CYBECO

Supporting Cyber-insurance from a Behavioural Choice Perspective

D5.2: CYBECO content and data collection manual

Due date: M14

Abstract:
This report describes the content collection, modelling and integration activities required to provide the CYBECO toolkit with relevant, attractive and validated cybersecurity related content. The goal is the creation of a structured qualitative and quantitative Knowledge Base which will encourage and sustain cybersecurity modelling research and development.

Dissemination Level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Status

Document Title	CYBECO content and data collection manual
Version	0.5
Work Package	5
Deliverable #	5.2
Prepared by	INTRASOFT
Contributors	Vassilis Chatzigiannakis, George Koutalieris, Aitor Couce Vieira, David Rios Insua
Checked by	
Approved by	
Date	
Confidentiality	PP

Document Change Log

Each change or set of changes made to this document will result in an increment to the version number of the document. This change log records the process and identifies for each version number of the document the modification(s) which caused the version number to be incremented.

Change Log	Version	Date
First draft (INTRASOFT)	0.1	May 15, 2018
Incorporated catalogue and KB structure suggestions from WP3	0.2	June 1, 2018
Included WP4 Use case analysis	0.3	June 10, 2018
Included KB implementation details	0.4	June 14, 2018
Comments from internal reviewers	0.5	June 26, 2018

Table of Contents

List of Tables

1 Introduction

Based on the outcomes of the other CYBECO work packages, the main objective and outcome of WP5 is the development of the information toolbox (CYBECO Toolbox 2.0 that will be available at M24).

The key idea here is to enable cyber insurance clients and insurance companies, research actors, policy makers and market stakeholders, not only to obtain easy access to information on relevant concepts of cyber insurance and the evaluation of the proposed models and experiments, but also to provide them with a framework of analysis and assessment of the preferred cybersecurity and cyber insurance choices regarding their specific needs and enquiries. To that end, the Toolbox will provide a set of Risk Analysis Templates, designed by WP3 and based on the use cases, scenarios, input and experience from WP4. These "CYBECO Risk Analysis Templates" will model aspects researched by WP6 and WP7.

This report describes the data and content collection procedures and specifies the annotation of content based on common expert-generated vocabularies. The goal is to manage the overall data and content collection, modeling and integration activities required to provide the CYBECO toolkit with relevant, attractive and validated cybersecurity related content in the form of a Knowledge Base (KB).

Special focus will be put on user generated feedback and content, in order for the content to be appropriately validated prior to becoming publicly accessible.

2 CYBECO Toolbox Content Requirements

The goal of the CYBECO project is to research, develop, demonstrate, evaluate and exploit a new framework for managing cybersecurity risks, one that is focusing on cyber-insurance, as key risk management treatment. The Modelling framework for cyber risk management is developed in WP3, whereas WP4 defines the use-cases and cyber insurance scenarios that will be used to validate the framework and models defined in WP3.

The use cases provided by WP4 cover some of the most generic risk scenarios, types of companies, and actors involved in the cyber-insurance process. It is useful to note that the provided use cases are of interest to both viewpoints in the insurance process (i.e. the insurance provider and the insured company), and more importantly so for the insured company, since they allow for an organization to identify its activities with the risk examples provided in one of the use cases, even if such use cases are far from exhaustive.

On the other hand, there are extensive well-established catalogues and vocabularies describing cyber-insurance related content that will be presented in the next section. Therefore, the goal of the CYBECO Knowledge Base is not to provide yet another extensive glossary, but to support the risk analysis module by providing information about all cyber-insurance related terms used in the risk analysis framework. The idea is to provide a structured hierarchical taxonomy of cyber-insurance related terms that are used in the CYBECO toolbox.

2.1 Cyber-insurance Related Catalogues and Vocabularies

Catalogue	Type	Description
ISO 31000	Standard	Risk management – Guidelines, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector[1].
ISO 27001	Standard	The ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. It is the specification for an ISMS, an Information Security

		Management System. BS7799 itself was a long-standing standard, first published in the nineties as a code of practice[2].
ISO 27002	Standard	The ISO 27002 standard was originally published as a rename of the existing ISO 17799 standard, a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001[2].
ISO 27003	Standard	The purpose of this proposed development is to provide help and guidance in implementing an ISMS (Information Security Management System). This will include focus upon the PDCA method, with respect to establishing, implementing, reviewing and improving the ISMS itself[2].
ISO 27004	Standard	Published in December 2009, ISO 27004 provides guidance on the development and use of measures and measurement for the assessment of the effectiveness of an implemented information security management system and controls, as specified in ISO 27001. The appendix of the document also suggests metrics which were selected to align with ISO 27002[2].
ISO 27005	Standard	ISO 27005 is the name of the prime 27000 series standard covering information security risk management. The standard provides guidelines for information security risk management (ISRM) in an organization, specifically supporting the requirements of an information security management system defined by ISO 27001[2].
STIX V2.0 Part 1	Serialization format and Vocabulary	Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX enables organizations to share CTI with one another in a consistent and machine-readable manner, allowing security communities to better

		understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively[3].
STIX™ Version 2.0. Part 2	Serialization format and Vocabulary	This document (STIX Objects) uses the concepts introduced in STIX™ Version 2.0. Part 1: STIX Core Concepts to define STIX Domain Objects and STIX Relationship Objects[4].
ENISA Threat Taxonomy v2016	Taxonomy	A Taxonomy of threats provided by ENISA[5]
CAPEC	Taxonomy	CAPEC™ is a comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defences[6].
MAEC	Catalogue	Malware Attribute Enumeration and Characterization (MAEC™) is a standardized language for sharing structured information about malware based upon attributes such as behaviours, artifacts and attack patterns[7]
CWE	Catalogue	CWE™ is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts[8].
CVE	Catalogue	CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD)[9]

OVAL	Standard	Open Vulnerability and Assessment Language: an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community[10] .
NIST SP 800-53 Rev 4	Standard	Security Controls and Assessment Procedures for Federal Information Systems and Organizations[11]

Table 1 cyber-insurance related catalogues

2.2 Risk analysis case content requirements

In this section we will analyze the content needs of the Risk Analysis module. The following risk analysis cases are planned for the first version of the Toolbox (CYBECO Toolbox 1.0, available at M14):

- The first risk analysis case models a single SME facing cybersecurity risks. The goal is to support the SME decision-making towards the optimal cyber security portfolio and cyber insurance product.
- The second risk analysis case is from the perspective of the insurer; Specifically, the decision on whether to insure a particular SME or not.

2.2.1 Risk analysis case for an SME - cyber-related terms

This risk analysis case takes the perspective of the SME. It provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework.

Overview of the use:

- The first screen requires the selection of the relevant security controls and insurance products the user wants to consider in risk analysis.
- The second screen will provide an information dashboard with dynamically generated risk analysis information, based on the elements selected in the first screen.

Input in the first screen is divided in the following categories:

- Assets: facilities, computer equipment, market share.

- Threats: Fire, computer virus, DDoS attack.
- Security Controls: Anti-fire system, Firewall, Risk mitigation procedures.
- Insurance Products: Traditional insurance, Cyber insurance, Comprehensive insurance.

2.2.2 Risk analysis case for an SME (insurance company perspective)- cyber-related terms

This risk analysis case takes the perspective of the insurance company. It provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework.

Overview of the use:

- The first screen asks for the configuration of the insurance products.
- The second screen will provide an information dashboard with dynamically generated risk analysis information, based on the elements selected in the first screen.

Input in the first screen is divided in the following categories:

- Assets: facilities, computer equipment, market share.
- Threats: Fire, computer virus, DDoS attack.
- Security Controls: Anti-fire system, Firewall, Risk mitigation procedures, Cloud-based DDoS protection.
- Insurance Selection: Coverage range (e.g. 80%—100%), Traditional insurance package and range of cost (e.g. € 300 - € 500), Cyber insurance package and range of cost (e.g. € 300 - € 500), Comprehensive insurance package and range of cost (e.g. € 300 - € 500).

2.2.3 WP4 Use cases

Moreover, the following use cases are presented in WP4 and will may be eventually incorporated in the CYBECO Toolbox, based on the availability of the modeling framework from WP3:

- Use case 1: Cyber-insurance selection process for an SME
    - Overview: This use case describes the selection process of a cyber-insurance product from an SME willing to cover from specific cyber-related risks, and how the SME will decide about the best price/coverage ratio amongst the options offered by the insurance company. The perspective of the selection process is that of the decision-maker in the SME, i.e. the company CEO. The risk case in section 2.2.1 is an example of this.
    - Cyber-insurance related terms: cyber-insurance products, internal data loss, Asset classification, Impact analysis of business interruption, Financial impact quantification & insurance price comparison.
- Use case 2: Loss of personally identifiable data for a large company in the financial sector
    - This use case addresses the risk of the loss of personally identifiable data for a large company, resulting in a number of negative impacts for the company such as brand damage, loss of competitive advantage, regulatory fines, etc.
    - Cyber-insurance related terms: Hackers, “command and control” component, personally identifiable information (PII).
- Use case 3: Insurance fraud for an SME in the professional services sector
    - This use case illustrates the risk that an insured company might attack itself intentionally to collect an insurance pay-out.
    - Cyber-insurance related terms: Insurance fraud, ransomware, Company insiders
- Use case 4: Products / Services Manipulation for a large company in the manufacturing sector
    - Overview: This use case addresses the risk of highly skilled attackers targeting large manufacturing companies. This type of attack involves manipulation of products or related services, compromising the entire production line.
    - Cyber-insurance related terms: insurance claim, hackers.
- Use case 5: Insufficient insurance coverage for an SME operating in the IT industry sector

- Overview: This use case accounts for the risk for an SME of insufficient cyber-insurance coverage, in the event that a cyber-attack on the SME has a significant impact to 3rd party companies relying on the SME's products or services.
- Cyber-insurance related terms: cyber-attack, DDoS, cyber-insurance coverage.

- Use case 6: Accumulation of cyber-incidents following a single large-scale attack with involvement of reinsurance in the claim process
  - Overview: This use case addresses the risk of a targeted or random large-scale attack from highly skilled attackers (for example, nation states or organized crime groups) that has major repercussions on a wide range of market segments and market sectors.
  - Cyber-insurance related terms: phishing, infected email attachment, vulnerability exploit, ransomware, Business continuity interruption, Loss of critical data due to malicious encryption, Reinsurance company.

2.3 KB structure and catalogue reference

By cross-referencing the content requirements analysis presented in 2.2 with the standards and catalogues presented in 2.1, we come up with the following basic hierarchy for the KB.

Category of entities	Entity	Parameters of entity	Source
RISK	**Risk term**	• Term • Definition	*Vocabularies of ISO 31000, ISO 73, and ISO 27000 to 27005* *Example: risk, vulnerability, …*
THREAT	**Threat actor**	• Threat actor type	*STIX V2.0 Part 1, Section 6.9 and Part 2, Section 2.10* *Example: activist, competitor, hacker, insider accidental, …*

			ETSI GS ISI 002 V1.2.1 Annex B (B.1.1)
			Example:
			• *Employee*
			  ○ *Administrator*
			  ○ *End user*
			• *On-premises or off-premises service provider*
			  ○ *Administrator*
			• *External agent*
			  ○ *Corporation*
			  ○ *Individual person (fraud)*

		• Threat actor role	*STIX V2.0 Part 1, Section 6.10* *Example: agent, malware-author, sponsor, …*
		• Threat actor sophistication	*STIX V2.0 Part 1, Section 6.11* *Example: minimal, intermediate, expert, innovator, …*
		• Threat actor motivation	*STIX V2.0 Part 1, Section 6.1 (Attack motivation)* *Example: accidental, coercion, ideology, personal gain, …*
		• Threat actor resources	*STIX V2.0 Part 1, Section 6.2 (Attack resource level)* *Example: individual, contest, team, government, …*
	Threat action	• Name • Description	*ENISA Threat Taxonomy v1.0, Section 3 (highest levels in general)* *Example: physical attack, unintentional loss of info or IT assets, …* *ETSI GS ISI 002 V1.2.1 Annex B (B.1.1, The Whys)* *A Taxonomy of Operational Cyber Security Risks V2*

	Cyberattack pattern	• Name
		• Description
			CAPEC
			Examples:
			• *Manipulate data structures*
			  ○ *Buffer manipulation*
			  ▪ *Overflow buffers*
			  • *SOAP array overflow*
			STIX V2.0 Part 2, Section 2.1: No catalogue, STIX refers to CAPEC as example catalogue
			ENISA Threat Taxonomy v1.0, Section 3 (some of the lowest levels)
			Examples: credential stealing trojans, rootkits, mobile malware, …
			ETSI GS ISI 002 V1.2.1 Annex B (B.1.2, The What and B.1.3, The Hows)
			Example:
			• *Unauthorized action on the information system and/or against the organization*
			  ○ *External fraudulent action on a VoIP or not voice system*
			  ▪ *Telephone capacity misappropriation*
			  ▪ *Artificial traffic increase in order to increase billing*
			  ▪ *Means for either events (external attackers) are first intrusions and then … [from the Hows]*

	Indicators of cyberattacks	• Name
		• Description
			ETSI GS ISI 001-1 V1.1.2 Section 5.5
			Examples:
			• *Intrusions and external attacks*
			  ○ *Forged domain or brand names impersonating or imitating legitimate and genuine names*
			  ○ *Wholly or partly forged websites (excluding parking*

			pages) spoiling company's image or business *STIX V2.0 Part 1, Section 6.5, and Part 2, Section 2.5 (Indicator level)* *Example: anomalous activity, benign, malicious activity, …*

	Malware	• Name
		• Description
			STIX V2.0 Part 1, Section 6.7 and Part 2, Section 2.7 (malware)
			Example: adware, bot, dropper, rootkit, …
			
			STIX V2.0 Part 1, Section 6.12 and Part 2, Section 2.11 (legitimate tools used maliciously)
			Example: denial of service, exploitation, remote access, …
			
			MAEC Language V4.1 Specification – Default Vocabularies v1.1 2.5.3.1 (malware capability) and 2.6 (strategic objectives and tactical objectives associated with specific MAEC capabilities)
			• *Example:*
			  ○ *Command and control,*
			  ○ *Privilege escalation,*
			  ○ *Anti-code analysis (capability)*
			  ▪ *Anti-debugging (strategic objective)*
			
			MAEC Language V4.1 Specification – Default Vocabularies v1.1 2.5.4.1 (malware common label)
			Example: adware, clicker, data diddler, downloader, …

DIGITAL SYSTEM	**System Assets**	• Name • Description	*ETSI GS ISI 002 V1.2.1 Annex B (B.1.6, on what kind of asset)* *Example:* • *Databases and applications* ○ *Public cloud*

			▪ *Enterprise standard application (ERP, supply chain, …)*

	Vulnerabilities /Weaknesses	• Name
		• Description
			STIX V2.0 Part 2, Section 2.12 No catalogue,
			
			CWE (weaknesses are generalizations of vulnerabilities, which are more technical)
			Examples
			• *Incorrect calculation*
			  ○ *Incorrect calculation of buffer size*
			
			ETSI GS ISI 001-1 V1.1.2 Section 5.5
			Example:
			• *Passwords illicitly handled or managed*
			  ○ *Weak password used*
			  ○ *Passwords not changed*
			
			ETSI GS ISI 002 V1.2.1 Annex B (B.2.1.1-6 vulnerabilities)
			Examples:
			• *Behavioral vulnerability*
			  ○ *Internet illicitly accessed*
			  ○ *Anonymization proxy used to access the Internet from a professional workstation …*
			
			CVE, OVAL are extremely huge DB (ten of thousands of vulnerabilities)

ORGANISATION	**Assets**	• Name • Description	
	Sector	• Name • Description	*STIX V2.0 Part 1, Section 6.6* *Example: agriculture, communications, non-profit, government local, …*
SECURITY ACTIONS	**Security control**	• Name • Description	*STIX V2.0 Part 2, Section 2.1 (Course of action, No catalogue)*

			No catalogue, but encompasses security controls like the ones in NIST SP 800-53
			
			NIST SP 800-53 Rev 4
			Example:
			• *Access control*
			  ○ *Account management*
			  ▪ *Automated system account management*
			  ▪ *Disable inactive accounts*

	Cyber insurance	• Name • Description	

IMPACTS	**Impacts**	• Name
		• Description
			ETSI GS ISI 001-1 V1.1.2 Section 5.6 (some web impacts)
			Examples: Average cost to tackle a critical security incident, average time of websites downtime due to successful malicious attack, …
			
			ETSI GS ISI 002 V1.2.1 Annex B (B.1.7, impacts in terms of confidentiality, integrity and availability)
			Examples:
			• *Loss of confidentiality*
			  ○ *Personal identifiable information*
			  ▪ *Customer*
			  • *Credit card number*
			ETSI GS ISI 002 V1.2.1 Annex B (B.1.8, impacts in general)
			Example:
			• *Direct impact*
			  ○ *Loss of productivity*
			  ○ *Incident recovery costs*
			  ▪ *Technical individual time*
			  ○ *Life or health consequences*

Table 2 cyber-insurance related catalogues and KB structure reference

3 CYBECO KB Design

3.1 KB Functionalities

KB Browsing

From the main page or using the main menu, the user may navigate to the KB and start browsing the taxonomy of various entities (threats, security controls, Risk Analysis Templates, etc.). For example, for every threat, there is a description page that also contains links to siblings, parent category and children categories/threats.

KB Search engine

The user may enter a term in the search box with Autocomplete functionality. The Autocomplete provides suggestions while the user types into the search field. If the user hits the search button, they are redirected to a search results page. The search results may be divided into entity types and are sorted by relevance.

Linking with Risk Analysis Templates

All cyber-insurance related information used in the risk analysis templates will be entered in the KB and there must have links to the KB for reference.

3.2 Data Collection Template

The Data Collection Template is a spreadsheet containing the basic structure of the KB. The idea is to create a file that can be parsed and can be used to upload data programmatically in the KB, in order to facilitate content collection. Partners are invited to use the primary hierarchy or add new categories when required.

The table is made in such a form that it can be translated into a hierarchical tree structure. However, a node in our hierarchy can be related to other nodes that are not parents or children.

Parent Category	Term	Has Children	Details/Definition	Other Attributes	Source	Comments	Related term	Related term2	Related term3
	ROOT Node	Yes	Hierarchy root node						
ROOT Node	RISK	Yes	Risk terms category						
ROOT Node	THREAT	Yes	In computer security, a threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.						
THREAT	Threat actor	Yes	A threat actor or malicious actor is a person or entity that is responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity.	type, role, sophistication, motivation, resource	*STIX V2.0 Part 1, Section 6.9 and Part 2, Section 2.10*				
THREAT	Threat action	Yes			STIX V2.0 Part 1, Section 6.10				
THREAT	Cyberattack pattern	Yes			CAPEC				
THREAT	Indicators of cyberattacks	Yes			ETSI GS ISI 001-1 V1.1.2 Section 5.5				
THREAT	Malware	Yes			STIX V2.0 Part 1, Section 6.7 and Part 2, Section 2.7				
ROOT Node	DIGITAL SYSTEM	Yes							

DIGITAL SYSTEM	System Assets	Yes			ETSI GS ISI 002 V1.2.1 Annex B (B.1.6, on what kind of asset)				
DIGITAL SYSTEM	Vulnerabilities/Weaknesses	Yes			STIX V2.0 Part 2, Section 2.12				
ROOT Node	ORGANIZATION	Yes							
ORGANIZATION	Assets	Yes							
ORGANIZATION	Sector	Yes			STIX V2.0 Part 1, Section 6.6				
ROOT Node	SECURITY ACTIONS	Yes							
SECURITY ACTIONS	Security control	Yes			STIX V2.0 Part 2, Section 2.1				
SECURITY ACTIONS	Cyber insurance	Yes	Cyber-insurance is an insurance product used to protect businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities.						
ROOT Node	IMPACTS	Yes			ETSI GS ISI 001-1 V1.1.2 Section 5.6				
Security control	IDS	No	An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.		https://en.wikipedia.org/wiki/Intrusion_detection_system				

Security control	IPS	No	An intrusion prevention system (IPS) is a system that monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.		https://www.techopedia.com/definition/15998/intrusion-prevention-system-ips				
Malware	rootkit	No	A type of malware that hides its files or processes from normal methods of monitoring in order to conceal its presence and activities. Rootkits can operate at a number of levels, from the application level – simply replacing or adjusting the settings of system software to prevent the display of certain information		STIX V2.0 Part 1, Section 6.7				
Malware	backdoor	No	A malicious program that allows an attacker to perform actions on a remote system, such as transferring files, acquiring passwords, or executing arbitrary commands		Mell, P., Kent, K. and Nusbaum, J., "Guide to Malware Incident Prevention and Handling", NIST Special Publication 800-83, November		IDS	IPS	

					2005. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-83.pdf.				

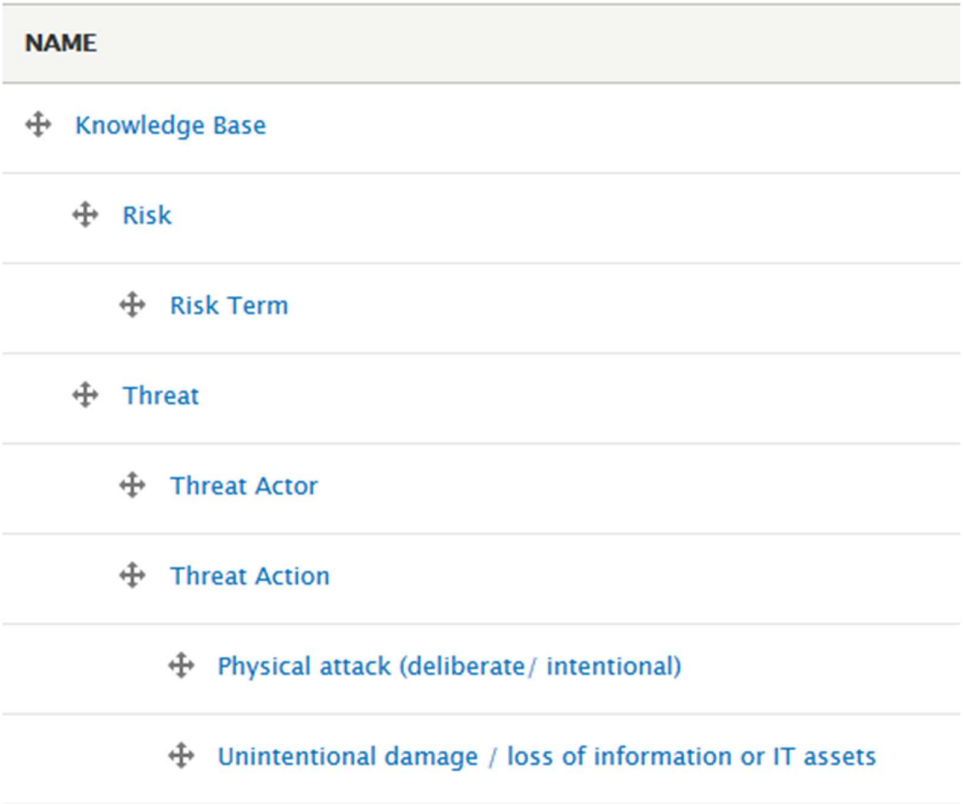
Table 3 KB data template

4 KB Implementation Details

CYBECO Toolbox is deployed on Drupal[12] and it is making use of various modules to provide the desired functionality. These modules are used for creating the entries for the knowledge base in an organised way and searching for terms assisted by autocomplete.

4.1 Taxonomy module

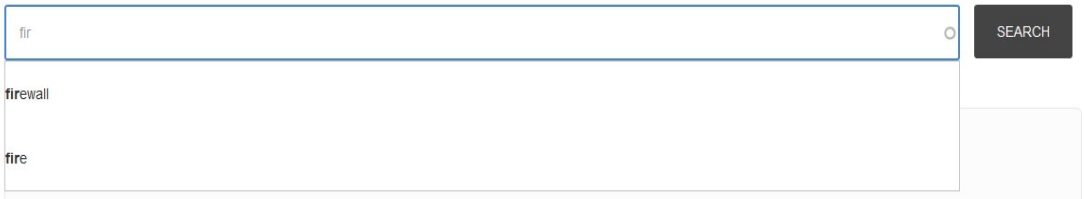
The Taxonomy module is one of the core modules installed on Drupal used for the CYBECO Toolbox. Using an additional module, the Taxonomy Menu, the KB content can be efficiently organised in categories and subcategories in a tree form.



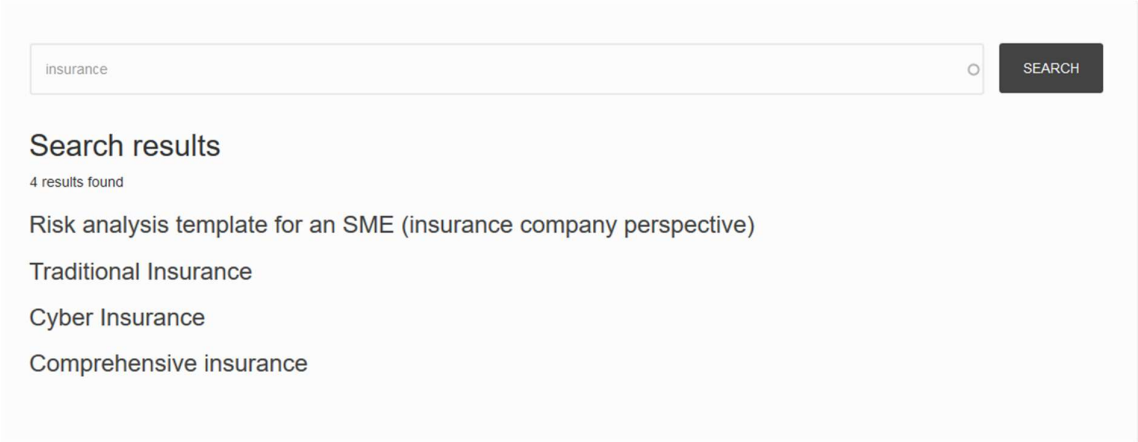
Using this structure, the Menu Breadcrumb module provides the breadcrumb [1]functionality which allows logged in users to easily see their current position in the knowledge base and navigate to previous nodes of the branch they are currently exploring.

4.2 KB search module

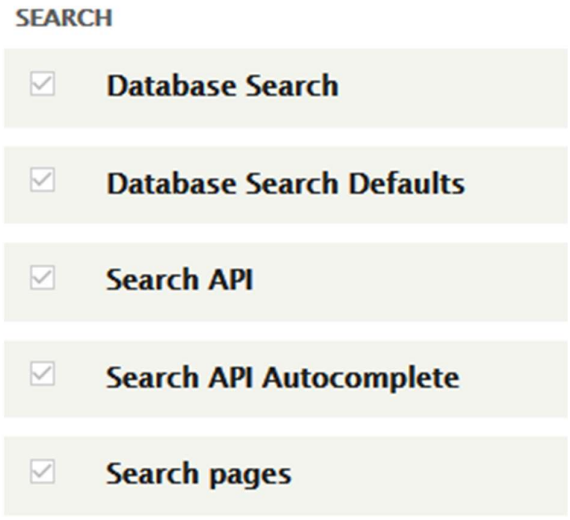
The search block appears in all pages that a logged in user has access, apart from the administrator pages. It allows the user to search for terms in the KB, assisted by autocomplete. This enables the user to quickly find the terms he or she is looking for.



If the search returns more that one results, the user can click any of them and will be redirected to the respective page, whereas if the term is not found a message appears.



[1] A type of secondary navigation scheme that reveals the user's location in a website



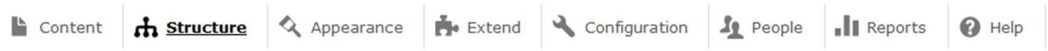
The search functionality is provided with the use of five modules under the search group on the modules page that can only be accessed by the administrator. Each module has its own role, and their combined use provides the desired functionality.

4.3 KB Editor module (Drupal back-office)

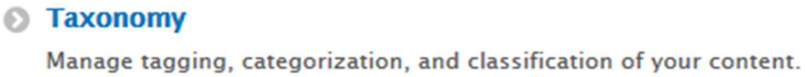
A user that has the appropriate rights is able to add content to the knowledge base utilizing the default Drupal 8 functionality along with the functionality provided by the taxonomy module mentioned previously.

Adding a new category/subcategory to the knowledge base.

In order to add a new category a user with the appropriate permissions has to start by clicking on the Structure menu on the administrator bar.



The next step is to select Taxonomy from the listed structures.

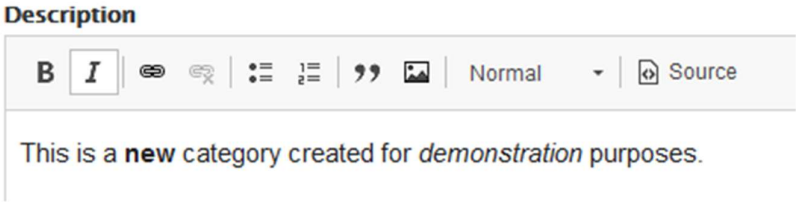


On the next page the user must click on List Terms next to KB.

Now the user can see the tree like structure of the knowledge base that was described before. Next to each of the current categories there is a button that can be used either for editing or deleting one of them. At the top of it there is the Add Term Button, which will allow the user to add a new category.

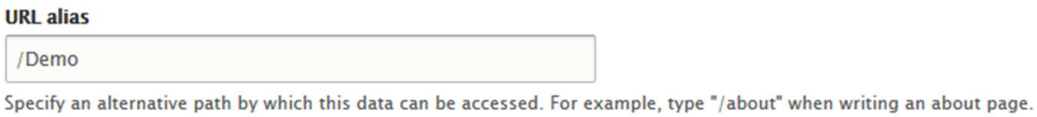
All the information for the new category has to be filled in the page that appears after clicking on Add Term button. The name field is the name of the category.

It is possible to create an optional description for the new category below it.



The next step is very important since it will determine where this category will be added. Clicking on RELATIONS below the description a box titled Parent Terms appears. The new category will become a subcategory of whichever term is selected here.

Finally, a friendly URL can be added, which will be what appears on the browser URL box when this category is visited.



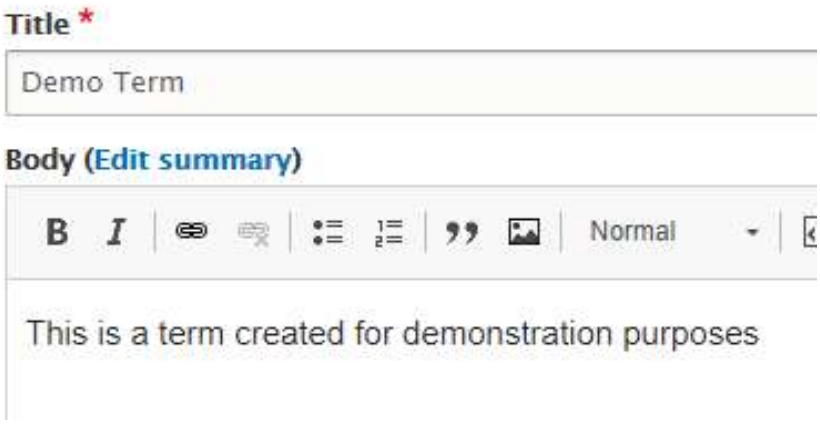
Clicking the Save button at the bottom will create this new category.

Adding a new term to a category.

A user with appropriate privileges starts by clicking on Content on the Administrator Bar.

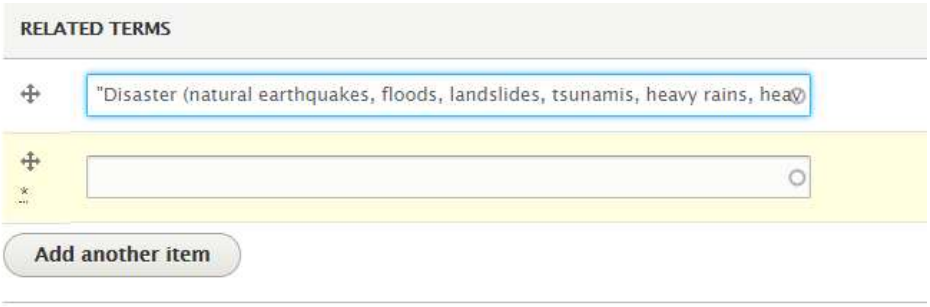
A list of all the pages appears. This is where the user can also delete or edit previously added terms to the knowledge base. The next step is to click on the Add Content button on the top of the page.

Here the user must select what king of content type needs to be added. After selecting it the user will have to fill in the “Title” field for the name of the new term and the Body field which refers to the actual content.



Next it is important to fill in the category in which this term will be added. This process is assisted by autocomplete after the user starts typing.

If the selected content type has the option for related terms, the user can also add these here. These terms will appear below the description of the term. This process is also assisted by autocomplete.



A friendly URL can be added by clicking on the URL PATH SETTINGS on the right side of the page, which is what will appear on the URL box of the browser when visiting this term.

The final step is to click on the SAVE button at the bottom of the page and the new term will be added to the knowledge base.

5 Conclusions

The goal of this deliverable is to manage the overall data and content collection, modeling and integration activities required to provide the CYBECO toolkit with relevant, attractive and standardized cybersecurity related content. Since there are extensive well-established catalogues and vocabularies describing cyber-insurance related terms, the goal of the CYBECO KB is not to provide yet another extensive glossary, but to support the risk analysis module by providing information about all cyber-insurance related terms used in the Risk Analysis module.

For that reason, we created a KB in the form of a hierarchical taxonomy of cyber-insurance related terms, organizing the main structure based on the needs of the Toolbox and the analysis of well-established catalogues and vocabularies. The KB supports browsing of the hierarchy, a search engine with autocomplete functionality and provides cross-references to the risk analysis templates of the Toolbox. For the population of the KB, a template was offered to the project consortium, and a web interface was developed for populating and maintaining the database.

6 References

1. ISO 31000 - Risk management: https://www.iso.org/iso-31000-risk-management.html
2. The ISO 27000 series of standards: http://www.27000.org/index.htm
3. STIX™ Version 2.0. Part 1: http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html#_Toc496709238
4. STIX™ Version 2.0. Part 2: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html
5. ENISA Threat taxonomy: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy
6. CAPEC: https://capec.mitre.org/
7. MAEC: https://maecproject.github.io/documentation/overview/MAEC_Overview.pdf
8. CWE: https://cwe.mitre.org/
9. CVE: https://cve.mitre.org/
10. OVAL: https://oval.mitre.org/
11. NIST Special Publication 800-53 (Rev. 4): https://nvd.nist.gov/800-53/Rev4
12. Drupal: https://www.drupal.org/

7 Acronyms and Abbreviations

KB	Knowledge Base
PII	personally identifiable user data
DDoS	Distributed Denial of Service
SME	Small and medium-sized enterprise