ENISA Threat Taxonomy

A tool for structuring threat information

INITIAL VERSION

1.0

JANUARY 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Author

Louis Marinos, ENISA.

Contact

For contacting the authors please use louis.marinos@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank Jakub Radziulis, iTTi, for his support in the consolidation of the threat taxonomy on the basis of available ENISA material. We would also like to thank the members of the ENISA ETL Stakeholder Group for reviewing this material: Paolo Passeri, Consulting, UK, Pierluigi Paganini, Chief Security Information Officer, IT, Paul Samwel, Banking, NL, Tom Koehler, Consulting, DE, Stavros Lingris, CERT, EU, Jart Armin, Worldwide coalitions/Initiatives, International, Thomas Häberlen, Member State, DE, Neil Thacker, Consulting, UK, Margrete Raaum, CERT, NO, Shin Adachi, Security Analyst, US, R. Jane Ginn, Consulting, US, Lance James, Consulting, US, Polo Bais, Member State, NL.

Table of Contents

1. Introduction/Method/Sources

The present threat taxonomy is an initial version that has been developed on the basis of available ENISA material. This material has been used as an ENISA-internal structuring aid for information collection and threat consolidation purposes. It emerged in the time period 2012-2015. The consolidated threat taxonomy is an initial version: in 2016, ENISA plans to update and expand it with additional details, such as definitions of the various threats mentioned.

For the presented threat taxonomy, Cyber Threats should be understood as *threats applying to assets related to information and communication technology*. Such threats are materialized mostly in cyberspace, while some threats included are materialized in the physical world but affect information and cyber-assets.

Besides the ENISA material, the following available threat taxonomies where analysed and – when relevant – have been integrated in the current version of the ENISA taxonomy:

- All previous ENISA documents in the area of threat landscape.
- forward-whitebook[1]
- Threat_Taxonomy_Luiijf_Nieuwenhuijs_v5[2]
- New Data Harmonization - abusehelper Collab[3]
- sp800_150_draft[4]
- Threat Classification Taxonomy Cross Reference View[5]
- Taxonomy of DDoS Attack and DDoS Defense Mechanisms[6]
- Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies[7]
- Two taxonomies of deception for attacks on information systems[8]
- Basic Concepts and Taxonomy of Dependable and Secure Computing[9]
- 1997_019_001_52455 taxonomy[10]
- sp800_30_r1 threat events[11]
- Threats catalogue IT Grundsutz[12]

[1] http://www.ict-forward.eu/whitebook/, accessed December 2015.
[2] http://www.researchgate.net/profile/Eric_Luiijf/publication/220592994_Extensible_threat_taxonomy_for_critical_infrastructures/links/0a85e53603c15d292b000000.pdf, accessed December 2015.
[3] https://github.com/certtools/intelmq/wiki/Data-Harmonization, accessed December 2015.
[4] http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf, accessed December 2015.
[5] http://projects.webappsec.org/w/page/13246977/Threat%20Classification%20Views, accessed December 2015.
[6] http://www.eecis.udel.edu/~sunshine/publications/ccr.pdf, accessed December 2015.
[7] https://s2erc.georgetown.edu/sites/s2erc/files/CyberISE%20Taxonomy.pdf, accessed December 2015.
[8] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.5398&rep=rep1&type=pdf, accessed December 2015.
[9] http://www.nasa.gov/pdf/636745main_day_3-algirdas_avizienis.pdf, accessed December 2015.
[10] http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=52454, accessed December 2015.
[11] http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf, accessed December 2015.
[12] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.html;jsessionid=A72092E049CA62A0A1B8521261DA8381.2_cid368, accessed December 2015.

- INSPIRE-D2.2 str. 23[13]
- OCTAVE Threat Profiles-OCTAVE threat Profiles[14]
- OWASP Application-threat-modeling-24-728[15]
- eCSIRT.net[16,17]
- Howard/Longstaff[18]
- Longstaff NCSC 2010[19]
- CIF API Feed Types v1[20]
- CIF Taxonomy Assesment v1[21]
- FICORA[22]
- Andrew Cormack[23]
- SURFcert[24]
- HP Tipping Point Event Taxonomy V 2.2[25]
- CESNET CERTS[26]
- Warden 2[27]
- Mentat[28]
- 7-steps-to-threat-modeling-6-638[29]
- 711_owasp_cats_colored[30]
- A Taxonomy of Operational Cyber Security Risks[31]

Following projects where analysed:

- FORWARD project[32]

[13] http://cordis.europa.eu/project/rcn/87757_en.html, accessed December 2015.
[14] http://www85.homepage.villanova.edu/timothy.ay/MIS2040/OCTAVEthreatProfiles%5B1%5D.pdf, accessed December 2015.
[15] https://www.owasp.org/index.php/Application_Threat_Modeling, accessed December 2015.
[16] http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6, accessed December 2015.
[17] http://www.terena.org/activities/tf-csirt/meeting39/20130523-DV1.pdf, accessed December 2015.
[18] http://infoserve.sandia.gov/sand_doc/1998/988667.pdf, accessed December 2015.
[19] https://www.ncsc.nl/conference/conference-2011/speakers/tom-longstaff.html, accessed December 2015.
[20] https://code.google.com/p/collective-intelligence-framework/wiki/API_FeedTypes_v1, accessed December 2015.
[21] https://code.google.com/p/collective-intelligence-framework/wiki/TaxonomyAssessment_v1, accessed
[22] http://personal.inet.fi/koti/erka/Studies/DI/DI_Erka_Koivunen.pdf, accessed December 2015.
[23] http://www.terena.org/activities/tf-csirt/pre-meeting3/TLversion0_2.html, accessed December 2015.
[24] http://www.terena.org/activities/tf-csirt/meeting39/20130523-DV1.pdf, accessed December 2015.
[25] http://h10032.www1.hp.com/ctg/Manual/c03964615, accessed December 2015.
[26] http://archiv.cesnet.cz/doc/techzpravy/2010/otrs-csirt-workflow/, accessed December 2015.
[27] ftp://homeproj.cesnet.cz/tar/warden/warden-client-2.1.tar.gz, accessed December 2015.
[28] https://csirt.cesnet.cz/en/services/mentat, accessed December 2015.
[29] http://www.slideshare.net/chinwhei/7-steps-to-threat-modeling, accessed December 2015.
[30] https://cwe.mitre.org/data/pdf/711_owasp_cats_colored.pdf, accessed December 2015.
[31] http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9395, accessed December 2015.
[32] http://www.ict-forward.eu/, accessed December 2015.

- VITA project[33]
- NI2S3 project[34]
- IMCOSEC project[35]
- INTERSECTION project[36]
- INSPIRE project[37]
- THREVI2[38]
- ESCORTS[39]

Developed threats taxonomy consist of following fields:

- *High level threats*: this is the top level threat category, used mainly to discriminate families of threats.
- *Threats*: this field indicates the various threats within a category.
- *Threats details*: in this field details of a specific threat are being described. Threat details are based on a specific attack type/method or targeting specific IT asset.

Additional fields can be added depending on the use case of this table (see also next section). In the information collection, for example, we use some additional fields indicating affected assets, threat agents, related sources/URLs, etc.

It should be noted that the ENISA threat taxonomy is a living document: during its use within ENISA, additional threats, references, definitions, etc. can be added. ENISA will publish the threat taxonomy every time new content has been created and consolidated. Interested individuals may visit the corresponding location and check availability of the ENISA threat taxonomy[40].

[33] http://www.researchgate.net/publication/220592994_Extensible_threat_taxonomy_for_critical_infrastructures, accessed December 2015.
[34] http://cordis.europa.eu/result/rcn/58659_en.html, accessed December 2015.
[35] http://cordis.europa.eu/result/rcn/55741_en.html, accessed December 2015.
[36] http://cordis.europa.eu/project/rcn/85347_en.html, accessed December 2015.
[37] http://cordis.europa.eu/project/rcn/87757_en.html, accessed December 2015.
[38] http://www.threvi2.eu/, accessed December 2015.
[39] http://cordis.europa.eu/result/rcn/55021_en.html, accessed December 2015.
[40] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape#b_start=0, accessed December 2015.

2. Purpose of threat taxonomy

Threat taxonomy is a classification of threat types and threats at various levels of detail. The purpose of such a taxonomy is to establish a point of reference for threats encountered, while providing a possibility to shuffle, arrange, amend and detail threat definitions. To this extend, a threat taxonomy is a living structure that is being used to maintain a consistent view on threats on the basis of collected information.

The current version of ENISA threat taxonomy has been developed over the past years as an internal tool used in the collection and consolidation of threat information. When collecting information on various threats, it is very convenient to store similar things together. To this extend, a threat taxonomy has been generated. It is worth mentioning that the initial structure has been updated/consolidated with various sources of threat information. Most of threat information included was from existing threat catalogues the area of information security and in particular risk management. Besides the references mentioned in the introduction section, an overview of further threat catalogues can be found here[41]. Hence, besides cyber-threats the ENISA threat taxonomy contains also physical threats that can cause harm to information technology assets. Yet, due to the focus of ENISA work in the area of cyber-space, the threat taxonomy presented has a better maturity in the field of cyber-threats.

As until now the threat taxonomy has been used for collection and consolidation of cyber-threat information, only the cyber-threat part of the taxonomy has been maintained and developed further. Although all information security threat areas are part of the threat taxonomy, those that are not related to cyber have not evolved over the time.

In 2015, ENISA has created a consolidated version of these threats, has added some short descriptions to these threats and has decided to make this material publicly available as a table by means of this document. The figure below shows this taxonomy in form of a mind map, together with some symbols indicating its possible use-cases (see Figure 1).

[41] http://opensecurityarchitecture.org/cms/images/OSA_images/TC_Comparison.pdf, accessed November 2015.

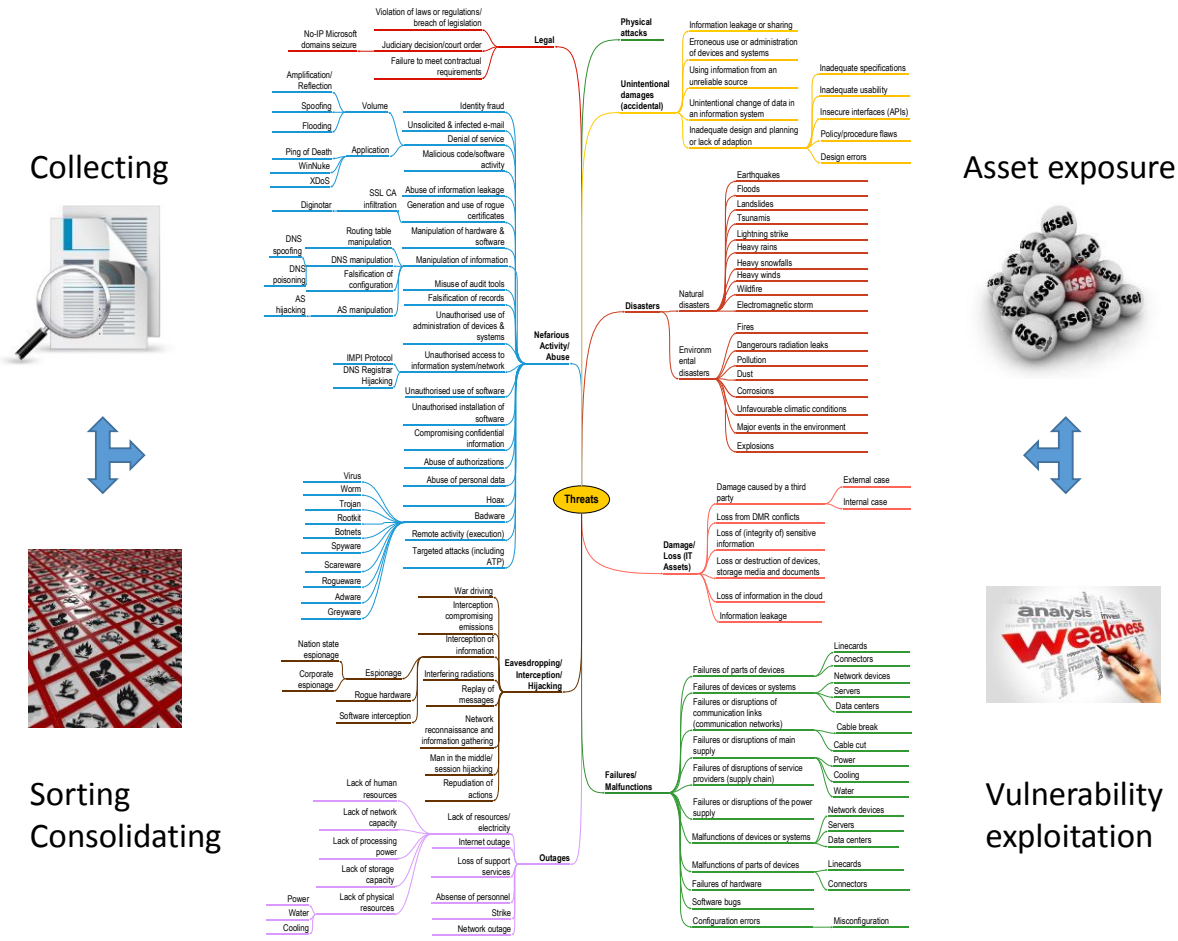

Figure 1: ENISA Threat Taxonomy and its use-cases

In short, the indicated use-cases for the threat taxonomy are:

- *Collection*: When information is being collected, findings can be grouped around a certain cyber-threat, although this is often not clearly mentioned in the source text. In the collection phase is as a place to associate various findings under a common threat, putting thus information in context.
- *Sorting/Consolidation*: When sufficient information has been collected about a cyber-threat, a consolidated view about the state-of-play may be generated. This information might include trends, statistics and references. It is then subject to further grouping and prioritization (i.e. in form of one of the top 15 cyber-threats, possibly containing a number of detailed threats).
- *Asset exposure*: The threats of the taxonomy may be assigned to assets. This is being done in order to express the exposure of an asset to threats. Usually, threats explore weaknesses/vulnerabilities of assets to materialise. Hence, vulnerabilities/weaknesses may also be assigned to threats exploring them, either directly or indirectly through the assets.

The current version of ENISA threat taxonomy is an initial document whose development will be continued in 2016. In addition to this document, the ENISA threat taxonomy is going to be published in form of an excel table. Please note that the excel table is contains fields used in the ENISA collection work and contains additional fields and some examples for the content of these fields.

In its current version, the ENISA threat taxonomy has been reviewed by the ENISA Threat Landscape Stakeholder Group.

2.1 State-of-play and next steps

As indicated in this document, the current version is considered to be “initial”. In 2016, ENISA is going to invest some effort in amending the threat taxonomy with some definitions of the threats and eventually additional information. In addition, examples are going to be given as they can found in various reports.

In addition to the tabular form presented in this document, additional formats of the threat taxonomy are going to be produced and adapted to the various use cases (e.g. excel sheet, mind maps, etc.). Finally, feedback that will be received from experts/users of the current version of the taxonomy are going to be included in the upcoming versions.

3. ENISA Threat Taxonomy

Line number	High Level Threats	Threats	Threat details	Comments
1	**Physical attack (deliberate/ intentional)**			Threats of intentional, hostile human actions.
2		***Fraud***		Fraud committed by humans.
3			Fraud committed by employees	Fraud committed by employees or others that are in relation with entities, who have access to entities' information and IT assets.
4		***Sabotage***		Intentional actions (non-fulfilment or defective fulfilment of personal duties) aimed to cause disruption or damage to IT assets.
5		***Vandalism***		Act of physically damaging IT assets.
6		***Theft (of devices, storage media and documents)***		Stealing information or IT assets. Robbery.
7			Theft of mobile devices (smartphones/ tablets)	Taking away another person's property in the form of mobile devices, for example smartphones, tablets.
8			Theft of fixed hardware	Taking away another person's hardware property (except mobile devices), which often contains business-sensitive data.
9			Theft of documents	Stealing documents from private/company archives, often for the purpose of re-sale or to achieve personal benefits.
10			Theft of backups	Stealing media devices, on which copies of essential information are kept.
11		***Information leak /sharing***		Sharing information with unauthorised entities. Loss of information confidentiality due to intentional human actions (e.g., information leak may occur due to loss of paper copies of confidential information).

12		***Unauthorized physical access / Unauthorised entry to premises***		Unapproved access to facility.
13		***Coercion, extortion or corruption***		Actions following acts of coercion, extortion or corruption.
14		***Damage from the warfare***		Threats of direct impact of warfare activities.
15		***Terrorist attack***		Threats from terrorists.
16	**Unintentional damage / loss of information or IT assets**			Threats of unintentional human actions or errors.
17		***Information leak /sharing due to human error***		Information leak / sharing caused by humans, due to their mistakes.
18			Accidental leaks/sharing of data by employees	Unintentional distribution of private or sensitive data to an unauthorized entity by a staff member.
19			Leaks of data via mobile applications	Threat of leaking private data (a result of using applications for mobile devices).
20			Leaks of data via Web applications	Threat of leaking important information using web applications.
21			Leaks of information transferred by network	Threat of eavesdropping of unsecured network traffic.
22		***Erroneous use or administration of devices and systems***		Information leak / sharing / damage caused by misuse of IT assets (lack of awareness of application features) or wrong / improper IT assets configuration or management.
23			Loss of information due to maintenance errors / operators' errors	Threat of loss of information by incorrectly performed maintenance of devices or systems or other operator activities.
24			Loss of information due to configuration/ installation error	Threat of loss of information due to errors in installation or system configuration.
25			Increasing recovery time	Threat of unavailability of information due to errors in the use of backup media and increasing information recovery time.

26			Loss of information due to user errors	Threat of unavailability of information or damage to IT assets caused by user errors (using IT infrastructure) or IT software recovery time.
27		***Using information from an unreliable source***		Bad decisions based on unreliable sources of information or unchecked information.
28		***Unintentional change of data in an information system***		Loss of information integrity due to human error (information system user mistake).
29		***Inadequate design and planning or improper adaptation***		Threats caused by improper IT assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors).
30		***Damage caused by a third party***		Threats of damage to IT assets caused by third party.
31			Security failure caused by third party	Threats of damage to IT assets caused by breach of security regulations by third party.
32		***Damages resulting from penetration testing***		Threats to information systems caused by conducting IT penetration tests inappropriately.
33		***Loss of information in the cloud***		Threats of losing information or data stored in the cloud.
34		***Loss of (integrity of) sensitive information***		Threats of losing information or data, or changing information classified as sensitive.
35			Loss of integrity of certificates	Threat of losing integrity of certificates used for authorisation services.
36		***Loss of devices, storage media and documents***		Threats of unavailability (losing) of IT assets and documents.
37			Loss of devices/ mobile devices	Threat of losing mobile devices.
38			Loss of storage media	Threat of losing data-storage media.
39			Loss of documentation of IT Infrastructure	Threat of losing important documentation.

40		***Destruction of records***		Threats of unavailability (destruction) of data and records (information) stored in devices and storage media.
41			Infection of removable media	Threat of loss of important data due to using removable media, web or mail infection.
42			Abuse of storage	Threat of loss of records by improper /unauthorised use of storage devices.
43	**Disaster (natural, environmental)**			Threats of damage to information assets caused by natural or environmental factors.
44		***Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)***		Large scale natural disasters.
45		***Fire***		Threat of fire.
46		***Pollution, dust, corrosion***		Threat of disruption of work of IT systems (hardware) due to pollution, dust or corrosion (arising from the air).
47		***Thunderstrike***		Threat of damage to IT hardware caused by thunder strike (overvoltage).
48		***Water***		Threat of damage to IT hardware caused by water.
49		***Explosion***		Threat of damage to IT hardware caused by explosion.
50		***Dangerous radiation leak***		Threat of damage to IT hardware caused by radiation leak.
51		***Unfavourable climatic conditions***		Threat of disruption of work of IT systems due to climatic conditions that have a negative effect on hardware.
52			Loss of data or accessibility of IT infrastructure as a result of heightened humidity	Threat of disruption of work of IT systems due to high humidity.
53			Lost of data or accessibility of IT infrastructure as a result of very high temperature	Threat of disruption of work of IT systems due to high or low temperature.

54		***Threats from space / Electromagnetic storm***		Threats of the negative impact of solar radiation to satellites and radio wave communication systems - electromagnetic storm.
55		***Wildlife***		Threat of destruction of IT assets caused by animals: mice, rats, birds.
56	**Failures/ Malfunction**			Threat of failure/malfunction of IT supporting infrastructure (i.e. degradation of quality, improper working parameters, jamming). The cause of a failure is mostly an internal issue (e.g.. overload of the power grid in a building).
57		***Failure of devices or systems***		Threat of failure of IT hardware and/or software assets or its parts.
58			Failure of data media	Threat of failure of data media.
59			Hardware failure	Threat of failure of IT hardware.
60			Failure of applications and services	Threat of failure of software/applications or services.
61			Failure of parts of devices (connectors, plug-ins)	Threat of failure of IT equipment or its part.
62		***Failure or disruption of communication links (communication networks)***		Threat of failure or malfunction of communications links.
63			Failure of cable networks	Threat of failure of communications links due to problems with cable network.
64			Failure of wireless networks	Threat of failure of communications links due to problems with wireless networks.
65			Failure of mobile networks	Threat of failure of communications links due to problems with mobile networks.
66		***Failure or disruption of main supply***		Threat of failure or disruption of supply required for information systems.
67			Failure or disruption of power supply	Threat of failure or malfunction of power supply.

68			Failure of cooling infrastructure	Threat of failure of IT assets due to improper work of cooling infrastructure.
69		***Failure or disruption of service providers (supply chain)***		Threat of failure or disruption of third party services required for proper operation of information systems.
70		***Malfunction of equipment (devices or systems)***		Threat of malfunction of IT hardware and/or software assets or its parts (i.e. improper working parameters, jamming, rebooting).
71	**Outages**			Threat of complete lack or loss of resources necessary for IT infrastructure. The cause of an outage is mostly an external issue (i.e electricity blackout in the whole city).
72		***Absence of personnel***		Unavailability of key personnel and their competences.
73		***Strike***		Unavailability of staff due to a strike (large scale absence of personnel).
74		***Loss of support services***		Unavailability of support services required for proper operation of the information system.
75		***Internet outage***		Unavailability of the Internet connection.
76		***Network outage***		Unavailability of communication links.
77			Outage of cable networks	Threat of lack of communications links due to problems with cable network.
78			Outage of short-range wireless networks	Threat of lack of communications links due to problems with wireless networks (802.11 networks, Bluetooth, NFC etc.).
79			Outages of long-range wireless networks	Threat of lack of communications links due to problems with mobile networks like cellular network (3G, LTE, GSM etc.) or satellite links.
80	**Eavesdropping/ Interception/ Hijacking**			Threats that alter communication between two parties. These attacks do not have to install additional tools/software on a victim's site.

81		***War driving***		Threat of locating and possibly exploiting connection to the wireless network.
82		***Intercepting compromising emissions***		Threat of disclosure of transmitted information using interception and analysis of compromising emission.
83		***Interception of information***		Threat of interception of information which is improperly secured in transmission or by improper actions of staff.
84			Corporate espionage	Threat of obtaining information secrets by dishonest means.
85			Nation state espionage	Threats of stealing information by nation state espionage (e.g. China based governmental espionage, NSA from USA).
86			Information leakage due to unsecured Wi-Fi, rogue access points	Threat of obtaining important information by insecure network rogue access points etc.
87		***Interfering radiation***		Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source.
88		***Replay of messages***		Threat in which valid data transmission is maliciously or fraudulently repeated or delayed.
89		***Network Reconnaissance, Network traffic manipulation and Information gathering***		Threat of identifying information about a network to find security weaknesses.
90		***Man in the middle/ Session hijacking***		Threats that relay or alter communication between two parties.
91	**Nefarious Activity/ Abuse**			Threats of nefarious activities that require use of tools by the attacker. These attacks require installation of additional tools/software or performing additional steps on the victim's IT infrastructure/software.
92		***Identity theft (Identity Fraud/ Account)***		Threat of identity theft action.
93			Credentials-stealing trojans	Threat of identity theft action by malware computer programs.
94		***Receiving unsolicited E-mail***		Threat of receiving unsolicited email which affects information security and efficiency.

95			SPAM	Threat of receiving unsolicited, undesired, or illegal email messages.
96			Unsolicited infected e-mails	Threat emanating from unwanted emails that may contain infected attachments or links to malicious / infected web sites.
97		***Denial of service***		Threat of service unavailability due to massive requests for services.
98			Distributed denial of network service (DDoS) (network layer attack i.e. Protocol exploitation / Malformed packets / Flooding / Spoofing)	Threat of service unavailability due to a massive number of requests for access to network services from malicious clients.
99			Distributed denial of application service (DDoS) (application layer attack i.e. Ping of Death / XDoS / WinNuke / HTTP Floods)	Threat of service unavailability due to massive requests sent by multiple malicious clients.
100			Distributed DoS (DDoS) to both network and application services (amplification/reflection methods i.e. NTP/ DNS /…/ BitTorrent)	Threat of creating a massive number of requests, using multiplication/amplification methods.
101		***Malicious code/ software/ activity***		Threat of malicious code or software execution.
102			Search Engine Poisoning	Threat of deliberate manipulation of search engine indexes.
103			Exploitation of fake trust of social media	Threat of malicious activities making use of trusted social media.
104			Worms/ Trojans	Threat of malware computer programs (trojans/worms).
105			Rootkits	Threat of stealthy types of malware software.
106			Mobile malware	Threat of mobile malware programs.
107			Infected trusted mobile apps	Threat of using mobile malware software that is recognised as trusted one.

108			Elevation of privileges	Threat of exploiting bugs, design flaws or configuration oversights in an operating system or software application to gain elevated access to resources.
109			Web application attacks / injection attacks (Code injection: SQL, XSS)	Threat of utilizing custom web applications embedded within social media sites, which can lead to installation of malicious code onto computers to be used to gain unauthorized access.
110			Spyware or deceptive adware	Threat of using software that aims to gather information about a person or organization without their knowledge.
111			Viruses	Threat of infection by viruses.
112			Rogue security software/ Rogueware / Scareware	Threat of internet fraud or malicious software that mislead users into believing there is a virus on their computer, and manipulates them to pay money for fake removal tool.
113			Ransomware	Threat of infection of computer system or device by malware that restricts access to it and demands that the user pay a ransom to remove the restriction.
114			Exploits/Exploit Kits	Threat to IT assets due to the use of web available exploits or exploits software.
115		***Social Engineering***		Threat of social engineering type attacks (target: manipulation of personnel behaviour).
116			Phishing attacks	Threat of an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy websites.
117			Spear phishing attacks	Spear-phishing is a targeted e-mail message that has been crafted to create fake trust and thus lure the victim to unveil some business or personal secrets that can be abused by the adversary.
118		***Abuse of Information Leakage***		Threat of leaking important information.
119			Leakage affecting mobile privacy and mobile applications	Threat of leaking important information due to using malware mobile applications.

120			Leakage affecting web privacy and web applications	Threat of leakage important information due to using malware web applications.
121			Leakage affecting network traffic	Threat of leaking important information in network traffic.
122			Leakage affecting cloud computing	Threat of leaking important information in cloud computing.
123		***Generation and use of rogue certificates***		Threat of use of rogue certificates.
124			Loss of (integrity of) sensitive information	Threat of loss of sensitive information due to loss of integrity.
125			Man in the middle/ Session hijacking	Threat of attack consisting in the exploitation of the web session control mechanism, which is normally managed by a session token.
126			Social Engineering / signed malware	Threat of install fake trust signed software (malware) e.g. fake OS updates.
127			Fake SSL certificates	Threat of attack due to malware application signed by a certificate that is typically inherently trusted by an endpoint.
128		***Manipulation of hardware and software***		Threat of unauthorised manipulation of hardware and software.
129			Anonymous proxies	Threat of unauthorised manipulation by anonymous proxies.
130			Abuse of computing power of cloud to launch attacks (cybercrime as a service)	Threat of using large computing powers to generate attacks on demand.
131			Abuse of vulnerabilities, 0-day vulnerabilities	Threat of attacks using 0-day or known IT assets vulnerabilities.
132			Access of web sites through chains of HTTP Proxies (Obfuscation)	Threat of bypassing the security mechanism using HTTP proxies (bypassing the website blacklist).
133			Access to device software	Threat of unauthorised manipulation by access to device software.
134			Alternation of software	Threat of unauthorized modifications to code or data, attacking its integrity.

135			Rogue hardware	Threat of manipulation due to unauthorized access to hardware.
136		***Manipulation of information***		Threat of intentional data manipulation to mislead information systems or somebody or to cover other nefarious activities (loss of integrity of information).
137			Repudiation of actions	Threat of intentional data manipulation to repudiate action.
138			Address space hijacking (IP prefixes)	Threat of the illegitimate takeover of groups of IP addresses.
139			Routing table manipulation	Threat of route packets of network to IP addresses other than that was intended via sender by unauthorised manipulation of routing table.
140			DNS poisoning / DNS spoofing / DNS Manipulations	Threat of falsification of DNS information.
141			Falsification of record	Threat of intentional data manipulation to falsify records.
142			Autonomous System hijacking	Threat of overtaking by the attacker the ownership of a whole autonomous system and its prefixes despite origin validation.
143			Autonomous System manipulation	Threat of manipulation by the attacker of a whole autonomous system in order to perform malicious actions.
144			Falsification of configurations	Threat of intentional manipulation due to falsification of configurations.
145		***Misuse of audit tools***		Threat of nefarious actions performed using audit tools (discovery of security weaknesses in information systems).
146		***Misuse of information/ information systems (including mobile apps)***		Threat of nefarious action due to misuse of information / information systems.
147		***Unauthorized activities***		Threat of nefarious action due to unauthorised activities.
148			Unauthorised use or administration of devices and systems	Threat of nefarious action due to unauthorised use of devices and systems.

149			Unauthorised use of software	Threat of nefarious action due to unauthorised use of software.
150			Unauthorized access to the information systems / networks (IMPI Protocol / DNS Registrar Hijacking)	Threat of unauthorised access to the information systems / network.
151			Network Intrusion	Threat of unauthorised access to network.
152			Unauthorized changes of records	Threat of unauthorised changes of information.
153		***Unauthorized installation of software***		Threat of unauthorised installation of software.
154			Web based attacks (Drive-by download / malicious URLs / Browser based attacks)	Threat of installation of unwanted malware software by misusing websites.
155		***Compromising confidential information (data breaches)***		Threat of data breach.
156		***Hoax***		Threat of loss of IT assets security due to cheating.
157			False rumour and/or fake warning	Threat of disruption of work due to rumours and/or a fake warning.
158		***Remote activity (execution)***		Threat of nefarious action by attacker remote activity.
159			Remote Command Execution	Threat of nefarious action due to remote command execution.
160			Remote Access Tool (RAT)	Threat of infection of software that has a remote administration capabilities allowing an attacker to control the victim's computer.
161			Botnets / Remote activity	Threat of penetration by software from malware distribution.
162		***Targeted attacks (APTs etc.)***		Threat of sophisticated, targeted attack which combine many attack techniques.
163			Mobile malware	Threat of mobile software that aims to gather information about a person or organization without their knowledge.

164			Spear phishing attacks	Threat of attack focused on a single user or department within an organization, coming from someone within the company in a position of trust and requesting information such as login, IDs and passwords.
165			Installation of sophisticated and targeted malware	Threat of malware delivered by sophisticated and targeted software.
166			Watering Hole attacks	Threat of malware residing on the websites which a group often uses.
167		***Failed business process***		Threat of damage or loss of IT assets due to improperly executed business process.
168		***Brute force***		Threat of unauthorised access via systematically checking all possible keys or passwords until the correct one is found.
169		***Abuse of authorizations***		Threat of using authorised access to perform illegitimate actions.
170	**Legal**			Threat of financial or legal penalty or loss of trust of customers and collaborators due to legislation.
171		***Violation of rules and regulations / Breach of legislation***		Threat of financial or legal penalty or loss of trust of customers and collaborators due to violation of law or regulations.
172		***Failure to meet contractual requirements***		Threat of financial penalty or loss of trust of customers and collaborators due to failure to meet contractual requirements.
173			Failure to meet contractual requirements by third party	Threat of financial penalty or loss of trust of customers and collaborators due to a third party's failure to meet contractual requirements
174		***Unauthorized use of IPR protected resources***		Threat of financial or legal penalty or loss of trust of customers and collaborators due to improper/illegal use of IPR protected material (IPR- Intellectual Property Rights.
175			Illegal usage of File Sharing services	Threat of financial or legal penalty or loss of trust of customers and collaborators due to improper/illegal use of file sharing services.
176		***Abuse of personal data***		Threat of illegal use of personal data.

177		***Judiciary decisions/court order***		Threat of financial or legal penalty or loss of trust of customers and collaborators due to judiciary decisions/court order.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu