreading (aggressiveness) of the threat, for example criticality of the vulnerability
- Whether attacks are ongoing (attacks-in-the-wild)
- Criticality of the systems potentially affected (e.g. mission-critical SCADA systems)
- Feasibility or availability of solutions or protection measures, which mitigate the threat
- Adequacy of industry standard and industry good practices in mitigating the threat

6 Impact of the incident

The second part of the taxonomy is used to classify the impact of the incident, i.e. the impact it has on services, in which sector(s) of the economy and society.

6.1 Sectors impacted

The impact on services, in the real world, indicating the sectors of the society and economy, where there is an impact on the services.

- **Energy** – The impact is in the Energy sector and its subsectors such as electricity, oil, or gas, for example, impacting electricity suppliers, power plants, distribution system operators, transmission system operators, oil transmission, natural gas distribution, etc.
- **Transport** – The impact is in the transport sector and subsectors such as air, rail, water, road, for example, impacting air traffic control systems, railway companies, maritime port authorities, road traffic management systems, etc.
- **Banking** – The impact is in the Banking sector, for example impacting banks, online banking, credit services, payment services, etc.
- **Financial** – The impact is in the Financial market infrastructure sector, for example, impacting traders, trading platforms, clearing services, etc.
- **Health** – The impact is in the Health sector, for example, impacting hospitals, medical devices, medicine supply, pharmacies, etc.
- **Drinking water –** The impact is in the Drinking water supply and distribution sector, for example impacting drinking water supply, drinking water distribution systems, etc.
- **Digital infrastructure** – The impact is in the Digital infrastructure sector, for example impacting internet exchange points, domain name systems, top level domain registries, etc.
- **Communications** – The impact is in the Electronic communications sector, for example, impacting mobile network services, fixed telephone lines, satellite communications, etc.
- **Digital services** – The impact is in the digital services sector, for example, impacting cloud services, online market places, online search engines, etc.
- **Trust and identification services** – The impact is in the electronic trust and identification services, for example, impacting certificate authorities, electronic identity systems, smartcards, etc.
- **Government** - The impact is in the government sector, for example, impacting the functioning of public administrations, elections, or emergency services

Note that for the sake of clarity cascading effects between sectors should not be considered here. For example, if a computer virus causes a large-scale outage of the mobile communication networks, then this will have also an impact across society. However this incident should be categorized as a computer virus with an impact in the sector ‘communications’. The fact that this incident in the communications sector also has cascading effects in other critical sectors would give it a high level (red e.g.) of impact across society and economy.

6.2 Severity of the impact

The severity of the impact, nationally, in the real world, for society and/or the economy, i.e. the level of disruption for the country or a large region of the country, the level of risks for health and/or safety, the level of physical damages and/or financial costs.

- **Red** – very large impact
- **Yellow** – large impact
- **Green** – minor impact
- **White** – no impact

Factors to take into considerations when assessing the severity of the impact.

- Risks for health and safety of the population, for example affecting emergency services
- Impact on economy and society, for example causing high losses
- Damages and costs for citizens and/or organizations affected
- Disruption of daily life
- Cascading effects in critical sectors
- Media impact and coverage
- Political impact and significance

Note that in case a large number of organizations are affected by incidents with a minor impact, then there may be a large impact in society, in which case it may be more appropriate to indicate a higher level of severity for the incident.

6.3 Outlook

The outlook for the incident, the prognosis, for the coming hours, considering the impact in the real world, the impact on services, for the society and/or the economy:

- **Improving** – Severity of impact is expected to *decrease* in the next 6 hours.
- **Stable**– Severity of impact is expected to *remain the same* in the 6 hours**.**
- **Worsening** - Severity of impact is expected to *increase* in the next 6 hours.

7 Labeling and technical taxonomies

In this section we cross-reference more technical taxonomies, which can be used as labels. This is particularly useful to further specify the nature of an incident.

7.1 Reference taxonomy for CSIRTs

The following terms are in the Reference taxonomy for CSIRTs, developed and supported by ENISA and TF-CSIRT, which is based on the widely used e-CSIRT taxonomy:

- **Abusive Content** - For example, spam, harmful speech, defacement, etc.
- **Malicious Code** – For example, a worm, trojan, spyware, dialler, rootkit, etc.
- **Information Gathering** - For example, scanning, sniffing, social engineering, etc.
- **Intrusion Attempts** – For example, exploiting known vulnerabilities, login attempts, etc.
- **Intrusions** – For example, account compromise, unprivileged account compromise, application compromise, etc.
- **Availability** – For example, DoS or DDoS attacks, sabotage, outage (no malice), etc.
- **Information Content Security** – For example, unauthorised access to information, unauthorised modification of information, etc.
- **Fraud** - For example, unauthorized use of resources, copyright, masquerade, phishing, etc.
- **Vulnerable -** For example, a vulnerability open for abuse, etc.

7.2 Detailed causes of telecom security incidents

The incident reporting in the telecom sector (under Article 13a of the EU's Framework directive for electronic communications) uses a shortlist based on frequently cited causes of incidents. Although the telecom sector has specific characteristics, some of these causes may be relevant also in other critical sectors.

- **Cable cut**
- **Cable theft**
- **Cooling outage**
- **Denial of Service attack**
- **Earth quake**
- **Electromagnetic interference**
- **Faulty hardware change/update**
- **Faulty software change/update**
- **Fire**
- **Flood**
- **Fuel exhaustion**
- **Hardware failure**
- **Hardware theft**
- **Heavy snow/ice**
- **Heavy wind**
- **Malware and viruses**
- **Network traffic hijack**

- **Overload**
- **Policy/procedure flaw**
- **Power cut**
- **Power surges**
- **Security shutdown**
- **Software bug**
- **Terrorist attack**
- **Wildfire**

8 Machine tags and namespaces

This section outlines a technical namespace for this taxonomy. It is important to develop and include a technical namespace for several reasons:

- It makes this taxonomy machine-readable. This is important for integration in tools.
- It avoids clashes with terms and definitions from other existing taxonomies, which makes it easier to use this taxonomy and other existing taxonomies.
- It facilitates versioning and updates more easy, because tools can fetch the updated namespaces automatically, for instance from GitHub.

8.1 Machine tags

Machine tags are used to attached a 'tag' (a term or a keyword) to a piece of information. A machine-tag is a simple triple-tag format of the form:

```
namespace:key = "value".
```

In other words, a machine tag has three parts For example, a machine defining economical impact definition, using an economical impact taxonomy at GitHub is[2]:

```
economical-impact:loss = less-than-100k-euro
```

This machine-tag could be used to 'tag' an incident or situation report with information about economic impact, using a specific taxonomy. This machine tag can be read as "using the economical impact taxonomy, this incident was tagged with causing a loss of less than 100k EUR".

Machine-readable tags are important when sharing incident data, especially across organizational and national borders. Machine tags allow a taxonomy to be expressed as a JSON file, making it easy to integrate the taxonomy in many types of applications. A large repository of JSON files expressing taxonomies, aimed at MISPs, is at https://github.com/MISP/misp-taxonomies

Parsers or automated systems can then automatically rely on the listed combinations of values of machine tags in order to map and match security events labeled via such machine tags.

8.2 Namespace

Machine tags require the definition of a unique namespace. Below we provide a first outline for such a namespace definition:

```
{
  "namespace": "eu-cyber-security-incident-taxonomy",
  "description": "Taxonomy for cybersecurity incidents – Recommendation under the EU Cybersecurity
Act",
  "version": 1,
  "predicates": [
    {
      "value": "root-cause-category",
      "expanded": "Root cause of the incident"
    },
    {
      "value": "severity-category",
      "expanded": "Severity (subjective estimate) of the incident"
```

[2] https://github.com/MISP/misp-taxonomies/blob/master/economical-impact/machinetag.json

```
    },
    {
      "value": "sector-category",
      "expanded": "Sector affected by the incident"
    }
  ],
  "values": [
    {
      "predicate": "sector-category",
      "entry": [
        {
          "value": "energy",
          "expanded": "Energy Sector"
        },
        {
          "value": "transport",
          "expanded": "Transportation Sector"
        },
        {
          "value": "finance",
          "expanded": "Financial Sector"
        },
        {
          "value": "health",
          "expanded": "Health Sector"
        },
        {
          "value": "drinking water",
          "expanded": "Drinking water supply and distribution Sector"
        },
        {
          "value": "government",
          "expanded": "Government Sector"
        },
        {
          "value": "communications",
          "expanded": "Electronic Communications Sector"
        },
        {
          "value": "digital-infrastructure",
          "expanded": "Digital infrastructure (for example IXPs)"
        },
        {
          "value": "digital services",
          "expanded": "General digital services Sector (for example cloud providers)"
        },
        {
          "value": "electronic-trust-and-identity",
          "expanded": "Electronic trust and identity providers (for example CAs)"
        },
        {
          "value": "other",
          "expanded": "Any other sector"
        }
      ]
    }
  ]
}
```


Please note that the example above merely helps to illustrate the idea and is not a final and complete machine tag specification for this taxonomy. The actual namespace needs to be developed further and then uploaded and maintained as part of the online repository of taxonomies for MIPSs at https://github.com/MISP/misp-taxonomies.

References and related work

- Good practice guide of using taxonomies in incident prevention and detection, ENISA, December 2017, https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
- ENISA Reference Incident Classification Taxonomy https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/
- EU CSIRTs network SOPs – Situation report Technical, Situation report Operational
  US CERT Cyber incident scoring system - https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System
  US Cyber Incident Severity Schema - https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf
- Open Threat Taxonomy - https://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf
- MISP taxonomies: https://www.misp-project.org/taxonomies.html#_introduction
- NIS CG Work Stream 3 on Notification Requirements for OESs
- NIS CG Work Stream 4 on Cross-Border dependencies
- NIS CG Work Stream 5 on Notification Requirements for DSPs
- Member States Good practices, guidelines, reporting templates and formats
- International norms and standards: OASIS (TAXII, Cybox, STIX), CC CERT (CMU)