GEIGER

Deliverable D3.1 Training Plan

Point of Contact	Bernd Remmele
Institution	Pädagogische Hochschule Freiburg (PHF)
E-mail	bernd.remmele@ph-freiburg.de
Phone	+49 761 682 625

Project Acronym	GEIGER
Project Title	GEIGER Cybersecurity Counter
Grant Agreement No.	883588
Topic	H2020-SU-DS03
Project start date	1 June 2020
Dissemination level	Public
Due date	M06
Date of delivery	30. Nov. 2020
Lead partner	PHF
Contributing partners	UU, TECH.EU, KASP, PHF, MI, KPMG, BBB, ATOS, KSV, HAAKO, CERT-RO, CLUJ IT, E-ABO, SCB, PT, SRA, CL
Authors	Bernd Remmele (PHF), Jessica Peichl (PHF)
Contributions	Alina Boutiuc-Kaiser (PHF), Samuel Fricker, Bettina Schneider, Natalie Jonkers, Petra Asprion, Martin Gwerder, Frank Grimberg, Mia Braunwalder, Alireza Shojaifar (FHNW), David Bar, Lior Armiev (KPMG), Wissam Mallouli, Edgardo Montes de Oca (MI), Amedeo D'Arcangelo (KSP), Max van Haastrecht, Ingy Sarhan (UU), Jürg Haller (BBB), Roland Marcel Rupp, Euplio Di Gregorio (SKV), Corjan Aalbregt, Tony van Oorschot (SRA), Stelian Brad, Adrian Colesa (ClujIT), Heini Järvinen (Tech.EU), Jose Franscisco Ruiz (ATOS)
Reviewers	Bettina Schneider, Petra Asprion, Samuel Fricker (FHNW), Marco Spruit (UU), Jürg Haller (BBB)

This document contains information that is treated as confidential and proprietary by the GEIGER Consortium. Neither this document nor the information contained herein shall be used, duplicated, or communicated by any means to any third party, in whole or in parts, except with prior written consent of the GEIGER Consortium.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883588 (GEIGER). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

Revision History

Version	Date	Author	Comment
0.1	06/11/2020	Bernd Remmele (PHF) Jessica Peichl (PHF) Samuel Fricker (FHNW) Max van Haastrecht (UU) Lior Armive (KPMG) Amedeo D'Arcangelo (KSP) Wissam Mallouli (MI) Lior Armive (KPMG) Jürg Haller (BBB) Lio di Gregorio (SKV) Stelian Brad (CLUJ IT) Tony van Oorschot (SRA)	Draft version in advance to WP3 plenary meeting (9.11.20)
0.2	16/11/2020	Bernd Remmele (PHF) Jessica Peichl (PHF)	Version for Review
0.3	20/11/2020	Bettina Schneider (FHNW) Petra Asprion (FHNW)	First Review
0.4	24/11/2020	Bernd Remmele (PHF)	Version for Second Review
0.5	24/11/2020	Samuel Fricker (FHNW)	Second Review
0.9	30/11/2020	Bernd Remmele (PHF) Jessica Peichl (PHF)	Final Version
1.0	30/11/2020	Samuel Fricker (FHNW) Bettina Schneider (FHNW)	Quality Control and Submission

Contents

Abbreviations, participant short names and glossary

Abbreviations

CSD	Certified Security Defender
ENISA	European Union Agency for Cybersecurity
GCG	GEIGER Competence Grid
GEE	GEIGER Education Ecosystem
KPI	Key Performance Indicator
LMS	Learning Management System
LRS	Learning Record Store
MSE	Micro or Small Enterprise
SCORM	Sharable Content Object Reference Model
SRL	Self-regulated Learning
TP	Training Plan
xAPI	Experience Application Programming Interface

Participant short names

FHNW	Fachhochschule Nordwestschweiz
UU	Universiteit Utrecht
TECH.EU	Fores Media Limited
KSP	Kaspersky Lab Italia Srl
PFH	Pädagogische Hochschule Freiburg
MI	Montimage EURL
KPMG	Somekh Chaikin Partnership
BBB	Berufsfachschule BBB Baden
ATOS	Atos IT Solutions and Services Iberia SL
SKV	Schweizerischer KMU Verband
HAAKO	Haako GMBH
CERT-RO	Centrul National de Raspuns la Incidente de Securitate Cibernetica
CLUJ IT	Asociatia Cluj IT
E-ABO	e-abo Gmbh
SCB	Braintronix Srl
PT	Public Tender Srl

SRA	Samenwerkende Registeraccountants en Accountants-Administratieconsulenten
CL	Coiffure Loredana

Glossary

Competence Competence is the capability of a person to deal with a specific task, i.e. there are always two sides: the operation/action and the object of the operation. Accordingly, a usual definition of competence consists of an operator and an object. Competence usually refers to declarative knowledge (about a topic) and practical skills (acting with a topical object). It can also include motivational and volitional aspects, i.e. not only the ability but also the readiness to fulfil a task.

Competence Grid For complex educational purposes, it is useful to structure the set of competencies to be trained. First, this concerns the (cumulative) competence development; simply put: from easy to difficult. This development can refer to the advancement of the complexity of the topical issue as well as of the operation. Second, as competences refer to tasks, it can be useful to distinguish topical fields that systematically, i.e. in regard to learning, subdivide the given field of knowledge.

Curriculum A curriculum defines the set of trainings/modules of a specific course in a general manner. In the given context, this implies that there will be different curricula for the different target groups that include specific selections from the competence grid and a set of topics. In this sense, the curriculum refers to the link between the competence grid and the syllabus. [Sometimes syllabus is used in the sense of curriculum.]

GEIGER Indicator The GEIGER Indicator is a key feature of the User Interface of the GEIGER Framework. It informs in a simple manner about the level of risk of the MSE (both social and technical) justified with recommendations for improvement.

Taxonomy of Operators There are different options to order operators for educational purposes. The fundamental distinctions, however, appear between theoretically know/understand, practically apply/use and innovatively analyse/synthesise, while this sequence implies an increase of competence.

Phases of Training A training sequence aiming at a specific competence or topic should be organised in specific phases to optimise learning. Typically, such a sequence starts with engaging/motivating the learner in concern of the learning goal, followed by reactivating of prior knowledge. In the next phases, new knowledge is presented and then applied by the learner. The sequences are usually close with tests or a control phase. Of course, training can deviate from this standard sequence where reasonable; e.g. motivation can be of different concern in relation to school or adult education.

(Certified) Security Defenders One of the main objectives of the GEIGER Education Ecosystem is the development of a scheme to train 'Security Defenders' specialised to work with GEIGER in MSEs – either with or without certification– and to conduct such training in an exemplary manner. Concerning the MSE context, the competencies are to be conceived in a way that they are acquirable by 'lay-persons', i.e. non-academic and non-ICT-specialist people. The focus lies on MSE-specific understanding of a coherent set of cyber-security issues including data privacy and detailed knowledge about GEIGER and its application within a (one) specific MSE usage environment as well as mentoring others about GEIGER in an MSE.

Self-Regulated Learning The focus of self-regulated learning in the present context is mainly on the dependency of the motivation of persons in MSEs to learn to improve cybersecurity and the ability to relate recognised learning objectives with potential learning opportunities. The focus is less on metacognition of learning strategies, as the learning of methodological choices in the GEIGER Educational Ecosystem may be limited for pertinent topics and competencies.

Syllabus A syllabus defines the set of trainings/modules of a specific course in a detailed manner. In addition to the competences and topics to be taught, a syllabus can include lesson plans, education materials, references to further resources etc.

[Sometimes curriculum is used in this sense.]

Topic A topic is a specific piece of content; a list of contents can define a field of knowledge. Topics are transverse to competences, i.e. dealing with a specific topic (GDPR), different competencies (analysing data processing; understanding private data) can be trained and also the same competence (handling settings) can be applied to different topics (browser or email settings). Nevertheless, within a specific topical field, a typical set of competencies will be salient.

List of tables

List of figures

Executive Summary

WP3 “Security Defenders Education” aims at building the GEIGER Education Ecosystem. It is directed at a set of interrelated objectives. These are educational schemes for ‘Security Defenders’ for MSEs, particularly including the development of educational infrastructure, course concepts, training materials of different types and a certification system for the ‘Security Defenders’, as well as the initiation and institutionalisation of the Communities of the ‘Security Defenders’ and of organisations providing education and training within the GEIGER context.

D3.1 “Training Plan” is the first deliverable of WP3. It summarises the specific conditions and requirements for the work to be done in concern of GEIGER Education Ecosystem and presents the result already achieved. The conditions and requirements result from:

- the specific expertise of partners contributing to the GEIGER Education Ecosystem,
- non-IT-experts in MSE environments being a major target group of the ‘Security Defenders Education’,
- the organisational conditions and specific target groups of partners providing courses, and
- perspectives of sustainable management of the GEIGER communities.

The results are mainly conceptual and thus will function as basis and guidance for the further work in WP3. The main results presented as part of the general elaboration of the GEIGER Education Ecosystem are:

- an overview of the theoretical learning background (e.g. game-based learning, reverse mentoring, or micro-learning),
- the basic organisation of the courses (e.g. their scheduling or the demand for specific educational features),
- the educational alignment of the GEIGER Toolbox (e.g. the levels of cybersecurity competence in an MSE as part of the GEIGER Score),
- the development of a competence grid (that identifies relevant competencies and models them in concern of levels and topical areas),
- the mapping of educational features provided by partners against the competence grid and learning scenarios specifically for the GEIGER Education Ecosystem, and
- management principles for the GEIGER communities (e.g. their openness).

1 Overview

This Training Plan (TP) is the first deliverable (D3.1) of WP3 “Security Defenders Education.” The general objectives of WP3 that are represented in the activities in the first six months concern:

- the reflection of security and data privacy issues in concern of the GEIGER Ecosystem; these have been systematically integrated into the GEIGER Competence Grid (see below) that will further function as the guiding tool for the concrete development and harmonisation of the GEE,
- outlining the conditions for the concrete production of educational materials and features for the different learning scenarios within the GEE, and
- the conceptualising the sustainable organisation the GEE, including the development of Educational Provider and Security Defender Community or training and certification.

1.1 KPI

There is a set of KPIs that relate directly and indirectly to the GEIGER Educational Ecosystem. They mainly refer to inputs provided by different partners in the form of educational features or materials, to the outputs in concern of target groups and their satisfaction with the GEE and commitments of long-term exploitation. It is the main rationale of this TP to align these aspects for guiding the project development reaching the KPIs systematically.

Among the partner inputs are within Objective 4: Experiential training for “Certified Security Defenders,” in particular:

- KPI 2.1/4.1: ≥ 5 Capability areas addressed by training modules
- KPI 2.2/4.2: ≥ 2/5 Learning games
- KPI 2.3/4.3: ≥ 5 Cyber-range supported challenges.

The GEIGER Competence Grid differentiates between four competence levels and three topical fields. This structuring can be considered as an advanced fulfilment of KPI 2.1/4.1.

Different partners will provide game-based and cyber-range-based of learning features for different target groups and educational scenarios that are part of the GEE

Among the outputs and commitments are within Objective 5: “Validate and demonstrate the approach in diverse, relevant operational environments,” in particular:

- KPI I2.1.5.2 and KPI I2.1.5.3: ≥200 Educated Cyber Security Defenders, including 100 Certified Cyber Security Defenders)
- KPI 5.2: GEIGER Framework will have been evaluated in ≥50 SMEs & MEs
- KPI I2.1.1.9: GEIGER capacity-building assessed in surveys with >1’000 responses.

1.2 Development Process for D3.1

This ‘Training Plan’ (D3.1) is the result of the cooperative work done in by the partners involved in WP3. PHF as WP-Leader – in close cooperation with the coordinator FHNW and the task leaders – summarised these results in this document that has been presented partially and as a draft to the partners involved during M1 to M6.

Due to specific heterogeneity of the partners involved and the complexity objective of developing an educational framework of a rather technical particularly for laypersons the general approach of PHF was to discuss the specific issues in bi-lateral meetings with the partners involved. As can be seen from the meeting log for WP3 PHF held series of meetings on the hand with partners providing educational materials and features and on the other hand with partners that are hosting a GEIGER Use Case.

Intermediate results, like, e.g. the draft Competence Grid, were used to guide the ongoing discussion.

For general coordination, feedback, and discussion, a multi-lateral series of meetings were held. The peak of the series were two plenary meetings (20 Aug and 9 Nov). Table 1 lists the meetings that were held for preparing the training plan.

Table 1: Meetings held for preparing the training plan.

Date	Topic	Format	Involved Partners
15.06.2020	KSP Educational Games	online	PHF, KSP
18.06.2020	KSP Educational Games	online	PHF, KSP
09.07.2020	Swiss Use Case	online	PHF, BBB
16.07.2020	MI contribution to Education	online	PHF, MI
21.07.2020	Romanian Use Case	online	PHF, ClujIT
28.07.2020	KPMG contribution to Education	online	PHF, KPMG
29.07.2020	T1.1 Use Case Call SRA	online	SRA, FHNW; PHF
11.08.2020	Coordination Dissemination / Education	online	PHF, Tech.EU
18.08.2020	T1.4 Education Definition Workshop	Freiburg, Germany and online	FHNW, PHF, BBB
20.08.2020	WP3 Plenary Meeting	online	FHWN, PH, MI, UU, SKV
24.08.2020	T1.1 Swiss Use Case Workshop, Kick-Off Cooperation with Coiffure Suisse	Brugg, Switzerland and online	FHNW, UU, BBB, SKV, HAAKO, CL, PHF, TECH.EU, KPMG, CLUJ IT, E-ABO, KPMG, MI, CERT-RO, KSP, SCB, NSCS, Coiffure Suisse
24.08.2020	T1.1 Swiss Use Case Workshop, Kick-Off Cooperation with Coiffure Suisse	Brugg, Switzerland and online	FHNW, UU, BBB, SKV, HAAKO, CL, PHF, TECH.EU, KPMG, CLUJ IT, E-ABO, KPMG, MI, CERT-RO, KSP, SCB, NSCS, Coiffure Suisse
02.09.2020	Alignment Indicator - Education	online	UU, PHF, MI
10.09.2020	GEIGER indicator prototype Meeting	online	PHF, UU
23.09.2020	Security Defenders Community discussion	Freiburg	FHNW, PHF
28.09.2020	Escape Room Game Test	Freiburg	FHNW, PHF
29.09.2020	Discussion Swiss Use Case Education	online	PHF, BBB
01.10.2020	Dutch Use Case Workshop	online	PHF, SRA, FHNW, UU, KSP, MI,
05.10.2020	Education Alignment	online	PHF, FHNW
06.10.2020	Toolbox Integration	online	PHF, Atos
07.10.2020	Romanian Use Case Discussion	online	PHF, Cluj IT

14.10.2020	KSP contribution to Education	online	PHF, KSP
15.10.2020	T3.3 Exchange with Swiss Cyber Defense DNAz an education provider	Basel, Switzerland	FHNW, SCD DANN
19.10.2020	MI contribution to Education	online	PHF, MI
20.10.2020	KPMG contribution to Education	online	PHF, KPMG
21.10.2020	Toolbox-Education Alignment	online	PHF, FHNW, UU, BBB
22.10.2020	Competence Grid, Communities	online	PHF, FHNW
26.10.2020	Swiss Use Case	online	PHF, BBB
26.10.2020	Dutch Use Case	online	PHF, SRA
09.11.2020	WP3 Plenary Meeting	online	PHF, FHNW, MI, KPMG, KSP, SKV, UU
09.11.2020	First Exchange on GEIGER communities	online	PHF, FHNW, TECH.EU
11.11.2020	Single Learner Toolbox Alignment	online	PHF, FHNW, MI, ATOS
12.11.2020	GEIGER communities	online	PHF, FHNW
19.11.2020	GEIGER communities	online	PHF, FHNW
24.11.2020	KPMG contribution to Education	online	PHF, KPMG

1.3 Result: The Training Plan (TP)

This TP provides a major draft of the Certified Security Defenders Education as a section of the Geiger Competence Grid, that allows differentiating competence levels and knowledge areas. The grid allows defining relevant partial sets of competences and topics that can be applied to the different MSE related contexts and educational scenarios the project addresses. Consequently, these implementations can be validated systematically in cooperation with the upcoming Validation WP.

The TP brings thus together the information relevant for structuring the work related to the GEIGER Education Ecosystem (GEE). The following analysis, outlining the GEE, brings together different dimensions that bear requirements and conditions for a successful work process, particularly:

- objectives of the project, including sustainability issues,
- contributions by partners (particularly educational features and materials),
- Use Case requirements, i.e. their educational elements,
- educational expertise, e.g. in concern of competence modelling or educational technology,
- educational management issues, e.g. like curriculum development and time planning, and
- community management.

There are salient issues, inherent in these conditional dimensions, that add specific complexity to the GEE, and which will turn up at certain points in this analysis – partially multiple times:

- the three Use Cases comprise heterogeneous target groups and learning scenarios,
- the Use Cases have due to their target groups have varying schedules for their course conduct,
- partners providing educational materials and features have very different approaches in concern of content, training approach and technology, and

- the GEE implies different forms or poles of training: for self-regulated learning (SRL, cf. glossary) single learners in a thus asynchronous way and for a learning group guided by a trainer synchronously in a physical or virtual 'classroom'.

As a result of the analysis conditions and issues, this TP is a tool for guiding work to be done as part of the GEE. In particular, it presents:

- the GEIGER Competence Grid (GCG) as a tool for guiding the further educational planning, e.g. to align the production of educational materials and features with the definition of target groups in the Use Cases,
- an overview of the scheduling of the different processes relevant for the GEE, i.e. the timing of the Use Case courses, the development of educational features provided by the partners and the development of the Toolbox, i.e. educational experiences of it,
- a description of the Educational Aspects of Use Case including a respective target group analysis, and
- an overview of these educational features to determine in which way they can be integrated with either form of the training – synchronous or asynchronous.

As the main result, the GEIGER Competence Grid functions as reference content-wise in concern of educational materials and measured. The Training Schedule (see below) serves as an organisational reference to harmonise the different processes within the GEE. A systematic analysis of the educational measures (games, simulations etc.) provided by the partners has been undertaken, competence goals have been referred to the GCG, and an educational structure has been related to the different learning scenarios within the GEE, i.e. mainly trainer-based courses and individual learning incidents in concern of competence requirements within a specific MSE.

1.4 Structure of this Deliverable

The remainder of the Training Plan Document is structured as follows. Chapter 2 covers relevant dimensions of standardisation aspects which derive from technological, organisational, and respective use case perspectives. In Chapter 3, an overview of the theoretical backgrounds on the underlying educational approaches of GEIGER education is given. Chapter 4 concerns the GEIGER Toolbox Alignment with GEIGER Education. Educational Aspects in concern of the specific use cases are covered in Chapter 5, followed by a specification of the overall learning goals in Chapter 6. The components of these learning goals are further examined in the GEIGER Competence Grid in Chapter 7. Considering the related practical arrangements of learning components, Chapter 8 describes the current state of educational features in the form of material contributions by respective consortium partners. The training schedule for the development and implementation of these educational features and further training arrangements is presented in Chapter 9. Chapter 10 concerns the GEIGER communities with a focus on the GEIGER Education Provider Community. The Training Plan concludes with Chapter 11 as an outlook on further tasks to be addressed in the next steps. Chapter 12 summarises and concludes.

2 Dimensions of ‘Standardisation’

Apart from the more general ‘Standardisation Mapping (T5.2)’ there are aspects that define standard-like conditions for specific educational endeavours within the GEE.

2.1 Swiss Use Case

The Swiss Use at BBB, partially due to its inclusion in the highly regulated system of dual vocational education in Switzerland, implies different aspects of standardisations.

Modules, which comprise typically 40 lessons of 45 minutes, are described in the form of a ‘Klassenlehrplan’ (course curriculum) that is a structured competence list. It includes, e.g. five ‘Handlungsziele’ (general learning objectives), which are further differentiated into 31 ‘Leistungsziele’ (detailed learning objectives). The former is based on competence guidelines of the federal vocational education administration (e.g. ICT-Berufsbildung 2020). The latter is described in a way that they can be self-assessed by the apprentices and the teachers for them – before and after the course. Three competence levels (mainly: reproduction, application, reflection) can be a target for each ‘Leistungsziel’.

The competences levels in the central ‘Bildungsplan’ of ICT-Berufsbildung, as part of the federal vocational education administration, are however differentiated following the six taxonomy (cf. glossary box) levels of Bloom (e.g. 1956). Due to Swiss vocational educational system being a dual system in this central ‘Bildungsplan’ the learning objectives are further differentiated between schools as well as within and across companies.

It is an important aspect for the GEIGER Education Ecosystem that the Swiss vocational education system is a dual system, i.e. apprentices are the same time working/learning in companies and at vocational school. On the one hand, apprentices can thus disseminate into their training companies. On the other hand, training companies want vocational schools to train useful competencies.

Taxonomy of Operators (cf. glossary):

There are different options to order operators for educational purposes. The fundamental distinctions, however, appear between theoretically know/understand, practically apply/use and innovatively analyse/synthesise, while this sequence implies an increase of competence.

2.2 Dutch Use Case

The Dutch Use at SRA is mainly conditioned by time restrictions and appeal to the target group.

SRA offers a diverse range of trainings and courses, i.e. small group training, workshops, classroom training, in-company training and e-learning. The training includes both knowledge and skills training. Depending on the subject and the objectives of the training, sessions may last from one or several half-day time slots (4 hours) up to several days spread over an extended period of time.

Until 2021, every accountant was obliged to obtain a certain number of permanent education points within each year. As of 2021, accountants have to write their personal development plan regarding the objectives they want to achieve. Therefore, the contribution of GEIGER to the respective learning plans must be clear to the learners.

The Dutch Digital Trust Center that supports businesses in concern of cyber threats provides – like CERTs – information on digital vulnerabilities that have to be taken into account in pertinent training.

2.3 Romanian Use Case

The Romanian Use organised by ClujIT can be handled in regard to different interests of the target groups within the framework of the Romanian National Matrix of Competencies for High-Level Education. As typical, the Romanian National Matrix of Competencies for High-Level Education refers to knowledge and skills mapped against six competence levels (from understanding fundamental concepts up to the usage of intelligent systems).

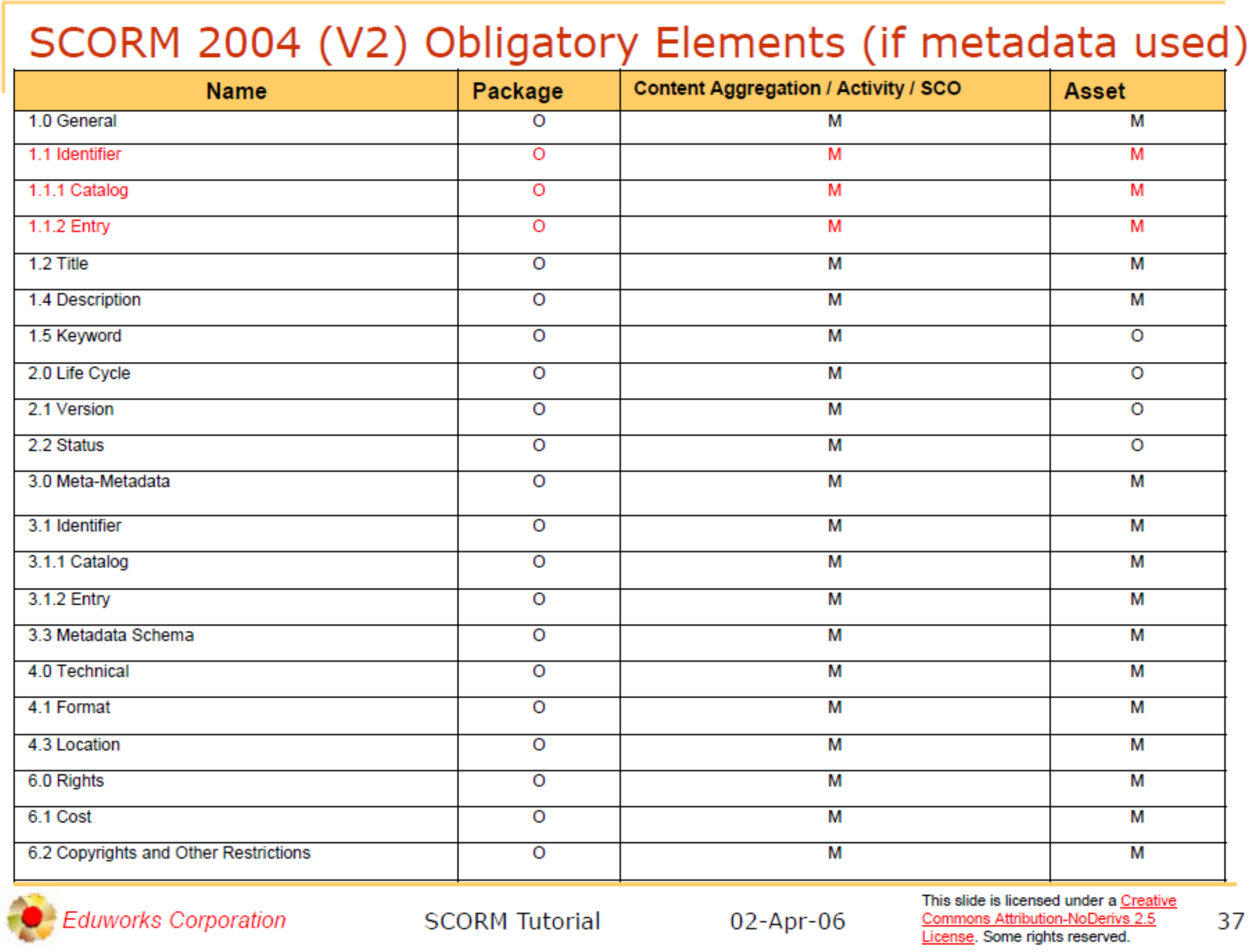
Courses are envisaged for MSE related target groups with and without IT-proficiency and with different scopes from one to several days or course time.

2.4 Transferability – Scorm Metadata-Standard vs xAPI

For the long-term sustainable success of the GEE the transferability of (digital) learning materials between Learning Management Systems (LMS) and beyond has to be secured. In the Use Cases, learning materials will be managed in LMSs such as „Moodle," which allow the combination of synchronous and asynchronous learning. The training sequences around the GEIGER Toolbox are likely to be implemented into independent applications.

The current metadata standard SCORM 2004 ensures transferability of content in between diverse LMS. In this way, materials can be easily adapted and embedded for future Use Cases. The creation of digital educational content follows along with the description of obligatory metadata elements listed below (Fig. 1). The full list allows, e.g. to automatically organise single materials/files within complex course structures.

Nevertheless, educational materials are usually created for specific educational purposes within a specific educational institution with its specific logistics for the specific target group with particular interests (cf. Remmele 2006). As these specificities are different from one case to another, the automated transfer has its limits. The complete list of SCORM Metadata fields also includes open fields that are to be read and interpreted by humans, i.e. translated into their context. This human dependence is still a general problem of automated transfer from one 'meaning-intensive' context into another.



SCORM 2004 (V2) Obligatory Elements (if metadata used)

Name	Package	Content Aggregation / Activity / SCO	Asset
1.0 General	O	M	M
1.1 Identifier	O	M	M
1.1.1 Catalog	O	M	M
1.1.2 Entry	O	M	M
1.2 Title	O	M	M
1.4 Description	O	M	M
1.5 Keyword	O	M	O
2.0 Life Cycle	O	M	O
2.1 Version	O	M	O
2.2 Status	O	M	O
3.0 Meta-Metadata	O	M	M
3.1 Identifier	O	M	M
3.1.1 Catalog	O	M	M
3.1.2 Entry	O	M	M
3.3 Metadata Schema	O	M	M
4.0 Technical	O	M	M
4.1 Format	O	M	M
4.3 Location	O	M	M
6.0 Rights	O	M	M
6.1 Cost	O	M	M
6.2 Copyrights and Other Restrictions	O	M	M

Eduworks Corporation SCORM Tutorial 02-Apr-06 This slide is licensed under a Creative Commons Attribution-NoDerivs 2.5 License. Some rights reserved. 37

Figure 1. SCORM 2004 Elements (Robson 2006)

2.5 Experience API

Another specification for learning technology to be considered for transferability is the Experience API (xAPI). In analogy to the SCORM format, xAPI captures learner's data in a standardised format. In contrast to SCORM it is not focused on LMSs. Furthermore, xAPI is oriented at learning activities that can be tracked within a wide range of systems by using a Learning Record Store (LRS) capable of receiving and processing requests. Through the LRS, the launching of content, as well as the managing of associated digital rights, can also be implemented (cf. also https://github.com/adlnet/xAPI-Spec).

SCORM vs xAPI: which is the better choice?

Choosing one of the two depends on the learning and target group requirements.

- Requirement 1: opt for SCORM if you are only interested in
    - Tracking a single learner at a time.
    - Creating an extensive library of learning objectives.
    - Using an LMS to manage and deliver your courses.
    - Tracking and collecting learners' performance.
    - Designing courses that monitor learners' behaviour and meet up with their needs.

- Requirement 2: opt for xAPI if you are interested in
    - Tracking learners' performance offline.
    - Recording all learning experiences, including simulation, serious games, mobile learning, and many more.
    - Tracking more than a single learner's performance or score.
    - Empowering learners to access your course at their convenience, on the go.
    - Tracking employees' performance.

Figure 2: Scorm vs xAPI (source: https://www.wizcabin.com/scorm-vs-xapi-the-right-choice-for-your-e-learning/)

BBB uses a Moodle LMS that complies with SCORM and xAPI. SRA uses „netdimensions" as LMS, which is also compatible with SCORM and xAPI. Cluj IT will also use Moodle.

However, apart from the possible advantage of SCORM concerning the transferability between LMSs, the intended interaction of learning features with the GEIGER Toolbox and its inclusion into business environments speaks for xAPI. From a sustainability point of view, it might furthermore be helpful to opt for the newer standard, which is xAPI, that might be supported by a larger number of applications on a long-term perspective.

2.6 Educational Service Provision: e.g. ISO 29993: 2017

The ISO landscape in concern of learning services is in constant change during the last years. Changes like digitalisation or the transfer from in-house training to independent service providers has changed the focus from the general quality management of such training organisations that provide a large set of courses to criteria that represent features that determine training quality. In this way, the new ISO 29993 'Learning services outside formal education – Service requirements' focuses on educational services in a general sense.

The ISO 29993: 2017 standard specifies the requirements for educational institutions when designing and implementing a learning service for vocational training and further education. These include among others: systematic learning needs analysis and its implementation into the curriculum, systematic preparation and delivery of the learning service in terms of staff, learning materials and learning environment, clear guidelines for the deployment of lecturers and their continuous further training, analysis of the requirements of learning assessments, systematic preparation, implementation and follow-up of the evaluation of the learning service.

Even if (commercial) educational institutions do not take the effort of an audit at a specific time, the criteria set by ISO standards structure an organisation and ease communication in these regards. For GEIGER related courses to be delivered by independent learning service providers, it would, of course, be favourable if they were certified according to ISO 29992:2017, however in the likely event that promising non-certified providers are interested or can be committed a respective quality check can be conducted.

Currently, there is no – known – similar standardisation approach to learning apps that could complement the learning sphere of the GEIGER Toolbox. It is thus a task– for the sustainable GEIGER body – to define a set of quality criteria in concern of topical, organisational, and technical fitting to the GEE.

3 Educational Approaches

Educational science has been dealing with a vast set of issues relevant to the GEIGER Education Ecosystem in the last decades: e-learning, game-based learning, activity-oriented learning, social learning etc. It is impossible to give a full account here. Thus, the following snippets only provide an idea of the general educational approach of GEIGER.

3.1 Experiential Learning

Kolb (1973) conceives the learning process as a learning cycle. Concrete Experiences are observed and reflected by the learner to form abstracts concepts and generalizations. This assimilation of the observations finally leads to action implications that are tested in new situations.

Kolb's theory is grounded in the learning models of Dewey, Lewin and Piaget aimed at suggesting a combined holistic perspective (cf. Kolb, 1984, pp. 20–23). Kolb offers the following coherent definition of learning: „Learning is the process whereby knowledge is created through the transformation of experience." (ibid., p. 38) He thereby emphasizes his view of the procedural nature of learning that is not limited to an outcome or content. Furthermore, Kolb perceives knowledge as a transformation process that continuously evolves. ibid., p. 38)

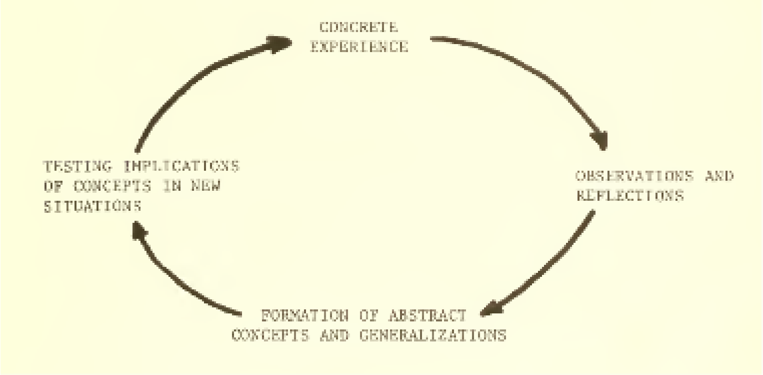

CONCRETE EXPERIENCE
OBSERVATIONS AND REFLECTIONS
FORMATION OF ABSTRACT CONCEPTS AND GENERALIZATIONS
TESTING IMPLICATIONS OF CONCEPTS IN NEW SITUATIONS

Figure 3. Learning cycle (Kolb 1973)

This continuous process of learning is grounded in experience, according to Kolb, more exactly in the „interplay between expectation and experience” (ibid., p. 28). Another dominant characteristic of the experiential learning concept is conflict. Conflicts that are routed between the concrete experience and abstract concepts, or likewise between observation and action also result in learning when resulted (ibid., p. 29). According to Kolb, learning is furthermore to be seen not as an isolated process directed inward, but a process that happens especially in the interaction between learner and environment (ibid., p. 34). He also underlines learning as an active and self-directed process that also applies to everyday life settings (ibid., p. 36).

With regard to the GEIGER educational approach that includes hands-on-experiences with the GEIGER Toolbox, Kolb’s experiential learning model is routed especially in the strong conjunction between the topics presented in the learning materials, their more or less guided active exploration of a demo-version of the GEIGER Toolbox, and the tasks that learners complete within their MSE working environment. Users might encounter the first concrete experiences on cybersecurity already in the tasks that are being presented to them. Observations and reflections are supported by background information on concrete examples on cybersecurity topics. The formation of abstract concepts and generalizations is supported by learning materials conveying general concepts. Single examples of threats or incidents are taken as a starting point for general cybersecurity rules.

3.2 Game-based learning

Salen and Zimmerman (2004) describe the concept of the game as a system in which *players* act according to *rules* within an *artificial conflict* that finally results in a *quantifiable outcome* (p. 80). Games are experienced as taking place outside the everyday life (cf. Huizinga 1956, p. 9). McGonigal (2012, p. 82) offers a similar definition of games based on four basic features: Goal, rules, feedback system and voluntary participation.

Game-based learning is found in serious games as a specialised form of games that are produced specifically for educational purposes. Whereas learning as such happens in all games, e.g. players acquiring game-specific skills to master the game (cf. Breuer, 2010, p.13), in serious games learning of specific content or skill, is intended. Pavlas describes this format as „games that work to provide learning, meaning, or similar outcomes rather than pure leisure experience“ (Pavlas, Heyne, Bedwell, Lazzara & Salas, 2010, p. 2398). Michael and Chen (2006) agree that „education (in its various forms) is the primary goal, rather than entertainment” (p. 17).

Underlying learning approaches in game-based learning environments may cover diverse learning theories, e.g. behaviourist, cognitivist or constructivist elements, as well as combinations of these approaches (cf. Plass et al., 2015, p. 261). Because of this wide variety of learning designs in games, an overarching theory of game-based learning will not be comprehensive. Plass et al. advocate a simplistic model that covers the basic structure of all learning games, containing the key elements of challenge, response and feedback (see Figure 3). When changes are constituted in the elements, and new challenges appear, a loop is generated. ibid., p. 262).

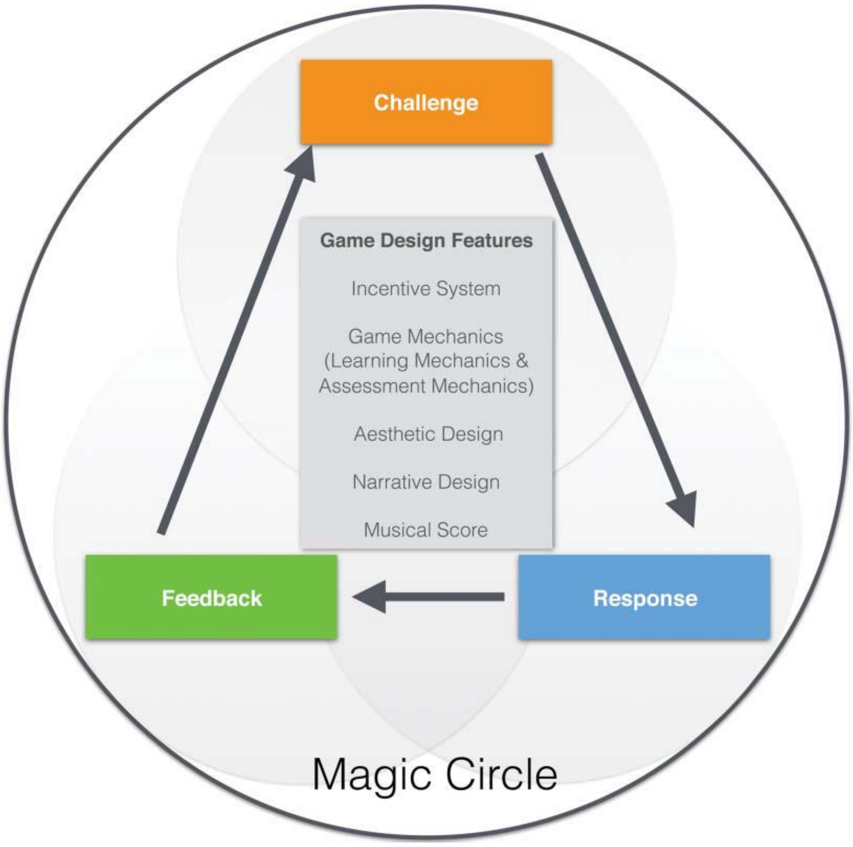


Figure 4 Challenge, Response and Feedback Loop in Games (Plass et al. 2015), p. 262

Plass et al. see arguments for applying game-based learning in positive aspects such as motivation or player engagement (ibid., p. 260). The authors emphasize, concerning their potential for learning, games have to convey learning engagement not only on a motivational, but also on a cognitive, affective, and sociocultural level (ibid., p. 277).

With regard to the learning materials deployed within the GEE, there is a number of games adapted to the topics (see Chapter 8). Within the scope of these games, a combination of different learning approaches can be identified.

Whereas game design features such as the narrative and aesthetic game design of the digital-based games show a wide variety, the games all comprise the general game elements. First of all, the available games provide a goal that has to be achieved by the players. The challenges within the game are adapted to the level of education. Therefore, response and feedback should occur on a level that neither demands too little nor overstrains the player's capabilities. The built-in incentive systems range from simple feedbacks within the narrative frame up to explicit numeric scores based on the player's actions.

3.3 Reverse Mentoring

Murphy (2012) defines the concept of reverse mentoring in the working context as „the pairing of a younger, junior employee acting as a mentor to share expertise with an older, senior colleague as the mentee." Reverse mentoring is based on the generational differences between mentor and mentee, especially the technological expertise of the younger mentors as well as their generational perspective (p. 555). The older mentee benefits from the expertise and innovative viewing points of the younger mentor, whereas mentors benefit from long-term experiences shared by the mentees.

The main focus for mentees is seen to a great extent in learning through knowledge sharing (ibid., p. 557). There are three types of learning generally elicited in mentoring relationships: Cognitive learning, skill-based learning and affective-based learning (Wanberg et al., 2003). In reverse mentoring, these types of knowledge sharing can operate in both directions (Murphy 2012, p. 557), e.g. while the mentor shares technological knowledge on software, the mentee may share declarative knowledge about organizational aspects in the company. Mentors can benefit from reverse mentoring in the sense of professional and leadership skill development (ibid., p. 555).

Successful reverse mentoring relationships in the sense of knowledge sharing and mutual support require a commitment of both parties „to the shared goal of mutual support and learning" (ibid., p. 558).

When looking at the Use Cases, the concept of reverse mentoring can be found in the interaction between MSEs and the Certified Cyber Security Defenders. In the specific example of the apprentices in the Swiss Use Case, the younger and most likely more tech-savvy coiffeuses in the apprenticeship undertake the first levels of the GEE and bring in their acquired knowledge on cybersecurity in their MSE. Based on the relationship of trust between the apprentice and their older co-workers – or mentees in terms of Murphy's concept – young adults bring in technological and behavioural advice concerning cybersecurity. Long-term co-workers have a broader view of the MSE structures and can help assess the implementation of cybersecurity aspects from an organisational point of view.

3.4 Micro/Nano-Learning

This specific pedagogical approach of Micro-Learning consists in reducing lessons into small, easy-to-absorb educational capsules. Its effectiveness is particularly related to the length of one capsule (e.g. 2 to 5 minutes; cf. Cole 2017) and to being optimized for Mobile Device Use. Hence, micro-lessons can be completed anywhere, anytime and, more importantly, at the learner's pace. In other words, it focuses on providing a learning experience to the learners, which is spread across a short time duration and fulfils the just in time learning objectives of the learners. This time aspect clearly matches the conditions of MSE environments where it might be difficult to follow longer or media-intensive learning incidents. With a growing amount of such small learning incidents learners can activate different prior knowledge or make more choices which to focus on and follow up – as of course, the most effective training is the one that motivates the learner to do/learn more her/himself; also sequences of learning incidents can end in different suggestions for following up.

3.5 Relation asynchronous (SRL) and synchronous

Learning within the GEE can happen – speaking of the mentioned two poles of the spectrum of learning scenarios – for self-regulated single learners in a thus asynchronous way and a learning group guided by a trainer synchronously in a physical or virtual 'classroom'. In the latter case, the persons teaching GEIGER related issues shall be able to rely on well-designed learning materials/features[1] adequately prepared for the specific context. The decision on whether and how to use these materials and features is, however, in the discretion of the individual trainer.

The objective of efficiency asks for the reusability of learner materials/features, like, e.g. digital educational content, online quizzes or assessments. In reference to the two poles, the reusability in the GEIGER context has two main fields of application: a) as part of trainer-based courses, e.g. as homework or for a kind of assessment during class, where teachers can didactically frame materials to the educational scenario; b) as part of applications in connection to the Toolbox, that need to be aligned in a pre-defined way (based on the GCG).

The two poles imply that also tracking of learner activity should be possible in both scenarios. This support means that the Toolbox should include the possibility to track learner activity, i.e. achievements, manually by trainers and learners as well as automatically as part of self-regulated online learning features.

3.6 Summary

Summarizing the theoretical approaches above, basic implications for the GEIGER educational approach can be outlined.

The most basic but also indispensable approach, especially concerning the SRL features is the necessity of a high usability and interaction grade. Learners need to receive consistent feedback within the progress and completion of activities. This concern lies in the challenge-response–feedback circle stated in the game-based learning approach, which concerns especially games that make up a considerable part of the SRL learning materials. Educational Levels will have to be considered and adapted for target groups.

Another approach to be considered for both SRL features and synchronous learning settings is the strong conjunction between the MSE and GEIGER environment. This concerns, in particular, the contents of the Demo Toolbox explored by learners. When looking at the reverse-mentoring approach, a lot of the potential success lies in the relationship between mentors and mentees. However, close conjunction between the learning environment and MSE can help justify Cybersecurity topics and is a necessary approach to enable the mentor to transfer Cybersecurity knowledge to the own MSE environment.

Considering the working environment of MSEs, individual approaches will have to be tailored for different target groups. Especially for the basic GEIGER educational levels, a limited timing schedule for the Romanian and Dutch Use Case can benefit from Nano/Micro-Learning and self-regulated features. Technical and didactical alignment of these different features will have to be ensured.

Specific requirements concerning the Demo Toolbox as a core feature of the GEIGER education are listed in Chapter 13.

4 GEIGER Toolbox Alignment

A basic assumption of GEIGER is that the Toolbox is part of a socio-technical environment. That environment not only comprises IT-features but is essentially dependent on the knowledge and behaviour of the people using it in their specific MSE context (in this regard MSEs seem much more diverse than bigger companies).

[1] ‚Material' expresses the didactical focus on content (e.g. a prioritized list of cyber-threats) whereas 'feature' expresses the focus on methodology (e.g. gamification) developed for a specific learning goal.

Accordingly, the GEIGER Indicator is conceived as representing not only the status of IT-systems but also of the capabilities of the people who are involved with the specific MSE implementation of the Toolbox. Thus, the Toolbox needs to be in alignment with the GEE because it aims at developing the knowledge and behaviour of the users.

This alignment has different dimensions:

- the Toolbox has to be part of trainer-based courses, like in the Use Cases, as an object of learning as interactive or action-oriented as possible,
- trainers should be able to report learning achievements to the Toolbox/Indicator of the company of the learners,
- persons responsible at a company, e.g. GEIGER Certified Security Defenders, should be able to report learning achievements in a similar way (e.g. when CSD or other experts disseminated cybersecurity or GEIGER specific knowledge in the company),
- self-regulated learning features that deal with relevant aspects of cybersecurity and are approved by GEIGER should be able to report the learning achievements automatically to the Toolbox/Indicator, and
- the GEIGER Toolbox should be able to identify (general and pressing) learning objectives and potentially recommend approved learning features or course topics.

Following the logic of the GEIGER Competence Grid (see below) self-regulated features for single learners it is sufficient to limit them to competences in the fields of general knowledge of a relevant set of cyber-security issues for any user, particularly in a business environment (Level 1) and of GEIGER related ones that can be reached by ICT-lay-people (Level 2 – Educated Security Defenders).

The training of persons to take responsibility, i.e. having to deal with the implementation of the Toolbox and the training of others on it, will rather be dependent on trainer-based courses or expert mentoring (Level 3 and 4).

5 Educational Aspects of the Use Cases

For the specification of the educational aspects of the three Use Cases, there is a need to define the target group entry levels and target organisational function or professions at the end of the training programme (cf. ANSSI 2017b, 14).

5.1 Swiss Apprentices: Non-ICT and ICT

In general, all Swiss apprentice classes within the Use Case are studying in their second school year, which is the pre-final year of their apprenticeship. Class-sizes are limited to a maximum number of 24 students aged between 17 and 18. Two diverse target groups are considered for the Use Case: hairdresser apprentices and apprentices in the field of systems technology. Different levels of competence and motivation have to be considered: The classes of hairdressers have less knowledge and confidence in IT-subjects and should be considered as students for basic modules. Students participating in technological courses have greater knowledge and interest and therefore, should be considered as students for the advanced modules.

Following the eminent difference of these two target groups in their previous knowledge and confidence in cybersecurity, a need for different entry levels emerges. On that account, the Level 1 (for the definition of levels see the GCG below) topics have been divided into sublevels 1a and 1b.

The entry point for hairdressers is at Level 1a, which includes the more basic topics of Level 1 in general. Once finished with Level 1a, the hairdressers can choose to proceed further to Level 1b. After completion of Level 1a and 1b, learners can continue with the education in Level 2 to become Educated Cybersecurity Defenders.

Apprentices in the technical and IT-field skip Level 1a to start the educational modules in Level 1b, where they refresh some basics they might already be familiar with and proceed to Level 2 and Level 3, to achieve the Security Defender Certificate by passing the assessment at the end of Level 3.

Contents and methods for both target groups should be closely linked to the working field of the students, e.g. giving students tasks on real-life working scenarios in their enterprises.

5.2 Dutch Accountants

In the Dutch Use Case of SRA (Samenwerkende Registeraccountants en Accountants-Administratie¬consulenten), the target group consists of accountants within the SRA community of accountant firms.

According to the explanations of SRA, the accountants have only basic knowledge or confidence on cybersecurity topics. In some firms, single tech-savvy or tech-interested employees have to be considered an exception to this general trend. In contrast to the lack of cybersecurity expertise, the overall awareness on the importance of the topic is rising, since gradually information and news on cyber-attacks increase. However, this awareness occurs on a rather abstract level that is not related to the own accountancy firm. A limited readiness on putting a high amount of effort into the topic of cybersecurity can be observed.

60-70 % of accountancy firms within the SRA network consist of fewer than 25 employees and in most cases don’t comprise an own IT-department. These firms might, therefore, potentially have an interest in piloting within the GEE. Most of the employees within this network can be seen as a target group starting in the basic Level 1. Exit Levels for accountants can be seen in general either at the end of Level 1 or Level 2. Tech-savvy employees within the accountancy field might proceed up to further levels.

5.3 Romanian Entrepreneurs

Around 60 MSEs within the ClujIT Cluster have indicated an interest in piloting in the GEE. Two diverging target groups can be determined within this cluster: A small number of MSEs that operate in the IT sector and a larger amount of MSEs that operate in the service field.

MSEs in the service field have little previous knowledge on cybersecurity, with some exceptions of specific competencies concentrated in a single person or position. Some MSEs have externalized IT-Services. The most important topic for MSEs in the service field is financial issues, e.g. banking fraud or financial transactions. The entry-level for this target group is determined at Level 1. Learners might proceed up to Level 2.

MSEs in the IT-Field have a high technical knowledge but need support on generating systematic cybersecurity management with a special focus on staff behaviour. The entry-level for this target group is specified at Level 3, and including a Security Defenders Certificate Assessment, as well as completion of Level 4 to arrange a business case of the GEE, i.e. it can be focused on the GEIGER specific columns (GEIGER Related and GEIGER Interaction cf. the GCG below).

Within the employees of both groups, managers in the technical or financial field are considered as the main target group.

6 Learning Goals

The learning goals of the GEE derive from different rationales in concern of the specificities of MSE target group.

GEIGER approaches a wide audience of potential users working in MSEs. Such small companies most often do not have professionalized IT processes or even departments, i.e. these users care for cybersecurity on the basis of their usually very limited private knowledge and experience. Often hardware and software is used both privately and professionally. Hence, the GEE has to build on and also advance general everyday cybersecurity knowledge to function as background for cybersecure behaviour also in business-life. Also, the motivational dimensions of cybersecurity learning cannot be severed from everyday IT-practice.

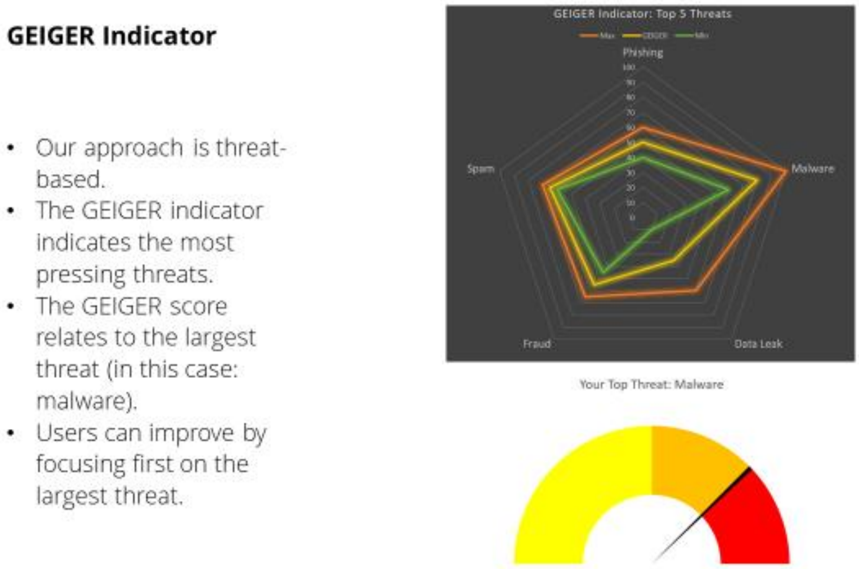
Insofar the cybersecurity of MSEs, due to lack of professionalized processes, MSEs are thus much more dependent on individual preparedness and behaviours. The GEE has to focus on threats that correspond to this situation. Business-related national and European cybersecurity initiatives have often neglected this target group and this non-specialist competence level.

Consequently, in concern of MSE specific lack of professionalized cybersecurity instruction, the GEE has also to reflect how knowledge is transferred from one person to another in such lay business contexts.

Another situational condition is that MSEs often use only very specific IT-applications and general consumer software. The GEE has thus to be flexible in concern of specific learning requirements of MSEs from different sectors or of different size.

Against this general backdrop, the GEE has of course to focus on the specific functionalities, advantages and terms of use the GEIGER Indicator implies.

In relation to these 'end-learner' issues, the GEE has also to integrate train-the-trainer schemes pertinent to the different context, i.e. in concern of the background of the learners as well as of the teachers, and schemes for professionalized services based on or related to GEIGER.



GEIGER Indicator

- Our approach is threat-based.
- The GEIGER indicator indicates the most pressing threats.
- The GEIGER score relates to the largest threat (in this case: malware).
- Users can improve by focusing first on the largest threat.

Figure 5 GEIGER Indicator

6.1 GEIGER Education Ecosystem for General – Business-related – Audiences

The GEE is addressed to the MSE related audiences. Not only IT-Experts are addressed, much more a wide range of entrepreneurs or MSE employees of different backgrounds and levels of previous IT-knowledge. The GEE has to fill gaps in general cybersecurity competences in order to make MSE specific competences fully functional.

When looking at curricular examples, there is a plethora of (academic) courses for IT specialist for different issues of cybersecurity and data protection/privacy (BSI, ISACA, CISCO …). In contrast, as many issues are not 'visible' or evident for lay people, there is a difficulty to outline a course that does not build on specialist technical knowledge.

One example of a course addressed at a general public that can be found within the European Union is ANSSI: "Syllabus pour le cours de sensibilisation et initiation à la Cybersécurité" of the French National Agency for Cybersecurity (ANSSI 2017a). ANSSI also provides a very detailed "MOOC de l'ANSSI" for the general public.

Another course, offered by the Electronic Frontier Foundation, provides a detailed free online course: "Security Education Companion - A free resource for digital security educators" (EFF 2020).

Also CISCO provides a set of courses from a beginners to a very professional technical level (e.g. CISCO 2018/19).

6.2 MSE Specifics

CERTs/CIRTs usually provide guidelines for the business world in concern of general cybersecurity issues as well as of most current threats, e.g. the instances of certain attacks. CERTs/CIRTS do not adequately differentiate in concern of relevance such issues dependent on the size of companies. It is thus necessary to prioritize MSE specific conditions.

In the narrower sense of cybersecurity, this can relate to issues of consumer software or everyday applications like email (whereas e.g. a food truck might not be the primary target of a ransomware attacker). Also, MSEs often – have the impression that they – have delegated cybersecurity responsibilities to large portals for web-shops, data-storage or email service providers. Having this impression can give them a deluding feeling of safety.

In the broader sense, this can also include compliance issues in concern of the Data Privacy regulations/laws like the Swiss 'Bundesgesetz über den Datenschutz' (DSG), or the EU General Data Protection Regulation (GDPR), as this directive applies to ubiquitous processes that– from a lay perspective – can look rather unproblematic, which are however illegal.

The long-term consequences of the GDPR on SMEs are not yet fully analysed. Kročil/Pospíšil (2020) have analysed this problem for a small subset:

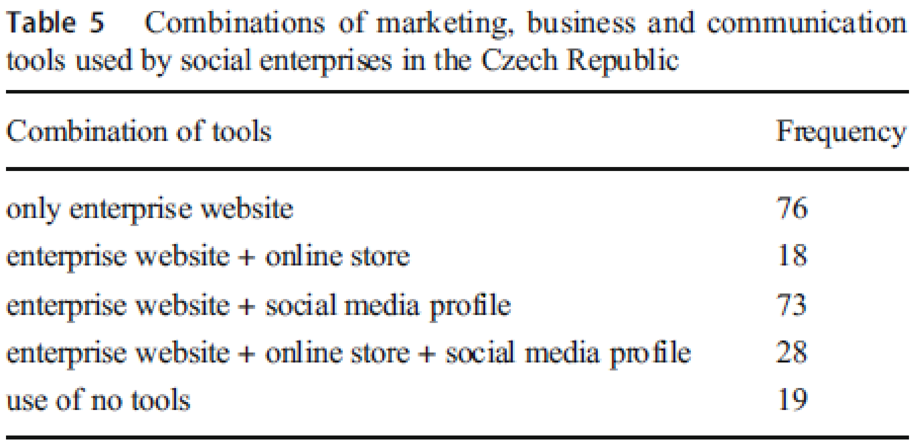


Table 5 Combinations of marketing, business and communication tools used by social enterprises in the Czech Republic

Combination of tools	Frequency
only enterprise website	76
enterprise website + online store	18
enterprise website + social media profile	73
enterprise website + online store + social media profile	28
use of no tools	19

Figure 6 GDPR Issues (Kročil/Pospíšil 2020)

It is necessary to take into account that there is a large scale of potential impacts due to individual action and a smaller scale of updated IT-security features in comparison to bigger companies.

As a conclusion, MSE specific training has thus to focus more on general routines of cybersecure behaviour than on tech-savvy handling of certain applications or default settings.

In this respect ENISA (2016) has conceived cyber hygiene as "establishing simple routine measures to minimise the risks from cyber threats" Also in the sense that "good cyber hygiene practices can drive increased immunity across businesses reducing the risk that one vulnerable organisation will be used to either mount attacks or compromise a supply chain."

In this respect, ENISA issued a set of recommendation for five compliance regimes, that can due to their very basic approach be adapted to MSE contexts, which relate to a big part to individual behaviour in different regards:

- Protect the perimeter
- Protect the network
- Protect individual devices
- Use the cloud in a secure manner

- Protect the supply chain.

Protecting the perimeter in MSEs that usually grant entry to work spaces in rather informal ways implies completely different advice than in a company with key card etc.

Further on ENISA outlined ten basic action points for protecting businesses against cyberthreats. However, these are again rather tech-savvy:

- Have a record of all hardware so you know what your estate looks like;
- Have a record of all software to ensure it is properly patched;
- Utilise secure configuration / hardening guides for all devices;
- Manage data in and out of your network;
- Scan all incoming emails;
- Minimise administrative accounts;
- Regularly back up data and test it can be restored;
- Establish an incident response plan;
- Enforce similar levels of security across the supply chain;
- Ensure suitable security controls in any service agreements).

Issues of such tech-savvy approaches need to be handled selectively and implied competences broken down to lay entry points and realistic competence expectations.

6.3 GEIGER-Related Topics

The learning goals of the GEE have to include issues that relate to the GEIGER Toolbox and its pertinent features. As the GEIGER Toolbox is conceived as a solution for many of the mentioned issues of general concern there are overlaps.

Depending on the function of a person in a company in relation to the GEIGER Framework there is a set of issues that are GEIGER specific – particularly:

- installing the GEIGER Toolbox and customizing it; this can e.g. include the ability to provide an overview of all CS-relevant hardware and software used in one's company,
- understanding which information the Indicator uses to generate a score,
- understanding general calculation principles of the score,
- understanding the automatic shielding the GEIGER Toolbox provides,
- ability to apply recommendations the GEIGER Toolbox generates,
- understanding the added value of connecting to the Geiger Cloud and the nature of the information that it processes.

Some of the functionalities that the GEIGER Toolbox integrates are also implied in other software solutions. Understanding what the GEIGER Toolbox does broadly implies understanding what other applications do. From an educational point of view, it is that being able to explain a function it is only a minor step to integrate different examples that fulfil this function, i.e. functional equivalents; e.g. computer-viruses can be detected by different antivirus programs. Also, from a general cyber-security point of view it is reasonable to aim at the capability to think also of other software than just GEIGER. Nevertheless, it cannot be the aim of the GEE to teach about the whole range of Cybersecurity software, providing e.g. the advantages of different anti-virus-applications, but it is a learning goal to distinguish the different functions and to know that they can be integrated in different applications, and also e.g. in a more specific way. This allows in contrast to present the added values of GEIGER.

Further on as the GEIGER framework is designed for work environments that – though small – can include several persons the GEE has also to take account of how relevant cybersecurity issues can be communicated effectively within such a work environment of IT-lay-people. It is a specific challenge to train persons to become trainers of something that they are not an expert. However, the GEE has the objective that lay people cannot only use GEIGER in a benefitting way but that are also able to communicate and mentor it – also in the sense of reverse mentoring (see above) - within their environment so that e.g. colleagues will also apply it in a benefitting manner.

A further GEIGER specific challenge is the interaction between educational features and the GEIGER Toolbox. This interaction can manifest in both ways: the assessment of knowledge or learning of persons in a work environment can change the GEIGER Indicator score into the more positive. The GEIGER Toolbox can recommend users to improve individual knowledge by using bespoken educational features. For a more detailed discussion cf. the chapter: Toolbox Alignment.

6.4 Train-the-Trainer-Schemes

In order to increase impact, the GEE has to provide a set of training materials for heterogeneous 'multipliers', like e.g.:

- teachers/trainers giving courses on cybersecurity related topics at schools or further education institutions,
- IT experts consulting MSEs or
- other professionals (like accountants) that could include GEIGER in their service portfolio.

As this would be additional to their usual professional activities, i.e. either they are already IT-experts or they have no interests in becoming one, the learning goals for these target groups will have their main focus on training GEIGER specific competences and topics (GCG Pillar 2 and 3 – GEIGER Related and GEIGER Communication). Hence, they will function as multipliers for GEIGER in different ways.

Level 4 is thus conceived as a container for – among others – the set of competences necessary to train others to become (Certified) Security Defenders, i.e. within the general GEIGER environment. The amount of IT-knowledge in train-the-trainer schemes has to adapted to their specific knowledge background and learning interests.

For the Use Cases Train-the-Trainer-Schemes will be developed that are apart from languages specific to the background of the trainers (e.g. certified vocational trainers at BBB or particular IT-experts in Romania) and the objectives of the courses (e.g. competence goals or available course time) and their target groups (e.g. prior knowledge or age).

As part of the development of Education Provider Community (T3.3) and as part of a sustainable development the Train-the-Trainer-Schemes will have to be mainstreamed and particularly provided in English in order to have a basis for further exploitation in different educational organisations and for easy translation into further languages.

7 GEIGER Competence Grid (GCG)

For educational planning, a competence grid is useful as it integrates the complex learning goals into a workable scheme allowing e.g. to carve out different course curricula for different target groups. Among the main functions of the GEIGER Competence Grid is hence to provide the basis for the development of the different educational schemes, i.e. particularly the Use Case courses, and the learning materials for them as well as for potential target groups beyond.

The main structure was derived from a series of bi- and multilateral meetings and workshops with partners. In consequence, it particularly reflects the requirements set by the application and the practical usage of the whole GEIGER Framework, the heterogeneous target groups of the Use Cases, and topical distinctions resulting from the relevant fields of knowledge and learning theoretical assumptions – as well as standard approaches to competence model development (cf. Seeber/Retzmann/Remmele/Jongebloed 2010).

The GCG is a two-dimensional matrix representing levels, that try to represent potential learning progression, and pillars, i.e. topical content areas.

7.1 Levels – Progression

The levels are conceived as cumulative, i.e. the knowledge/abilities of Level 1 are part of Level 2 and so on. This partly implies prioritizing, i.e. Level 1 can be more important or more general than Level 2 and so on.

To define such competence levels, it is necessary to bring two – developmental – dimensions together:

- the capability of the learner, particularly what is their prior knowledge, e.g. for the GCG it is important that there IT-savvy and non-IT-savvy target groups as well as academic and non-academic ones with their specific learning interests and strategies, and
- the complexity or specificity of the tasks; e.g. can the task be handled with knowing the answer to a certain question, or by applying some more or less general rule of thumb or is it an even more difficult task that needs an analytic approach.

Apart from the entry Level 0, i.e. random everyday knowledge of CS, that we have to consider as rather low, we have thus figured out 4 levels for conceptualizing potential trainings:

- Level 1 – trained on this level a person would have basic Cyber-Security and Data Privacy Literacy that everyone – particularly in a business context – should have,
- Level 2 – a GEIGER Beginner would be a - non-ICT - person that could interact with the GEIGER Toolbox in a general manner,
- Level 3 – the GEIGER "Certified Security Defender" is somebody who is proficient with the GEIGER Toolbox – at least in one company, and
- Level 4 – GEIGER Multiplier – somebody that can exploit GEIGER, i.e. in concern of cyber security services or in training of lower levels.

7.2 Content Areas - Pillars

There is usually a mixture of systematic and pragmatic reasons to differentiate content areas in a competence model. For the GEIGER Education Ecosystem, it is reasonable to have the following distinctions:

- there is cyber security knowledge (in a very sense) that is independent of the GEIGER indicator but highly important – particularly in MSE contexts, and
- reflecting the ideas of the application of the 'Education Provider Community' and 'GEIGER Security Defenders' as kind of ambassadors (→ communication/dissemination/exploitation) it seems reasonable to have an area that deals with personal interaction around GEIGER.

Hence we have the three 'Pillars':

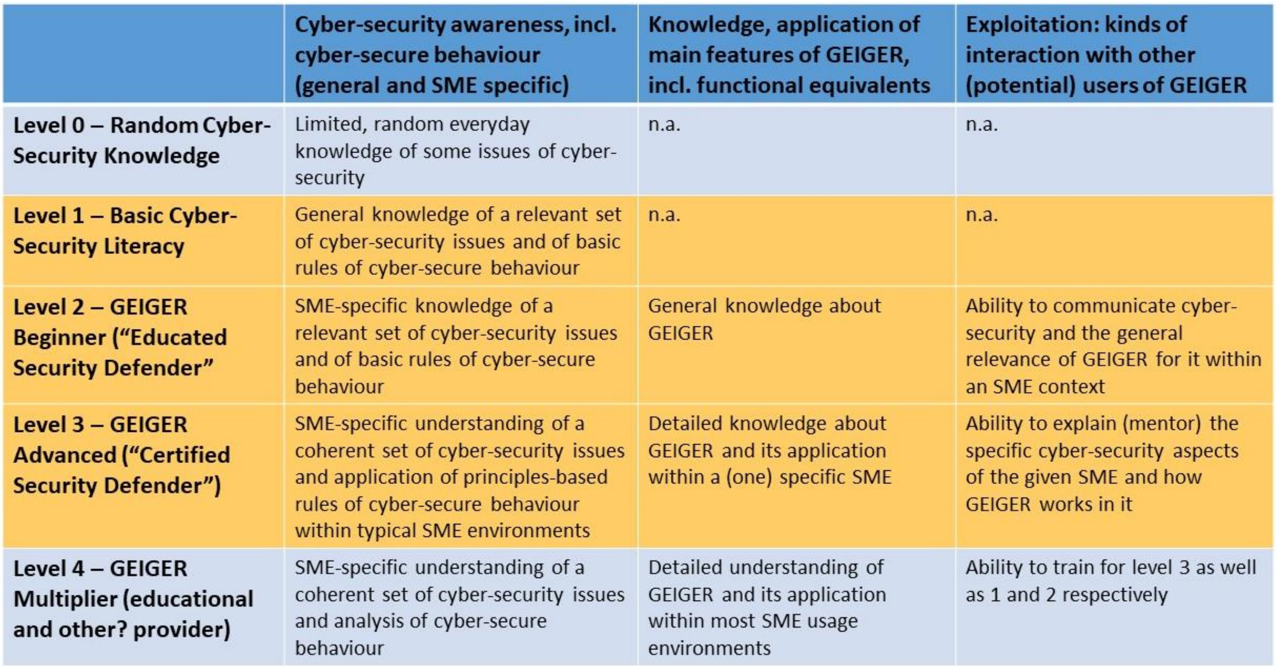
- cyber security and data privacy in general,
- basic practical and technical knowledge about the GEIGER Toolbox and functional equivalents. As for teaching about the working of the GEIGER Toolbox it is helpful to explain the functions, which implies also to take alternatives for partial functions into account, and
- communication, dissemination and exploitation or GEIGER – particularly in an MSE context.

There is some overlap between the pillars: e.g. knowledge of cyber security in general can include technical knowledge of functions GEIGER is dealing with or interactional knowledge about governance of access to critical data. However as long as the competences are on their adequate level, it can easily be dealt with such overlaps/ambiguities in the actual learning materials.

7.3 Knowledge - Ability

Competence is an umbrella term that relates to different kinds of performances. In our context we distinguish between knowledge and ability:

- knowledge (about/of - know what) is something you write down or provides you with an answer to a question (knowledge can be faked by learning by heart). Its descriptions in the grid starts with an object (e.g. 'general and MSE-specific CS threats').
- ability (to - know how) is something that allows you to do something (ability cannot be faked – you hit the nail, or you don't). Its descriptions in the grid starts with an infinitive (e.g. 'install and customize security software').



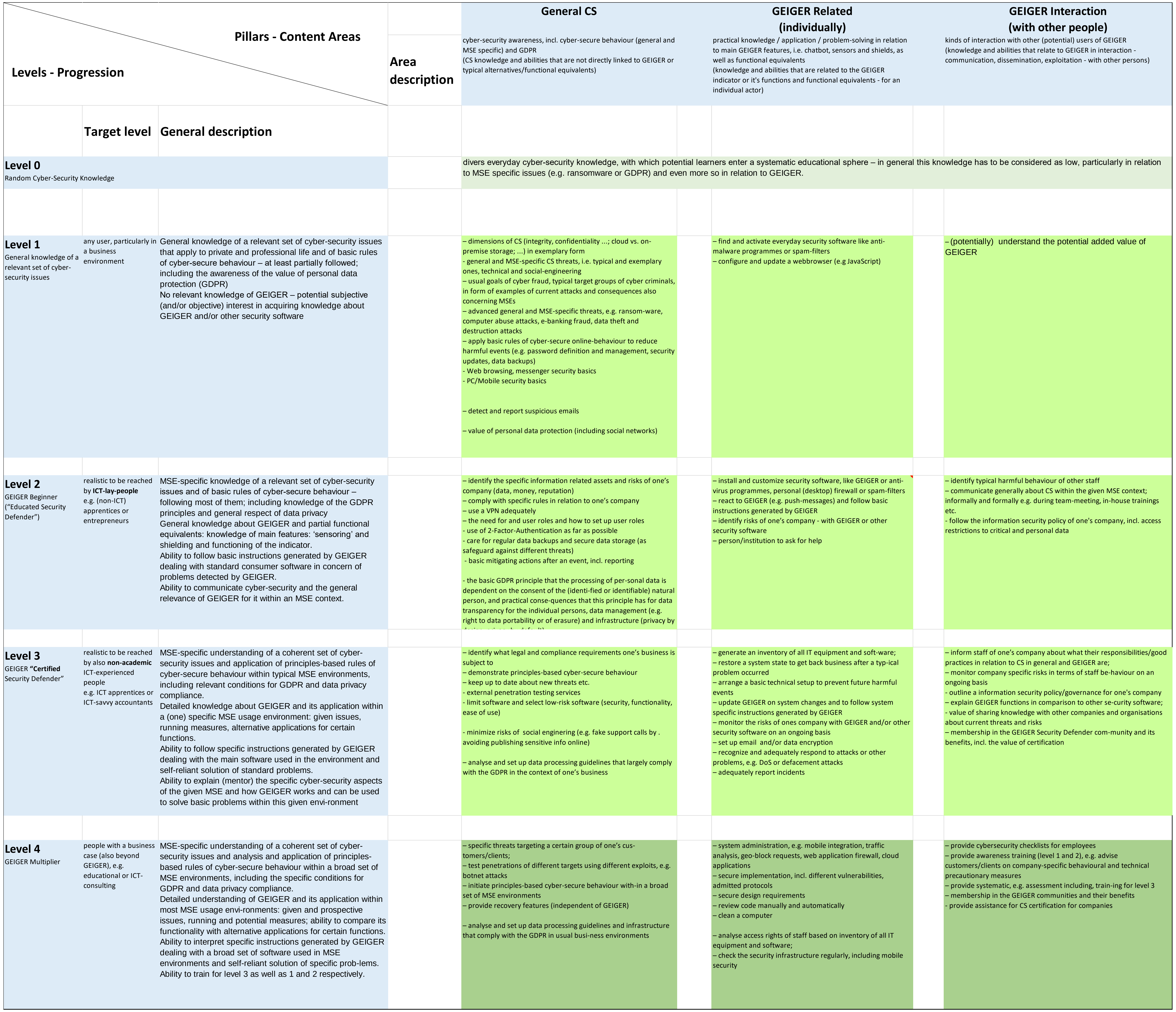
	Cyber-security awareness, incl. cyber-secure behaviour (general and SME specific)	Knowledge, application of main features of GEIGER, incl. functional equivalents	Exploitation: kinds of interaction with other (potential) users of GEIGER
Level 0 – Random Cyber-Security Knowledge	Limited, random everyday knowledge of some issues of cyber-security	n.a.	n.a.
Level 1 – Basic Cyber-Security Literacy	General knowledge of a relevant set of cyber-security issues and of basic rules of cyber-secure behaviour	n.a.	n.a.
Level 2 – GEIGER Beginner ("Educated Security Defender"	SME-specific knowledge of a relevant set of cyber-security issues and of basic rules of cyber-secure behaviour	General knowledge about GEIGER	Ability to communicate cyber-security and the general relevance of GEIGER for it within an SME context
Level 3 – GEIGER Advanced ("Certified Security Defender")	SME-specific understanding of a coherent set of cyber-security issues and application of principles-based rules of cyber-secure behaviour within typical SME environments	Detailed knowledge about GEIGER and its application within a (one) specific SME	Ability to explain (mentor) the specific cyber-security aspects of the given SME and how GEIGER works in it
Level 4 – GEIGER Multiplier (educational and other? provider)	SME-specific understanding of a coherent set of cyber-security issues and analysis of cyber-secure behaviour	Detailed understanding of GEIGER and its application within most SME usage environments	Ability to train for level 3 as well as 1 and 2 respectively

Figure 7 Competence Grid abbreviated

In M4, as part of the development of the GCG, we asked partners to give feedback to a draft version, e.g. concerning their understanding of the importance and complexity of specific competences and of the relevance of given examples. We got valuable feedback from partners, mainly concerning further relevant issues or alternative mapping of competences to levels, that has been used to refine the GCG.

The GCG is will function as tool for guiding the further educational planning, e.g. to align the production of education materials and features with the definition of target groups in the Use Cases. Nevertheless, it remains to be work in progress, as it needs to be further differentiated to fit better to certain target groups, to set the most effective scope of competences for the 'Certified Security Defenders' and in the next months of the project to develop a measuring system for CS-competence and thus to guide the creation of educational materials for the Use Cases and the Toolbox.

The specific content in the first version of the GCG is based on CERT recommendations for protections and up-to-date collections on cyber threats by NCSC, CERT-RO and the Dutch Digital Trust Center.



Levels - Progression		Pillars - Content Areas	Area description	General CS	GEIGER Related (individually)	GEIGER Interaction (with other people)
				cyber-security awareness, incl. cyber-secure behaviour (general and MSE specific) and GDPR (CS knowledge and abilities that are not directly linked to GEIGER or typical alternatives/functional equivalents)	practical knowledge / application / problem-solving in relation to main GEIGER features, i.e. chatbot, sensors and shields, as well as functional equivalents (knowledge and abilities that are related to the GEIGER indicator or it's functions and functional equivalents - for an individual actor)	kinds of interaction with other (potential) users of GEIGER (knowledge and abilities that relate to GEIGER in interaction - communication, dissemination, exploitation - with other persons)
	Target level	General description				
Level 0 Random Cyber-Security Knowledge				divers everyday cyber-security knowledge, with which potential learners enter a systematic educational sphere – in general this knowledge has to be considered as low, particularly in relation to MSE specific issues (e.g. ransomware or GDPR) and even more so in relation to GEIGER.		
Level 1 General knowledge of a relevant set of cyber-security issues	any user, particularly in a business environment	General knowledge of a relevant set of cyber-security issues that apply to private and professional life and of basic rules of cyber-secure behaviour – at least partially followed; including the awareness of the value of personal data protection (GDPR) No relevant knowledge of GEIGER – potential subjective (and/or objective) interest in acquiring knowledge about GEIGER and/or other security software		– dimensions of CS (integrity, confidentiality ...; cloud vs. on-premise storage; ...) in exemplary form - general and MSE-specific CS threats, i.e. typical and exemplary ones, technical and social-engineering – usual goals of cyber fraud, typical target groups of cyber criminals, in form of examples of current attacks and consequences also concerning MSEs – advanced general and MSE-specific threats, e.g. ransom-ware, computer abuse attacks, e-banking fraud, data theft and destruction attacks – apply basic rules of cyber-secure online-behaviour to reduce harmful events (e.g. password definition and management, security updates, data backups) - Web browsing, messenger security basics - PC/Mobile security basics – detect and report suspicious emails – value of personal data protection (including social networks)	– find and activate everyday security software like anti-malware programmes or spam-filters – configure and update a webbrowser (e.g JavaScript)	– (potentially) understand the potential added value of GEIGER
Level 2 GEIGER Beginner ("Educated Security Defender")	realistic to be reached by **ICT-lay-people** e.g. (non-ICT) apprentices or entrepreneurs	MSE-specific knowledge of a relevant set of cyber-security issues and of basic rules of cyber-secure behaviour – following most of them; including knowledge of the GDPR principles and general respect of data privacy General knowledge about GEIGER and partial functional equivalents: knowledge of main features: 'sensoring' and shielding and functioning of the indicator. Ability to follow basic instructions generated by GEIGER dealing with standard consumer software in concern of problems detected by GEIGER. Ability to communicate cyber-security and the general relevance of GEIGER for it within an MSE context.		– identify the specific information related assets and risks of one's company (data, money, reputation) – comply with specific rules in relation to one's company – use a VPN adequately – the need for and user roles and how to set up user roles - use of 2-Factor-Authentication as far as possible - care for regular data backups and secure data storage (as safeguard against different threats) - basic mitigating actions after an event, incl. reporting - the basic GDPR principle that the processing of per-sonal data is dependent on the consent of the (identi-fied or identifiable) natural person, and practical conse-quences that this principle has for data transparency for the individual persons, data management (e.g. right to data portability or of erasure) and infrastructure (privacy by	– install and customize security software, like GEIGER or anti-virus programmes, personal (desktop) firewall or spam-filters – react to GEIGER (e.g. push-messages) and follow basic instructions generated by GEIGER – identify risks of one's company - with GEIGER or other security software – person/institution to ask for help	– identify typical harmful behaviour of other staff – communicate generally about CS within the given MSE context; informally and formally e.g. during team-meeting, in-house trainings etc. - follow the information security policy of one's company, incl. access restrictions to critical and personal data
Level 3 GEIGER **"Certified** Security Defender"	realistic to be reached by also **non-academic** ICT-experienced people e.g. ICT apprentices or ICT-savvy accountants	MSE-specific understanding of a coherent set of cyber-security issues and application of principles-based rules of cyber-secure behaviour within typical MSE environments, including relevant conditions for GDPR and data privacy compliance. Detailed knowledge about GEIGER and its application within a (one) specific MSE usage environment: given issues, running measures, alternative applications for certain functions. Ability to follow specific instructions generated by GEIGER dealing with the main software used in the environment and self-reliant solution of standard problems. Ability to explain (mentor) the specific cyber-security aspects of the given MSE and how GEIGER works and can be used to solve basic problems within this given envi-ronment		– identify what legal and compliance requirements one's business is subject to – demonstrate principles-based cyber-secure behaviour – keep up to date about new threats etc. - external penetration testing services - limit software and select low-risk software (security, functionality, ease of use) - minimize risks of social enginering (e.g. fake support calls by . avoiding publishing sensitive info online) – analyse and set up data processing guidelines that largely comply with the GDPR in the context of one's business	– generate an inventory of all IT equipment and soft-ware; – restore a system state to get back business after a typ-ical problem occurred – arrange a basic technical setup to prevent future harmful events – update GEIGER on system changes and to follow system specific instructions generated by GEIGER – monitor the risks of ones company with GEIGER and/or other security software on an ongoing basis – set up email and/or data encryption – recognize and adequately respond to attacks or other problems, e.g. DoS or defacement attacks – adequately report incidents	– inform staff of one's company about what their responsibilities/good practices in relation to CS in general and GEIGER are; – monitor company specific risks in terms of staff be-haviour on an ongoing basis - outline a information security policy/governance for one's company – explain GEIGER functions in comparison to other se-curity software; - value of sharing knowledge with other companies and organisations about current threats and risks – membership in the GEIGER Security Defender com-munity and its benefits, incl. the value of certification
Level 4 GEIGER Multiplier	people with a business case (also beyond GEIGER), e.g. educational or ICT-consulting	MSE-specific understanding of a coherent set of cyber-security issues and analysis and application of principles-based rules of cyber-secure behaviour within a broad set of MSE environments, including the specific conditions for GDPR and data privacy compliance. Detailed understanding of GEIGER and its application within most MSE usage envi-ronments: given and prospective issues, running and potential measures; ability to compare its functionality with alternative applications for certain functions. Ability to interpret specific instructions generated by GEIGER dealing with a broad set of software used in MSE environments and self-reliant solution of specific prob-lems. Ability to train for level 3 as well as 1 and 2 respectively.		– specific threats targeting a certain group of one's cus-tomers/clients; – test penetrations of different targets using different exploits, e.g. botnet attacks – initiate principles-based cyber-secure behaviour with-in a broad set of MSE environments – provide recovery features (independent of GEIGER) – analyse and set up data processing guidelines and infrastructure that comply with the GDPR in usual busi-ness environments	– system administration, e.g. mobile integration, traffic analysis, geo-block requests, web application firewall, cloud applications – secure implementation, incl. different vulnerabilities, admitted protocols – secure design requirements – review code manually and automatically – clean a computer – analyse access rights of staff based on inventory of all IT equipment and software; – check the security infrastructure regularly, including mobile security	– provide cybersecurity checklists for employees – provide awareness training (level 1 and 2), e.g. advise customers/clients on company-specific behavioural and technical precautionary measures – provide systematic, e.g. assessment including, train-ing for level 3 – membership in the GEIGER communities and their benefits - provide assistance for CS certification for companies

Figure 8 GEIGER Competence Grid

7.4 Certified Security Defenders Education

The Certified Security Defenders Education, which is a defining core of the GEE, will consist of the levels 1, 2 and 3 with a focus on the interaction pillar, as CSDs are supposed to propagate GEIGER in their environment. Educational providers will be able to adapt their course curricula to their specific target groups, e.g. in concern of entry level or company requirements, or to their specific national, e.g. in concern of dominant threats.

It is planned to include an experiential part of GEIGER in a real-world environment (or a short report of such an experience) into the definition of the competence assessment scheme for the certification.

8 Educational Features/Materials to be Adapted to the Competence Grid

The educational features and materials that are generated during the project lifetime from the consortium have to fit into the two scenarios:

- trainer-based courses, i.e. particularly the Use Cases, with learners who are probably not involved in a company that has GEIGER Toolbox installed yet. They thus need adaption to their specific conditions a demo version of the GEIGER Toolbox.
- self-regulated learning ‘around’ and interacting with the GEIGER Toolbox for learners who are already participating in a company that has it installed.

Some of the features described in the following are conceived to be used in courses, e.g. because they have the form of a competitive game, others are online features that can easily be aligned with GEIGER Toolbox, others are in state of planning that might allow the development of versions for both scenarios.

To integrate these features in a systematic way into the GEE, including interoperability with the GEIGER Toolbox/Indicator, it is necessary to devise a measuring system for CS-competence of persons in MSEs, including their competence-development. Scores in concern of certain topics and the respective competence development have to be calculated that feed into the GEIGER Indicator Score. This system will be based on the GEIGER Competence Grid, prioritized topics/threats, the degree of technicality and complexity of such issues.

8.1 ATOS: Toolbox Demo Version

Security Defender Educational Level: 2 and 3

ATOS and other partners contributing to the GEIGER Toolbox will create a GEIGER Demo that is optimized to work as educational object, so that learners can actively experience what the GEIGER Toolbox does and how it works.

Train the Trainer Materials have to be provided along with the Toolbox Demo Version.

8.2 Kaspersky Cybersafety Management Games (CSMG)

Security Defender Educational Level: 1

CSMG is an online learning game that focuses on behaviour and attitude of staff towards cybersecurity issues. It can be played by staff of all working fields and hierarchies and no previous knowledge is required.

Small groups of 4-5 players compete either in an online or offline setting to win the game by earning points. In the current state, the game takes place in a synchronous setting, where a moderator leads the game and structures the playing process. The groups operate within an online simulation of a typical workplace situation, where several working fields are shown. Players have to go through each workplace situation that may contain hidden cybersecurity threats. By making the right choices in terms of cybersecure behaviour, they can earn points.

Future adaptions are planned on the content itself concerning up-to-date threats. Training materials will be provided for independent trainers.

8.3 Kaspersky Interactive Protection Simulation (KIPS)

Security Defender Educational Level: 3 – 4

KIPS is an online learning game that focuses on cybersecurity implementation strategies of MSE’s.

In the current state, the target group of the game is mainly working in the field of IT. Previous knowledge in the IT-field is necessary. The game is played in a synchronous mode either online or offline, where a moderator leads through the game and structures the playing process.

The game is set online in a working environment where players take the role of staff responsible for the cyber security of a fictional enterprise. They have to consider time and financial budget to make sustainable choices on the cyber security implementation. Small groups of staff compete against each other by gaining points for making the right decisions, respectively loosing points by making harmful choices.

Adaptions are planned for a target group with less or no previous knowledge. Training material will be provided for independent trainers.

8.4 Montimage: Advanced Cyber Range Challenges

Security Defender Educational Level: 4

The Cyber Range Challenges are created to raise awareness on current cyber-threats and their impact on organisations. Based on practical examples, users can understand the necessity of a serious monitoring of the enterprise network and have an insight on network intrusion detection and prevention systems (N-IDPS)

The Cyber Range Challenges in their current state consist of a theoretical and a practical training.

The theoretical training is in a synchronous format and requires a trainer who conveys specific topics, e.g. network monitoring or concepts of network intrusion detection and prevention systems. In the practical training, users explore the Montimage Cyber Range Platform by generating different kinds of attacks and detecting these attacks, as well as triggering countermeasures.

8.5 Montimage: Beginner Cyber Range Challenges

Security Defender Educational Level: 1

An app will be created that covers the topic of phishing mails. Users can either download the app or register on the website. Depending on their preferences, they regularly receive E-mails in the app, e.g. once a week. Users then have to guess, whether the e-mails they just received are valid mails or phishing mails. They furthermore have to give reasons for their choice in form of a multiple-choice input.

Within the scope of the competence grid, the topic of phishing mails can be located in Level 1. Since the present learning scenarios of the Use Cases comprise mostly compact courses, learners will once receive a collective amount of 5 – 10 phishing mail questions on request.

8.6 FHNW Experiential Cybersecurity Escape Room

Security Defender Educational Level 1

This educational escape room game can be played either in a physical (synchronous) or virtual (browser-based, asynchronous) format. In both versions, it is a story-based game covering the topics of physical security, password hygiene, code security, information disposal, securing sensitive digital data and public oversharing/identity theft. The learner, who is either physically or virtually located in an office room, has to follow different hints and solve several puzzles during the game. Narration is intensified by an introduction video. In the offline version, a trainer is needed to give playing instructions and support, as well as leading a discussion after the game. The game can be played in single mode or include up to 3 players per session.

Since players can play the game with low or advanced knowledge on cyber-secure behaviour, the game can be applied on different levels within the GEE, starting at Level 1.

Whereas the game components in physical format are already available in a final version, further adaptions on the virtual and scalable version of the escape room are planned.

8.7 FHNW Data Privacy Impact - Assessment Tool

Security Defender Educational Level: 2

The Data Privacy Impact Assessment Tool was developed with the goal to support SME&MEs to conduct Privacy Assessments according to Art. 35 GDPR based on the existing tool and materials provided by the French Data Protection Authority CNIL. In the current version, the tool is planned in an asynchronous offline format, e.g. an Excel Sheet, and can be experienced either in single or collaborative mode. The goal of the interaction with the tool is to assess the privacy impact of a new data handling technology within the SME&ME.

According to GDPR (Article 35 (1)), any new data processing technology applied within an enterprise needs to be evaluated through a DPIA (Data Protection Impact Assessment) process. The DPIA-tool helps in conducting this assessment.

Users should have a previous basic understanding of GDPR and data privacy principles. The tool can be applied in Level 3 of the GCG with regard to the competence to “analyse and set up data processing guidelines that largely comply with the GDPR in the context of one’s business”.

It is foreseen to adapt the template to needs of SME&MEs by simplifying wherever possible and by using a language understandable for non-tech people.

8.8 FHNW „The value of the data“ GDPR Quiz

Security Defender Educational Level: 2

This GDPR training module is based on a storytelling and gamification approach adapted for SME&MEs in an online format of a story-based quiz on GDPR-related topics with scoring that can be compared among players in the end.

In the original setup, the quiz can be played as multiplayer quiz synchronously to compare the results of players and get “a winner” at the end. A new version has been adapted to be applied as single player quiz. Topics of the current prototype cover the basic GDPR concept (the terms “personal data, sensitive personal data”) and applicability of GDPR. Basic GDPR principles of personal data and consent should be familiar to the learners in advance. The quiz helps to improve the existing knowledge and understanding and can therefore be located in the scope of Level 2 of the GCG.

The game can be played either in asynchronous format or as a synchronous format supported by trainers that bring in their background knowledge in GDPR. Further individual adaptions of country-specific contents with regard the specific Use Cases, as well as to further relevant aspects on GDPR are planned.

8.9 FHNW „Am I GDPR compliant?” GDPR Self-assessment

Security Defender Educational Level: 3

The present self-learning module is based on a GDPR self-assessment tool for Higher Education Institutions to raise awareness and to assess current state of GRPR. The format is an excel-based asynchronous offline application that covers flowchart- and questionnaire-based self-assessment of existing GDPR regulations and related processes. It can either be played in a single mode or applied within discussion groups.

Learners are required to have medium or advanced GDPR knowledge. This tool can therefore be applied in Level 3 of the GCG. Further content adaptions for SME&MEs need to be undertaken as well as a transformation to an ‘easy to use’ file type (e.g. web-based, HTML questionnaire).

8.10 KPMG: GDPR

KPMG offers curricular knowledge and guidance on the subject of GDPR in order to develop respective learning modules. KPMG has already developed and is further updating a training path on basic GDPR aspects in the form of presentation slides. The topics covered are Personal Identifiable Information, Data Controller, Data Holders and Data Processors. The information presented in the slides can be used as guidelines for creating specific learning materials.

8.11 FHNW: CYSEC Adaption

Security Defender Educational Level: 1 and 2

CYSEC is a modularized learning framework for cybersecurity of FHNW. It is designed for desktop use, with a coarse-grained learning path not specified for MSE environments.

FHNW together with PHF will adapt CYSEC to the GEIGER Toolbox for mobile learning, with fine-grained learning paths (micro-learning) and prioritizing MSE specific issues.

9 Training Schedule

The following table shows the different timelines of the development processes that are integral part of the GEE. These parts are:

- GEIGER Indicator as such, because it is of course an essential learning object for the GEE,
- Educational contributions of the partners, because they can only be applied in the Use Cases in one or the other way when they are ready and relate to the specific learning targets and target groups of the Use Cases, and
- Course scheduling of the Use Cases – the different Use Cases have different schedules when e.g. courses have to be promoted and when they can be conducted.

As the exact timing of the different processes is partially open for changes and partially not definable yet the training schedule is work in progress. Its function, and its updating, is just to harmonize the developments and to identify potential risks and mismatches.

Training Schedule

	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	Components MVP						Integration + Intermediate Training Report						Framework MVP						Release + Final Training Report					
	Dez 20	Jan 21	Feb 21	Mrz 21	Apr 21	Mai 21	Jun 21	Jul 21	Aug 21	Sep 21	Okt 21	Nov 21	Dez 21	Jan 22	Feb 22	Mrz 22	Apr 22	Mai 22	Jun 22	Jul 22	Aug 22	Sep 22	Okt 22	Nov 22
Development of the Tool Box																								
Sandbox						?																		
Prototype												?												
Minimum Viable Product																		?						
Swiss Use Case																								
concept for train the trainer																								
Educational Materials for level 1				X																				
Educational Materials for level 2						X																		
Educational Materials for level 3										X														
Content for level 4 (raw)						X																		
Certification of trainer											X													
Methodically refined content level 4																			X					
course(s) outline/registration																								
Level 1a with test-classes (CF)						X	X																	
Level 1b with test-classes (IN)									X	X														
Level 1a open to all the BBB-classes											X	X	X	X	X	X	X	X	X	X	X	X	X	
Level 1b open to all the BBB-classes											X	X	X	X	X	X	X	X	X	X	X	X	X	
Level 1a with all the first-year apprentices									X															
Level 2 with test-candidates											X	X	X	X										
Level 3 with test-candidates															X	X	X	X	X					
Level 2 with additional volunteers															X	X	X	X	X					
Level 3 with additional volunteers																			X	X	X	X	X	
mse																								
mse CF / IT						X																		
mse skv											X													
other mse															X									
Dutch Use Case																								
Educational Materials for level 1						X																		
Educational Materials for level 2								X																
Educational Materials for level 3										X														
Educational Materials for level 4																				X				
train the trainer										X														
Certification of trainer											X													
course(s) outline/registration																								
Level 1 - Basic Cyber-Security Literacy											X	X	X				X	X	X	X	X	X	X	
Level 2 - Geiger Educated Security Defender - Pilot																	X							
Level 2 - Geiger Educated Security Defender																		X	X	X	X	X	X	
Level 3 - Geiger Certified Security Defender - Pilot																			X					
Level 3 - Geiger Certified Security Defender																				X	X	X	X	
Level 4 - Geiger Multiplier																							X	

Romanian Use Case																								
course outline/registration						X	X																	
train the trainer								X			X													
Adaption of materials (service field MSEs)									X															
Adaption of materials (IT field MSEs)													X											
course with MSEs (service field)																X								
course with MSEs (IT field)														X										
Materials from Consortium																								
KPMG																								
GDPR - curriculum guidance																								
GDPR - in indicator																								
KSP																								
CSMG - Zones for MSE definition		X																						
CSMG - End of game implementation (English version)							X																	
CSMG - Master-Train-The-Trainer (M-T-T-T)							X																	
CSMG - Swiss Use Case - Translation and Local Adaptation								X																
CSMG -Romanian Use Case - Translation and Local Adaptation									X															
CSMG - Dutch Use Case - Translation and Local Adaptation										X														
CSMG - Swiss Use Case - Validation											X													
CSMG -Romanian Use Case - Validation												X												
CSMG - Dutch Use Case - Validation													X											
KIPS - Scenario for MSE definition		X																						
KIPS - End of game implementation (English version)										X														
KIPS - Train-The-Trainer (T-T-T)										X														
KIPS - Swiss Use Case - Translation and Local Adaptation											X													
KIPS -Romanian Use Case - Translation and Local Adaptation												X												
KIPS - Dutch Use Case - Translation and Local Adaptation													X											
KIPS - Swiss Use Case - Validation														X										
KIPS -Romanian Use Case - Validation															X									
KIPS - Dutch Use Case - Validation																X								
KIPS - Master-Train-The-Trainer (M-T-T-T)																	X							
MI																								
Phishingmail in app/web 1 (prototype)						x																		
Phishingmail in app/web 2 (whole set of mails)																		x						
(Further topics)																								
Cyberrange (old) ready to use	?																							
train the trainer manual			?																					
FHNW																								
Data Privacy Impact - Assessment Tool			x									x												
“Am I GDPR compliant?” GDPR self-assessment												x												
Experiential Cybersecurity Escape Room			x																					
„The value of the data“ – A GDPR Quiz												x												
Materials in cooperation PHF																								
Materials for essential not yet represented competences??																								

Figure 9 Training Schedule. “(Further topics)” is after M30 during exploitation.

10 Education Provider Community (T3.3)

The Education Provider Community describes a long-term organisational network of educational providers of GEIGER training with the vision of keeping the GEE sustainable.

The community will consist of relevant members such as vocational schools (such as BBB in the Swiss pilot use case), associations offering training to service providers for SMEs (such as SRA in the Dutch pilot use case), and networks and clusters offering training to entrepreneurs and small businesses (such as ClujIT in the Romanian pilot use case), including training providers for adult education.

10.1 Core Tasks

The Education Provider Community constitutes one of the building blocks of the GEIGER Education Ecosystem. From a sustainability point of view, establishing and maintaining a community of education providers is essential, especially to keep the learning content on cybersecurity for MSEs up-to-date. Major tasks of the community lie in the coordination of the GEE after the project lifetime.

Coordination tasks include:

a) Coordinating existing educational networks and third-party providers

The coordination of the community members constitutes the key coordination task. This includes e.g. recruiting and welcoming new members, organisation of regular and exceptional community 'events', as well as general dissemination activities.

Further on, the Education Provider Community shall be closely linked to the Certified Security Defenders Community and therefore organise exchange channels or respective events. Cooperation with other pertinent projects, particularly within the H2020 program, are to be considered in terms of dissemination and possible synergy effects.

b) Providing of trainer courses and train-the-trainer courses

The first conceptualizations of trainer courses are established within the GEIGER project lifetime. In this manner, a first cohort of trainers is educated for the different use case scenarios. Trainers within the consortium will likewise participate in train-the-trainer activities, which enables them to teach prospective trainers. Training materials will be provided on a long-term perspective, as well as self-learning materials for Train-the-Trainer courses.

c) Providing of access to training materials and regular MSE-specific updating of materials and training contents

Access to general training materials will be ensured through a centralized platform that will be either part of, or directly linked to the Education Provider Community communication platform. In order to ensure topicality, regular updates of learning materials may include content or technical updates, as well as substitution of materials where necessary. Keeping training contents up-to-date also implies that an update of the CGC and the training curricula and syllabi must be undertaken on a regular basis.

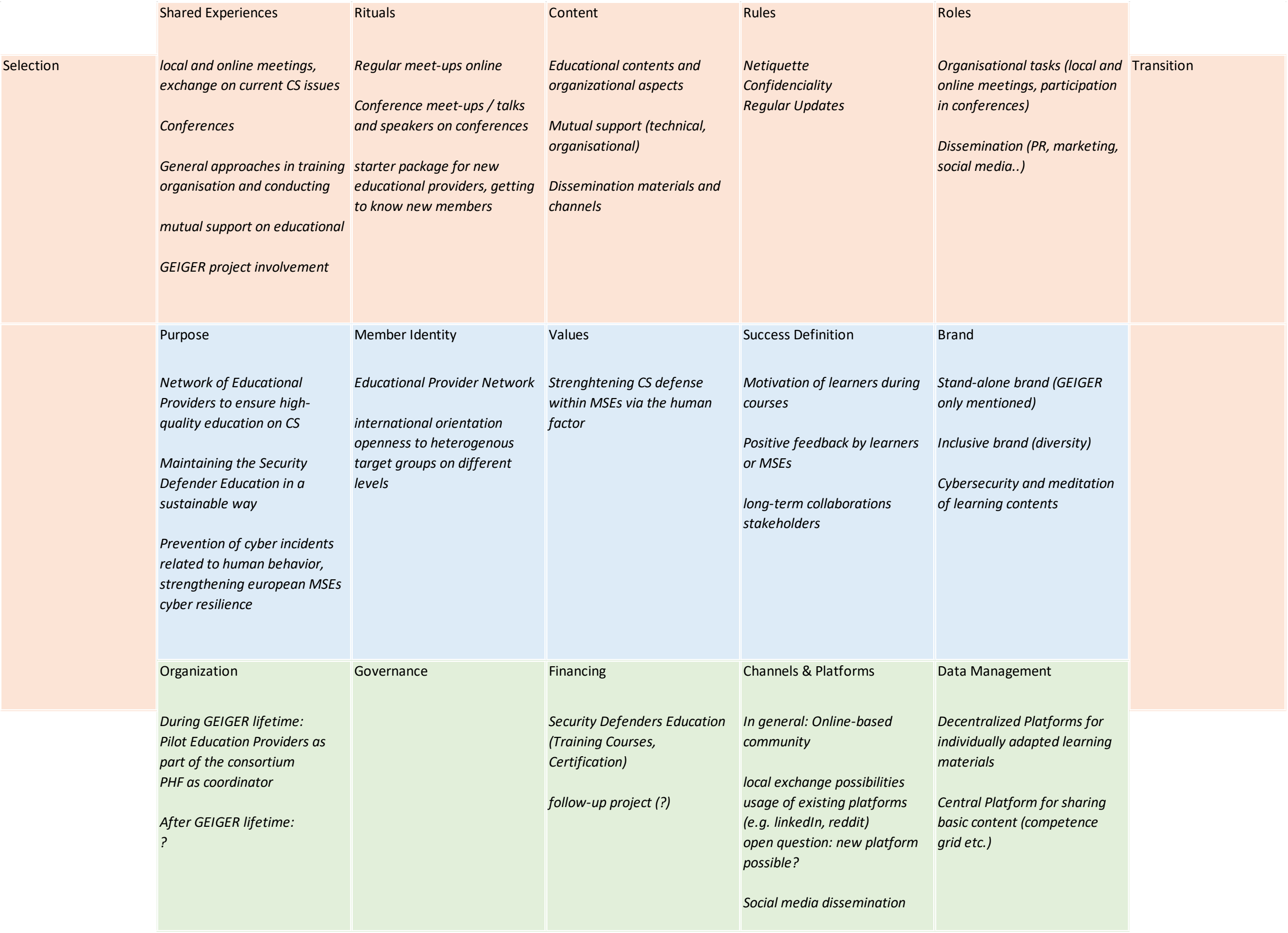
For this purpose, the community will involve members with expertise in cyber security and shall be closely linked with CERT organisations who can offer their expertise on current cyber threats.

d) Maintaining and coordinating the Security Defenders Certification (See also Chapter 13)

During the GEIGER project lifetime, partners involved in WP3 will act as certification body and provide assessments. After the GEIGER project lifetime, the organisation of the certification organisations will be one of the tasks to be adressed within the sustainable body of GEIGER. This may happen by either a) cooperating with a certification organisation that certifies individual learners or b) certifying the Education Providers, e.g. by offering a certification aligned with the community. In both cases, communication with potential external partners or else internal certification procedures will have to be managed within the Education Provider Community.

10.2 Community Characteristics

As an initial approach to further defining the overall tasks and goals of the Education Provider Community, a usual community canvas is used. First ideas on the overarching fields on community identity, experience and structure are shown in the community canvas:



	Shared Experiences	Rituals	Content	Rules	Roles	
Selection	*local and online meetings, exchange on current CS issues* *Conferences* *General approaches in training organisation and conducting* *mutual support on educational* *GEIGER project involvement*	*Regular meet-ups online* *Conference meet-ups / talks and speakers on conferences* *starter package for new educational providers, getting to know new members*	*Educational contents and organizational aspects* *Mutual support (technical, organisational)* *Dissemination materials and channels*	*Netiquette* *Confidenciality* *Regular Updates*	*Organisational tasks (local and online meetings, participation in conferences)* *Dissemination (PR, marketing, social media..)*	Transition
	Purpose	Member Identity	Values	Success Definition	Brand	
	Network of Educational Providers to ensure high-quality education on CS *Maintaining the Security Defender Education in a sustainable way* *Prevention of cyber incidents related to human behavior, strengthening european MSEs cyber resilience*	*Educational Provider Network* *international orientation* *openness to heterogenous target groups on different levels*	*Strenghtening CS defense within MSEs via the human factor*	*Motivation of learners during courses* *Positive feedback by learners or MSEs* *long-term collaborations stakeholders*	*Stand-alone brand (GEIGER only mentioned)* *Inclusive brand (diversity)* *Cybersecurity and meditation of learning contents*	
	Organization	Governance	Financing	Channels & Platforms	Data Management	
	During GEIGER lifetime: *Pilot Education Providers as part of the consortium* *PHF as coordinator* *After GEIGER lifetime:* *?*		*Security Defenders Education (Training Courses, Certification)* *follow-up project (?)*	*In general: Online-based community* *local exchange possibilities* *usage of existing platforms (e.g. linkedIn, reddit)* *open question: new platform possible?* *Social media dissemination*	*Decentralized Platforms for individually adapted learning materials* *Central Platform for sharing basic content (competence grid etc.)*	

Figure 10 GEIGER Community Canvas

10.3 Community Building

Potential members of the Education Provider Community include:

- Educational institutions such as vocational schools, universities or other institutions
- MSE associations or similar, that (are willing to) offer training
- IT-companies as well as IT-experts willing to offer trainings and other services in relation to GEIGER
- other commercial partners that offer services to MSEs
- organisations that care for cybersecurity and data privacy, like CERTs and pertinent interest groups.

As an approach to maximize the number of potential Education Providers, the community shall be organized in an open way, which sets a low threshold for institutions to become a member and offer GEIGER related trainings. GEIGER needs to disseminate the specific added value of the Toolbox in combination with the GEE to respective audiences, i.e. for some audiences the specific improvement of cybersecurity and for other audiences the potential of improving one’s service offer will be the ‘selling point’.

The core Educational Providers to start with are within the nearer scope of the GEIGER consortium. In the current phase of the GEIGER project consortium partners are adding their ideas on further potential Education Providers to a list of potential third parties that will have to be contacted in a later phase of the task.

In the current stage, existing communities of a similar scope and within the subject area of cybersecurity are to be examined, so that the GEIGER Education Provider Community can be oriented at successful community models and their structures. Further evaluation on possible synergy effects and collaborations with communities of this kind are to be undertaken.

From a dissemination perspective, there is a need for a branding of the community that will attract members and communicate the core idea of the community. For this reason, WP3 will closely cooperate with WP5 to set up target-group oriented branding and reach out in relevant communication channels. Awareness-raising and networking will be organised through participation in events and targeted publications, coordinated with consortium members with connections to education providers. At the outset of the community, consortium members constitute the core members of the community. In the next step, an outreach starting from the consortium will be undertaken in an approach to gradually widen the circle of community members in the first phase.

Dissemination activities and respective materials will be set up in a sustainable way, so that they can be used and adapted also on a long-term perspective.

10.4 Link to the GEIGER Security Defenders Community

T3.4. – Security Defender Community is still to commence in Project Month 12. Nevertheless, first conceptualisations on this community have been developed, since there are a lot of interdependencies and common interests between the Security Defender Community, typically consisting of natural persons, and the Education Provider Community, typically consisting of organisations and professionals.

In a first approach, the Security Defender Community is likewise defined in an analogue way to the Education Provider Community as a mostly open community, that accepts members of all learning levels and backgrounds. Certified Security Defenders are becoming part of the community, likewise learners that have achieved a lower level within the GCG. The community is moreover open to potential members that might not have completed a GEIGER related training but who are interested in the Security Defender Community, coming from diverse backgrounds in cybersecurity.

From an organisational point of view, it is a useful approach to create synergies between the Education Provider Community as well as the Security Defender Community. Therefore, possible organisational aspects, e.g. the community platform, shall be merged so that it can host both target groups and furthermore exchange possibilities are created. Therefore, this aspect demands closer examination in the next steps of conceptualising both communities. A closer examination of further possible linkings between both community groups to the 'GEIGER Community' will be undertaken in a further approach.

11 Upcoming

11.1 Issue: Demo Toolbox

The analysis of these different conditions and processes forming the GEE showed two fields that need imminent further planning as they were not clearly anticipated and differentiated in the outline of the project. The outline of these fields follows the distinction between asynchronous, single or self-directed learning and synchronous trainer based learning in groups.

It has shown as favourable that the 'Toolbox' will be represented in the Use Case courses, i.e. from an educational perspective trainers and/or the learners should be able to see/do something in the Toolbox. Particularly apprentices training is based on action-oriented education. Hence it needs to be as much hands-on or activating as possible. This could be met e.g. by providing a laptop and a mobile with a demo version of the Toolbox.

From a didactical point of view this Demo should provide:

- high usability and interaction grade,
- an overview of (essential) tools and functions,

- the possibility to fulfil some tasks
- a choice (for trainers) at start between an implementation (potentially to add own company data – or predefined choices in regard of company profile) and with a 'running system' (e.g. with exemplary company data, potentially different ones),
- a set of different tasks for learners, from which trainers can choose,
- the possibility of learners to switch to an explanation/guide, and
- minimised technical hurdles (preparation time, trainer guidelines, …).

11.2 Issue: Self-Regulated Learning Features

The number of asynchronous educational features that are interacting with the Toolbox – as or both:

- training sequences that can be recommended by the Toolbox to improve (human based) security, and
- such that can (more or less) automatically improve the Geiger Score. In general, there should be self-learning modules aligned with (or as part of) the GEIGER Toolbox, i.e. these modules should work e.g. for employees of an MSE independent of course providers or trainers etc. – but could also be guided by a GEIGER Security Defender who might work at or consult this MSE.

A general objective would be that the level of GEIGER related cybersecurity competences and their potential improvement due to learning activities of people working in an MSE feeds in and potentially improves the GEIGER Indicator Score or this MSE.

Hence the competence level of employees etc. has to be part of the data structure of the GEIGER Indicator Score and there should be different possibilities to influence that score also after the initial data collection: manually by the learner him/herself or by the potentially involved GEIGER Security Defender and automatically via an interface by the learning application itself.

Overall, the GEIGER Toolbox, potentially recommending certain learning activities, has to work within MSE environments with only lay people. Also, it is not realistic that the necessary competence level of GEIGER Security Defenders can be reached by self-learning around the GEIGER Toolbox, i.e. whereas Security Defenders are on levels 3 and 4 of the Competence Grid the self-learning can be limited to competences/topics of levels 1 and 2.

11.3 Issue: Competence Measure

To allow interoperability of the GEIGER Toolbox with the SRL features but also with the synchronous courses and the dissemination activities of (Certified) Security Defenders, i.e. in an automated and manual way, a measuring system for CS-competence and its development for persons in MSEs is required. Scores in concern of certain topics and the respective competence development have to be calculated that feed into the Indicator Score. Based on the analysis of similar approaches this system will built on the GEIGER Competence Grid, it will prioritize topics/threats and build learning paths following the degree of technicality and complexity of such issues.

11.4 Issue: Certification

The certification within the GEE that results in the title of „Certified Security Defender" is intended for learners acting within Competence Level 3.

For the time being a model for the organisation of the certification is suggested:

- the GEIGER Consortium certifies courses and assessments of educational organisations, including GEIGER partners, and provides a curriculum and a set of further education materials (in different languages). Educational organisations can adapt these materials to their specific target group(s) and conduct the certification of the learners.

In terms of a long-term sustainable perspective, depending on further differentiation of educational approaches, a more advanced model, that is often used in expert further education, is possible:

- the (follow-up of the) GEIGER Consortium defines curriculum and further relevant parts of the syllabus. Educational organisations further develop the syllabus and their learning materials for their target groups. The certification of individual learners (of CSD, i.e. Level 3, or GEIGER Multipliers/Trainers, i.e. Level 4) is conducted by an independent certification body.
- In an alternative approach, curriculum and syllabus development are arranged in the same way, whereas the certification is applied on the level of the education providers. Consequently, single learner would not obtain their certificate form the educational provider or from the GEIGER sustainable body via the educational provider.

Accordingly, within the scope of WP3, further refinement of the current and future sustainable certification concept of GEIGER is needed from an organisational, as well as from an educational and content-specific point of view.

ISO/IEC 17024 4.2.5

The certification body shall not offer or provide training, or aid others in the preparation of such services, unless it demonstrates how training is independent of the evaluation and certification of persons to ensure that confidentiality and impartiality are not compromised.

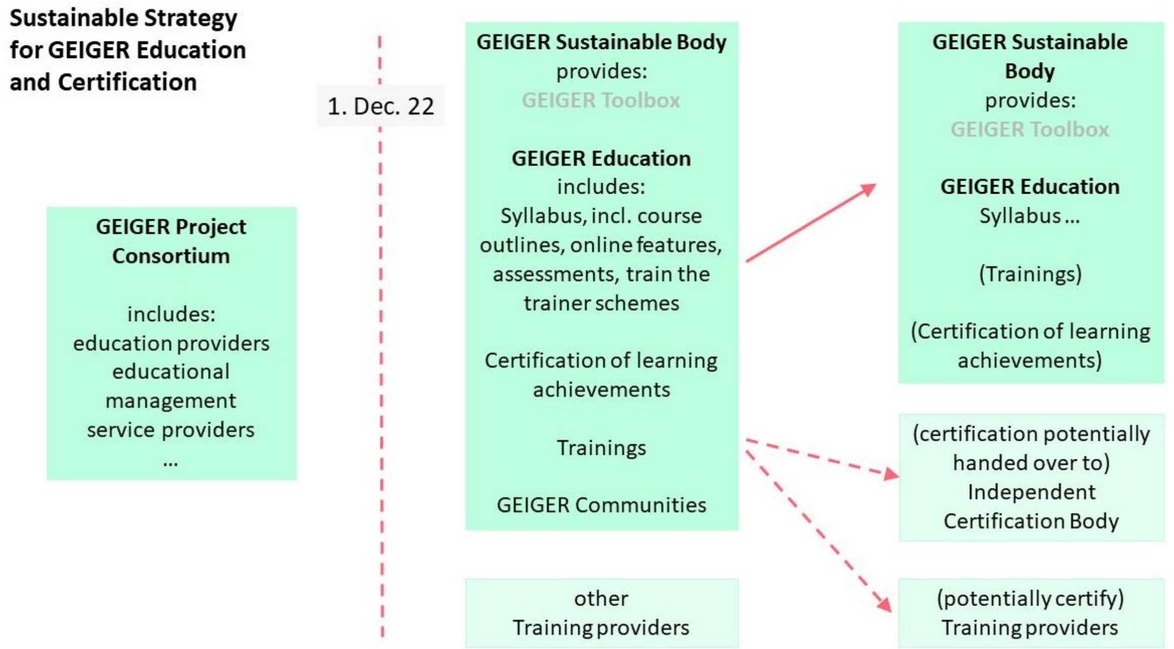

Sustainable Strategy for GEIGER Education and Certification
1. Dec. 22
GEIGER Project Consortium
includes:
education providers
educational management
service providers
...
GEIGER Sustainable Body
provides:
GEIGER Toolbox
GEIGER Education
includes:
Syllabus, incl. course outlines, online features, assessments, train the trainer schemes
Certification of learning achievements
Trainings
GEIGER Communities
other Training providers
GEIGER Sustainable Body
provides:
GEIGER Toolbox
GEIGER Education
Syllabus ...
(Trainings)
(Certification of learning achievements)
(certification potentially handed over to) Independent Certification Body
(potentially certify) Training providers

Figure 11 Sustainable Certification Organisation

11.5 Exploitation

The cyber threat landscape is rapidly evolving, as can be seen in regular reports and updates of CERT organisations. These changes go along with a necessary evolvement of new sensors and protection tools. For that reason, the scope of GEIGER trainings need to constantly evolve over time with a focus on current cyber threats and possible tools to prevent attacks.

With regard to the deliverable of the Final Training Report, major challenges concerning the long-term strategy of the GEE in terms of exploitation and sustainability are to be discussed. The overall organisation and first steps of ensuring a vivid Education Provider Community and Security Defender Community will be following the current process of conceptualizing these communities. On the exploitation part, cost and licencing questions will be addressed. A major task will be to ensure an up-to-date GEE after the project lifetime that also considers potential future target groups.

For the purpose of creating a coherent sustainable GEE, the stated aspects have to be handled not as single and separate tasks, but as a network of interdependent matters. Exploitation planning of respective consortium partners will have to be considered as well when looking at long-term approaches for an evolving GEE.

11.6 Importance until Intermediate Training Report

The overarching task to be addressed until the delivery of the Intermediate Training Report (D3.2) is the coordination and support of the Use Case Training Modules in T3.1 – Security, Privacy, and Personal Data Protection Training Modules. As part of the specific training concepts, train-the-trainer schemes will have to be further specified and coordinated for the Use Cases. For the Task T3.2 – Cyber Range-supported Security Defender Challenges, the target groups (e.g. their prior knowledge or learning group size etc.) will have to be further defined, as well as the general concept on conveying the cyber range challenges.

Within the scope of T3.3. – Education Provider Community, PHF has taken first decisions on the conceptualization and is currently gathering lists of potential members, likewise similar communities which can serve as model. From this starting point, PHF will substantiate the ideas and lead the institutionalisation of the Education Provider Community, also considering suitable platforms.

For T3.4 – Security Defender Community, further specifications on the community structure, tasks and identity will be undertaken under the lead of FHWN, with the support of PHF. A special focus of the University of Education Freiburg will be the organization of the certification environment for Cyber Security Defenders. This topic concerns the certification within the GEIGER lifetime, as well as a sustainable solution after the project lifetime (see also subsection "Certification").

The value of D3.1 with regard to the developments in the Framework-WP2 is the clarification of the interdependence with WP3 and the clarification of interface requirements.

The value of D3.1 with regard to the developments in the Validation-WP4 is the basis for differentiating relevant criteria within the framework conditions and concern of the pertinent KPIs.

The value of D3.1 with regard to the developments in the Dissemination-WP5 is the basis for identifying mapping target audiences and related added values to focus on.

12 Summary and Conclusions

This deliverable D3.1 has reported the results of the training plan definition resulting from the work performed in WP3 during the months M01-M06. The training plan is based on the analysis of relevant background theories on education and anchored in the use cases' educational contexts and needs.

The first contribution is the training plan in the format of the GEIGER Competence Grid (GCG), which defines educational outcomes over four levels and five pillars. The learning objectives have been defined in terms of knowledge and know-how goals. The deployment of the grid into the Swiss, Romanian, and Dutch use cases has been described, including a feasible time series of teaching activities for educating security defenders. Also, the mapping of the partners' background tools into the GCG for enabling the respective learning has been described.

The second contribution is the definition of the education provider community. Described have been the core tasks of the community, the community characteristics with the help of the Community Canvas structure, and the links of the education provider community with the security defenders community.

The deliverable is used as follows in the GEIGER project. Within WP5 it is used to further refine the Security Defenders education (resolution of the still open issues) and guide the development of the training modules and cyber range-supported challenges. The eventually validated and demonstrated Security Defenders education scheme will be standardised or contributed to standards in collaboration with WP5. It will also be used as a description of the basic methodology for how to foster the education provider and certified security defenders communities in collaboration with Dissemination in WP5. The deliverable is further used to synchronise the adaptation and integration of educational tools into the GEIGER Toolbox. Also, the preliminary training schedule is used as a basis to plan validation and demonstration in WP4.

References

ANSSI (2017a) CyberEdu. Syllabus pour le cours de sensibilisation et initiation à la Cybersécurité - https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/

ANSSI (2017b) Request dossier for SecNumedu labelling - https://www.ssi.gouv.fr/en/cybersecurity-in-france/formations/secnumedu-labeling-of-higher-education-courses-in-cybersecurity/

ANSSI (n.y.) MOOC de l'ANSSI - https://secnumacademie.gouv.fr/

Bloom, Benjamin S. Taxonomy of Educational Objectives. Boston, MA.

Breuer, J. (2010) Spielend lernen? Eine Bestandsaufnahme zum (Digital) Game-Based Learning. Düsseldorf: Landesanstalt für Medien Nordrhein-Westfalen (LfM). http://www.lfm-nrw.de/fileadmin/lfm-nrw/Publikationen-Download/Doku41-Spielend-Lernen.pdf

CISCO (2018/19) Introduction to Cybersecurity (2.10) - https://www.netacad.com/portal/web/self-enroll/c/course-725477

Cole, Megan (2017) Just how Micro is Microlearning - https://www.td.org/insights/just-how-micro-is-microlearning

ECSO (2018) Gaps in European Cyber Education and Professional Training. https://ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

EFF (2020) Security Education Companion - A free resource for digital security educators - https://sec.eff.org/

ENISA (2016) Review of Cyber Hygiene practices. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport

GitHub (2020) xAPI-Spec. https://github.com/adlnet/xAPI-Spec

Horn, Michael (2014) KAIST Doesn't Wait For Change In Korea, Pioneers 'Education 3.0'. Forbes Magazine March 2014.

Huizinga, J. (1956) Homo Ludens. Vom Ursprung der Kultur im Spiel. Reinbek bei Hamburg: Rowohlt.

ICT-Berufsbildung (2020) Bildungsplan Informatikerin / Informatiker. https://www.ict-berufsbildung.ch/fileadmin/user_upload/01_Deutsch/01_Grundbildung/PDF/BiPla_Informatiker_20200615-d.pdf

ISO.org (2018): Transitioning from ISO 29990 - Briefing Note.

Kolb, David Allen (1984): Experiential learning. Experience as the source of learning and development. Englewood Cliffs, N.J.: Prentice-Hall.

Kročil, O., Pospíšil, R. The Influence of GDPR on Activities of Social Enterprises. Mobile Netw Appl 25, 860–867 (2020). https://doi.org/10.1007/s11036-020-01513-7

LOM-DE (2010) - Specification of a LOM Profile for German metadata exchange Version 0.9 http://sodis.de/lom-de/LOM-DE.doc

McGonigal, J. (2012). Besser als die Wirklichkeit! Warum wir von Computerspielen profitieren und wie sie die Welt verändern. München: Heyne.

Michael, D., & Chen, S. (2006). Serious Games: Games that Educate, Train, and Inform. Boston: Thomson Course Technology PTR. https://doi.org/10.1021/la104669k

Murphy, Wendy Marcinkus (2012) Reverse Mentoring at Work: Fostering Cross-Generational Learning and Developing Millennial Leaders, Human Resource Management, Vol. 51, No.4.

Neel, Praveen (2019) SCORM vs xAPI: The Right Choice for Your eLearning. https://www.wizcabin.com/scorm-vs-xapi-the-right-choice-for-your-e-learning/

Pavlas, D., Heyne, K., Bedwell, W., Lazzara, E., & Salas, E. (2010). Game-based Learning: The Impact of Flow State and Videogame Self-efficacy. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 54, 2398–2402. https://doi.org/10.1177/154193121005402808

Plass, Jan L.; Homer, Bruce D.; Kinzer, Charles K. (2015) Foundations of Game-Based Learning. In: Educational Psychologist 50 (4), S. 258–283. DOI: 10.1080/00461520.2015.1122533.

Remmele, B. (2006) Open Educational Resources – anonymity vs. specificity, in: European Journal of Open and Distance Learning 2006/2.

Retzmann, T., Seeber, G., Remmele, B., Jongebloed, H.-C. (2010): Ökonomische Bildung an allgemeinbildenden Schulen: Bildungsstandards - Standards für die Lehrerbildung.

Robson, Robby (2006): A Practical Introduction to SCORM – Part 1

Salen, Katie; Zimmerman, Eric (2004) Rules of play. Game design fundamentals. Cambridge, Mass.: The MIT Press.

Wanberg, C.R., Welsh, E.T., & Hezlett, S. A. (2003). Mentoring research: A review and dynamic process model. Research in Personnel and Human Resources Management, 22, 39-124.