Deliverable D5.2

Intermediate Impact Report

Point of Contact	Samuel Fricker
Institution	FHNW
E-mail	samuel.fricker@fhnw.ch
Phone	+41 79 196 9629

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	M18
Date of delivery	30/11/2021
Lead partner	TECH.EU
Contributing partners	UU, TECH.EU, KASP, PHF, MI, KPMG, BBB, ATOS, KSV, HAAKO, CERT-RO, CLUJ IT, E-ABO, SCB, PT, SRA, CL
Authors	Heini Jarvinen (TECH.EU), Samuel Fricker (FHNW), Stelian Brad (CLUJ IT)
Contributions	Jessica Peichl (PHF), Bernd Remmele (PHF), Tony van Oorschot (SRA), Euplio Digregorio (SKV), Max van Haastrecht (UU)
Reviewers	Tony van Oorschot (SRA), Wissam Mallouli (MI)

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	05/10/2021	Heini Järvinen, TECH.EU	Table of content, first draft
0.2	20/20/2021	Jessica Peichl, PHF Bernd Remmele, PHF	1.2.1 Multiplier outreach & collaboration, ecosystem building 1.3.1 Ecosystem bootstrapping, partnerships with the stakeholders 2.2 xAPI for Interoperability with Educational Tools 2.5 Security Defenders Curriculum for ICT Berufsbildung Schweiz and Coiffeur Suisse
0.3	25/10/2021	Heini Järvinen, TECH.EU	1.2.1 Multiplier outreach & collaboration, ecosystem building 1.2.3 Communication materials 1.2.4 Events 1.2.5.1 Scientific publications 1.2.6 Overview of dissemination activities 1.4 Management of key success factors and risks
0.4	05/11/2021	Heini Järvinen, TECH.EU	1 T5.1 Dissemination and MSE ecosystem-building 1.1 Impact goals and timeline 1.2.2 Tools and channels 1.2.4 Events 1.4 Management of key success factors and risks
0.5	09/11/2021	Tony van Oorschot, SRA Euplio Digregorio, SKV Heini Järvinen, TECH.EU	1.2.1 Multiplier outreach & collaboration, ecosystem building 1.2.4 Events 1.2.5 Publications 1.3.3 Recruitment of SMEs for the pilot studies 1.3.4 Dissemination linked to exploitation
0.6	12/11/2021	Heini Järvinen, TECH.EU	1.1.1 Publications 1.2 Achievements M7-M18 1.2.6 Crisis communication plan 1.2.8 Impact tracking 1.3.1 Ecosystem bootstrapping, partnerships with the stakeholders 1.3.2 Preparation of the launch party
0.7	14/11/2021	Stelian Brad, CLUJ IT	1.2.1 Multiplier outreach & collaboration, ecosystem building 1.3.3 Recruitment of SMEs for the pilot studies 3 T5.3 Exploitation Planning
0.8	15/11/2021	Heini Järvinen, TECH.EU	1.2.1 Multiplier outreach & collaboration, ecosystem building 1.2.4 Events 1.2.5 Publications Editing and integrating contributions
0.9	18/11/2021	Heini Järvinen, TECH.EU Max van Haastrecht, UU	1.2.3 Communication materials 1.3.3 Recruitment of SMEs for the pilot studies

1.0	23/11/2021	Tony van Oorschot, SRA Heini Järvinen, TECH.EU Ioana Gaboreanu, TECH.EU	Review comments (draft v0.8) on the whole document Abbreviations, Glossary
1.1	24/11/2021	Heini Järvinen, TECH.EU	Introduction 1.5 Summary and Conclusions Conclusions 1.2.4 Events 1.2.7 Overview of dissemination activities
1.2	26/11/2021	Wissam Mallouli, MI Heini Järvinen, TECH.EU	Review comments (draft v0.9) on the whole document Executive summary
1.3	27/11/2021	Heini Järvinen, TECH.EU	1.2.5.4 Overview of non-scientific publications
1.4	28/11/2021	Stelian Brad, CLUJ IT	3 T5.3 Exploitation Planning, edits Review T5.1
1.4	28/11/2021	Samuel Fricker, FHNW	2 T5.2 Standardisation and Liaison with Policy
1.9	30/11/2021	Samuel Fricker, FHNW	Quality Check
2.0	30/11/2021	Bettina Schneider, FHNW	Quality Check

Contents

Abbreviations, participant short names and glossary

Abbreviations

3B ICT	Balkan, Black Sea and Baltic ICT (3B ICT) Cluster Network
API	Application programming interface
CERT	Computer emergency response(/readiness) team
CLEMS	Cluster Eco-Inovativ Pentru Un Mediu Sustenabil
CONCORDIA	Cyber Security Competence for Research and Innovation
CSIRT	Computer security incident response team
CyberKit4SME	Tools for cybersecurity and data protection risk awareness, monitoring, forecasting, and management in small businesses
CyberSec4Europe	Governance structures for a future European Cybersecurity Competence Network
DEIP	A platform to collect all innovations done by all partners and protect as proof of ownership the results using blockchain technology
DEIP	A platform to collect all innovations done by all partners and protect as proof of ownership the results using blockchain technology
DIH	Digital Innovation Hub
ECHO	European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations
ECSO	European Cybersecurity Organisation
EEN	Enterprise Europe Network
ENISA	European Union Agency For Cybersecurity
FIC	International Cybersecurity Forum
GA	Grant agreement
GDPR	General Data Protection Regulation
GEE	GEIGER Educational Ecosystem
ICT	Information and communications technology
IP	Intellectual property
IPR	Intellectual property rights
KPI	Key Performance Indicator
ME	Micro enterprise
MISP	An open source threat intelligence platform and open standards for threat information sharing
MoU	Memorandum of Understanding
MSE	Micro and small enterprise
MVP	Minimum viable product
NBA	Royal Netherlands Institute of Chartered Accountants

NDA	Non-disclosure agreement
NGO	Non-governmental organisation
NIS Directive	The EU Directive on security of network and information systems
POC	Point of contact
PUZZLE	Designing and implementing state-of-the-art cybersecurity, privacy and data protection management framework
SDO	Standards-defining organisation
SME	Small and medium sized enterprise
SPARTA	Re-imagining the way cybersecurity research, innovation, and training are performed in Europe
TLR	Technology Readiness Level
TRAPEZE	Transparency, privacy and security for European citizens

Participant short names

FHNW	Fachhochschule Nordwestschweiz
UU	Universiteit Utrecht
TECH.EU	Fores Media Limited (Tech.eu)
KSP	Kaspersky Lab Italia Srl
PHF	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	Romanian National Cyber Security Directorate
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

Apprentice	A person who is learning a trade from a skilled employer, having agreed to work for a fixed period
atalyst organisation	An organisation with the aims of facilitating change or transformation
Cluster organisation	A legal entity that supports the strengthening of collaboration, networking and learning in innovation clusters and act as innovation support providers
Communication	A strategically planned process that starts at the outset of the action and continues throughout the entire project, aiming at promoting the action and its results, and requiring strategic and targeted measures for communicating to a multitude of audiences, including media and the public, and possibly engaging in a two-way exchange
Dissemination	The public disclosure of the results by any appropriate means (other than resulting from protecting or exploiting the results), including by scientific publications in any medium
Interoperability	The ability of computer systems, software, or platforms to exchange and make use of information
IT-lay person	A person who does not have specialised or professional knowledge of the subject of IT
Launch party	A sequence of events that are planned to coincide with and to follow the launch of the Beta version of GEIGER
Multiplier	An organisation or individual who contributes to the promotion of and communications around the project towards its target audiences, amplifying the messages and bringing higher visibility to the project
Op-ed	A piece of writing that expresses a personal opinion and is usually printed in a newspaper opposite the page on which the editorial is printed
Peer projects	Projects funded under the same call or dealing with connected topics (also 'sister projects')
Primary target audience	The segment or group of individuals or organisations that is most likely or desired to be the user of a particular product or service
Secondary target audience	The second most important segment or group to target the communications of a business or a project
Stakeholder	An individual, group, or organisation, who may affect, be affected by, or perceive itself to be affected by a decision, activity, or outcome of a project
Target audience	The intended audience or group of recipients for a particular message
Technology Readiness Levels	Indicators of the maturity level of technologies. This measurement system provides a common understanding of technology status and addresses the entire innovation chain. There are nine technology readiness levels; TRL 1 being the lowest and TRL 9 the highest.
Umbrella organisation	An association of institutions who work together formally to coordinate activities or pool resources

List of Tables

List of Figures

Executive summary

As a solution for small businesses to improve their level of cybersecurity, data protection, and privacy, GEIGER aims at contributing to the reduction of economic damage caused by harmful cyber attacks, privacy incidents and data protection breaches, and to paving the way for a trustworthy EU digital environment benefitting all economic and social actors.

To reach this impact, GEIGER has adopted a multidimensional strategy for its dissemination, standardisation, and exploitation activities. The core of it is to:

1) build communities around the solutions to cybersecurity challenges that micro and small enterprises (MSEs) experience, and encourage a low-threshold adoption of the tools to address of these challenges;
2) harmonise the GEIGER technical framework and an education programme with third parties through standardisation;
3) contribute to the policy development with recommendations and dialogue;
4) establish a spin-off to assure the full exploitation of the project results.

GEIGER's dissemination efforts (T5.1) have until today focused on approaching "multipliers" – associations, networks and organisations, including mass media, that will allow us to reach our primary target audience, MSEs – and on securing partnerships with them. This outreach will continue throughout the project, and we will deepen our relations with the engaged multipliers, and increasingly initiate joint dissemination activities, to raise awareness around the GEIGER project and solution among the potential end-users. In addition to the outreach towards MSEs, the project's dissemination and communication Task has successfully initiated the work, and will continue it, on assuring the attention and engagement of all other stakeholder groups, such as CERTs/CSIRTs, cybersecurity providers, and education providers, that are critical to building a functioning solution and an ecosystem that is able to support it.

The GEIGER consortium's potential areas for contributions to standardisation and policy identified in D5.1 have been considered for design and implementation in in WP2 (GEIGER Technical Framework) and in WP3 (Security Defenders Education Framework). At the same time, GEIGER has initiated dialogues with stakeholders for discussing lessons-learned and prepare eventual contributions. The areas include:

- C1 Security Defenders Curriculum
- C2 Open GEIGER API for Interoperability with Cybersecurity Tools
- C3 Open GEIGER API for MISP-based Interoperability with CERTs
- C4 Protection of MSEs whose Business depends on Social Networks and Cloud-based Services under non-European Ownership

Meetings with ENISA, the European Digital SME Alliance, and Small Business Standards offered the opportunity to further increase standardisation work targeting new areas of relevance for GEIGER. These include:

- C5 SME Guide on Information Security Controls
- C6 SME Classification
- C7 Open GEIGER API for xAPI-based Interoperability with Education Tools

For exploitation, until today, we have investigated the impact of value for the market by interacting with end-users and potential buyers. The process has not ended, it will continue with new investigations to consolidate our vision for positioning in the market. We have also collected the first data about pricing and possible business models. An internal task force was constituted to provide feedback on various documents that are going to be elaborated for exploitation. The framework for IP management and IP exploitation is formulated to this date. Currently, we are working on the elaboration of the business model. We have activated the Horizon Booster Programme, where we had the first meetings with the consultants.

1 Introduction

This document presents the status of the implementation of the dissemination and communication, standardisation, and exploitation strategies for the GEIGER project, and lists the key achievements for the WP5 work during the period of M7-M18 of the project.

The **dissemination and communication (T5.1)** work supports the overall impact goals of the GEIGER project: reducing economic damage caused by harmful cyber incidents, and paving the way for a trustworthy EU digital environment that benefits the entire European economy. During the past year, the project's initial dissemination and communication plan has been refined and implemented. The focus has been in preparing ground for our communications towards our primary target audience, MSEs. This has been done by creating partnership with "multipliers", key players that will allow us to reach the potential future end-users of the GEIGER solution, including networks and associations, as well as mass media. As of M18, we will continue the outreach towards new multipliers, and initiate further joint activities with the engaged partners to reach out to their audiences.

The work on **standardisation and liaison with policy (T5.2)** concerned the design and implementation of the Security Defenders Curriculum, the Open GEIGER API for Interoperability with Cybersecurity Tools, the Open GEIGER API for MISP-based Interoperability with CERTs, and the Open GEIGER API for xAPI-based Interoperability with Education Tools. It also included the formulation of a policy brief on the Protection of MSEs whose Business depends on Social Networks and Cloud-based Services under non-European Ownership. Finally, work has been performed SME Guide on Information Security Controls and SME Classification.

The efforts linked to planning the **exploitation of the results of the project (T5.3)** are directed to valorise these results in various ways, mostly to transform them into assets for a start-up, but also to create or expand some business-related activities of the consortium members. However, the major focus will be on setting up an international start-up, with a unique position in the European market. Our goal is to differentiate the value to the market with a innovative business model, driven by the developed technology and based on an unique ecosystem which is constructed in the context of the GEIGER project.

The remainder of this document is structured as follows. Chapter 2, T5.1 Dissemination and MSE ecosystem-building, gives an update on the status of the multiplier outreach and ecosystem building, and presents the dissemination and communication activities conducted during M7-M18, and lays out a detailed strategy and planned activities to reach the objectives set for the period of M19-M30. Chapter 3, T5.2 Standardisation and Liaison with Policy, describes [add]. Chapter 4, T5.3 Exploitation planning, presents a detailed exploitation planning roadmap, as well as agreements and documents critical for the exploitation planning. It describes the status of the process to define the GEIGER business model and pricing, and lays out the action plan towards a sustainable rollout that allows for a lasting and long-term positive impact on SMEs and the European economy at large.

2 T5.1 Dissemination and MSE ecosystem-building

T5.1 implements the dissemination work of the GEIGER project, aiming at awareness of the GEIGER challenge and project, raising interest in the GEIGER solution and ecosystem, and stimulating the desire to adopt GEIGER. Tech.eu leads the consortium in this task.

The dissemination and communications objective in the GEIGER project is to raise awareness and interest towards the project among stakeholders, potential customers, interested communities, potential funders and collaborators, and all other audience groups that are relevant for the adoption of the project results. The dissemination plan is designed as a blend of activities adapted to the target groups they are addressing.

The key goals of T5.1 are to **1) maximise our reach towards our primary audience, micro and small enterprises** (MSEs), through associations and networks representing them, and through their trusted service providers (e.g. accountants) or apprentices, to convert them to users of the GEIGER solution**, 2) to facilitate the outreach towards all other stakeholders groups or audiences, such as education providers** and

institutions (to secure their commitment to add the Digital Security Defenders education to their offering), CERTs/CSIRTs (to secure their commitment to collaboration and sharing of the threat landscape data), and cybersecurity providers (to secure their commitment to interoperate with the GEIGER platform) and **3) to support T5.3 in securing partner commitment for the establishment of the GEIGER startup** and sustainable exploitation of the results after the project period.

The dissemination and communication strategy addresses a range of geographically and operationally diverse audiences. It relies on collaboration with "multipliers" – organisations that are able to echo our message and multiply our reach among our principal target audience of MSEs – and use of mass media. By mobilising multipliers and activating mass media at the European and national levels in the pilot use case countries, we reduce our points of contact and create a cascade approach with trusted sources, to reach more MSEs.

A detailed dissemination and communication plan for the GEIGER project has been laid out in the *D5.1 Impact Plan*. The chapter 1 Dissemination and MSE ecosystem-building adds to this plan by providing updates to the planning, introducing complementary precisions to it, and describing corrective actions and any minor modifications to the plan, based on the results of the impact tracking implemented during M7-M18.

2.1 Impact goals and timeline

The dissemination and communication work supports the overall impact goals of the GEIGER project; reducing economic damage caused by harmful cyber attacks, privacy incidents, and data protection breaches, and paving the way for a trustworthy EU digital environment benefitting all economic and social actors.

Until M18, T5.1 has successfully initiated building awareness around the GEIGER and the GEIGER solution's added value to different stakeholder groups, and facilitated generating interest and building partnerships with them. The key objectives for M19-M30 are to consolidate and extend these partnerships, and to coordinate and facilitate activities in collaboration with multiplier partners and mass media to attract MSEs to scale, and to enable exploring point of views of other stakeholders. T5.1 also contributes to the planning of the sustainable exploitation of the project results and the launch of the GEIGER startup, supporting the long-term impact beyond the project lifetime.

The first version of the table below was presented in the *D5.1 Impact Plan*. This version gives an updated overview of dissemination and communications objectives, key messages, target audiences, focus channels and the most relevant materials and actions already completed and planned for each stage of the project.

	M1 - M6	**M7 - M18**	**M19 - M24**	**M25 - M30**	**Post-project**
Stage of GEIGER project	Project launch & preparation phase	GEIGER MVP development	GEIGER MVP development & refinement	GEIGER MVP rollout & release	Exploitation
		Education Provider community	Security Defender community		
Dissemination Objective	Awareness building	Generating interest	Register	Install (letters of intent)	Sustainability
Dissemination and communications strategy					
Goals	Internal alignment: Initiating contacts and awareness on the project	Building communities: Education providers and SME associations/ networks	Coordinating actions with multipliers to reach and activate our primary audience	Introducing the GEIGER toolbox (beta version) and activating MSEs to install and test it	Facilitate a successful roll-out of the GEIGER spin-off to bring a finalised solution to MSEs
Key messages	Introducing project,	Acknowledging the typical cybersecurity	Encouraging to test the cybersecurity	Explaining the practical	Presenting the benefits to

<table>
<tr><td></td><td>highlighting cybersecurity challenges and GEIGER's role in overcoming them</td><td>challenges, emphasising the potential benefits of GEIGER to MSE & education provider communities</td><td>practices of your MSE, evaluate level of risks

Encouraging to sign up for the Beta launch (event & testing GEIGER)

Encouraging to join the GEIGER education community</td><td>functionalities of GEIGER toolbox and its benefits for the user

Presenting the benefits of getting connected to the GEIGER platform</td><td>different target audiences, and explaining how to adopt the solution / to get connected</td></tr>
<tr><td>Key target audiences</td><td>Consortium members, their existing contacts, potential multipliers</td><td>Education providers, SME associations and networks</td><td>SME associations and networks, MSEs, education providers, Security Defenders community</td><td>MSEs, Education provider and Security Defenders communities, cybersecurity provider SMEs, CERTs, potential funders of the GEIGER start-up</td><td>MSEs, Education provider and Security Defenders communities, cybersecurity provider SMEs</td></tr>
<tr><td rowspan="2">Focus channels</td><td>Setting up all channels, mass media</td><td>Event participation, direct contacts and networking, targeted publications</td><td>Targeted publications, mass media, event participation/ organisation, newsletter</td><td>Mass media, targeted publications, event participation/ Organisation (incl. GEIGER launch event), newsletter</td><td rowspan="2">Multipliers, sale partners, educational programmes, VCs, crowdfunding, pitching events</td></tr>
<tr><td colspan="4">GEIGER website and social media channels, partner channels, Tech.eu channels</td></tr>
<tr><td rowspan="3">Materials and actions</td><td rowspan="2">Collection of use case material, articles, flyer, roll-up, giveaways, event participation, panel discussion</td><td>Visual and audio-visual material, panel discussions, social media / website updates</td><td>Op-eds / opinion pieces, targeted workshops, webinars, newsletter updates</td><td>Op-eds / opinion pieces, panel discussions, keynotes, practical workshops, project's final workshop, webinars, newsletter calls-for-action</td><td rowspan="3">Business model, business plan, IP exploitation agreement, entrepreneurial plan, go-to-market plan, pitching materials, cost analysis</td></tr>
<tr><td colspan="3">High impact stories, interviews</td></tr>
<tr><td colspan="4">Press releases and briefings, social media contents, web articles / blogs, event participation and organising, scientific publications</td></tr>
</table>

Table 1: Dissemination timeline, target audiences, messaging and blend of channels, tools and activities

2.2 Achievements M7-M18

During M7-M18, T5.1 has refined and implemented the dissemination and communication plan laid out in the *D5.1 Impact Plan*. The focus during these 12 months has been in developing a strategy to approach associations, networks and organisations that will allow us to reach our primary target audience, and in providing the consortium members the tools for implementing the actions defined in this strategy, in order to secure partnerships with these "multipliers".

T5.1 has also contributed to:

1) WP2 by assisting in the development of the contents for the GEIGER UI, creating drafts of the visuals and text elements, in the role of "GEIGER curator".

2) WP3 by bringing the communication perspective and expertise into its work of preparations for building the GEIGER education ecosystem – Education Provider community, and the Security Defenders community – and the launch of the GEIGER community platform.

3) WP4 by supporting the recruitment of MSEs for the validation and demonstration of GEIGER, collaborating with the pilot use case leaders to build tailored framing and messaging for each target audience and preparing communication materials to be used in the outreach.

2.2.1 Multiplier outreach & collaboration, ecosystem building

Due to the diverse audiences to which the GEIGER project aims at reaching out, building relationships to stakeholders who can help us multiply our reach and boost our visibility, and collaborating with these "multipliers" to coordinate joint activities and publications is a critical part of our dissemination and communication strategy.

During the first three phases of the project (M1- M18), the main objective has been to prepare ground for our communications towards our primary target audience, MSEs, initiating partnership with key players at the EU level and in the pilot use case countries.

The ways to reach out to the potential end-users of the GEIGER solutions have been first investigated and tested with the multiplier organisations in the consortium (SRA, SKV, Cluj IT). Starting from M14, all consortium members, in particular those operating in the three use case countries (Romania, Switzerland and The Netherlands), have reached out to potential external multipliers, making use of the guidelines and communication materials prepared by T5.1 for this purpose.

As of M18, we will continue the outreach towards new potential multipliers. In addition to that, there will be a strong focus in initiating concrete forms of collaboration to the engaged multiplier partners, to reach out to their audiences, MSEs that are potential end-users of the GEIGER Solution.

2.2.1.1 Switzerland

The GEIGER consortium member Schweizerische KMU Verband SKV, a Swiss SME association, supports small businesses directly at the basic level in their daily work, as a complement to industry associations. Together with the SME networks (KMU-Netzwerke), SKV looks after and informs over 70.000 companies in Switzerland and offers active help and support. SKV is one of the key multipliers in the GEIGER consortium, helping us to reach out to Swiss MSEs, and to understand the particular needs and preferences of this audience.

The SKV has a very wide reach towards the potential GEIGER end-users, covering nearly one sixth of all SMEs in Switzerland. Its electronic newsletter is frequently sent out to approximately 70.000 companies, and published on numerous regional platforms (such as www.netzwerk-appenzell.ch and www.netzwerk-zuerich.ch). SKV members also receive five times per year a newspaper "Erfolg", which is being used for one of the channels to disseminate information on the GEIGER project.

The current President of the association, Mr. Roland M. Rupp, has a strong interest in the continuous improvement of small businesses' IT security. On his initiative, and encouraged by SKV's participation in the GEIGER project, the SKV Computer & Cyber Security Center portal went online at the beginning of 2020. The portal is a centralised source of information and a contact point for SKV members, accessible also for all other Swiss small businesses, who have questions on IT and cybersecurity and want to learn more. For the GEIGER project, the portal offers an efficient channel to raise awareness among the potential end-users of the GEIGER solution around cyber risks and the tools for small businesses to manage them.

2.2.1.2 The Netherlands

SRA is an association of accountancy firms that specialise in the SME sector. It's the consortium use case multiplier in the Netherlands, playing an important role in developing, in collaboration with T5.1, the

messaging, formats and contents of communications in the Dutch use case. SRA membership consists of 375 accounting firms that provide their services to MSEs.

The key idea in the Dutch pilot use case is to introduce GEIGER to MSEs via their accountants, who are their familiar and trusted service providers. Many of these accounting firms are also SMEs. This means that GEIGER can be used by the accounting firms themselves, and they can propose it to their clients as a recommended tool for managing cybersecurity risks.

Four times a year, SRA publishes a 'SRAadviseur' magazine targeted to its members. Until the end of the GEIGER project (M30), each edition will include an article around the various aspects of cybersecurity, with a link to the GEIGER project. The first article of the series was published in the second edition of 2021 of the magazine in August.

In addition to the articles published in the SRA magazine, a dedicated webpage has been introduced to inform accountants about the project. This page will also function as a funnel for onboarding them to the concrete GEIGER tool, once available.

For the validation of the GEIGER tool (WP4) and the education programme (WP3), personas were defined, based on the different type of accountants and accounting firms. These personas can help in the communication for both onboarding and dissemination.

2.2.1.3 Romania

Cluj IT is the consortium use case multiplier in Romania. It's a cluster organisation with over 90 members from IT industry, 10 catalyst organisations, and 13 universities. The cluster has also signed partnerships with other professional associations of owners and clusters from Romania and abroad. Cluj IT is a member of the European Digital SME Alliance, and of the Balkan, Black Sea and Baltic ICT (3B ICT) Cluster Network. It also initiated a Digital Innovation Hub, in partnership with several chambers of commerce and industry, centres for SME assistance, etc. Cluj IT is also part of the Enterprise Europe Network (EEN). This large ecosystem offers to us the possibility to interact easily with different multipliers in Romania. In this respect we have also used the channels of our DIH-partners for communication with other multipliers. In addition to that, we set up a partnership with a Club of Entrepreneurs that catalyses owners of small businesses, being orchestrated by a bank (Transylvania Bank).

Until now, we have used this network to disseminate basic information about GEIGER, and to identify the need for cybersecurity services in small and micro businesses. The most important action was related to the first tests of the value proposition of the forthcoming GEIGER solution. Over 300 micro and small enterprises have been contacted with the aim to gather feedback regarding the value proposition drafted together with the MSEs in the consortium. We have used only a part of these channels, to collect the first feedback and to calibrate the message for a next series of investigation.

We also disseminate GEIGER on the website of DIH4S and its social media.

2.2.1.4 Europe

At the EU level, we have conducted active outreach towards peer projects (such as Cyberwatching.eu, Cybersec4Europe, PUZZLE, TRAPEZE, CyberKit4SMEs, and EU CyberNet), networks and umbrella organisation (such as Digital SME Alliance, Accountancy Europe, and European Startup Network), and agencies and bodies in the area of cybersecurity (such as ENISA and ECSO), and secured partnerships with these key actors.

Collaboration with these external multipliers has been started, for example with Cyberwatching.eu project (GEIGER has been communicated through a mini-page and news articles published on the platform, and listed in their Project Radar), ENISA (GEIGER listed on ENISA's SecureSME cybersecurity resource portal for small businesses), and ECSO (GEIGER invited as a guest to the Cyber Investor Days). We have also collaborated to present GEIGER in the context of a number of events organised by these multipliers (see chapter 2.2.4 Events).

2.2.1.5 Overview of multiplier outreach

The table below lists the multipliers – associations, networks, and organisations collaborating with GEIGER for the project's dissemination and endorsing the project – that have been approached until M18 by the consortium members, and presents the status of the collaboration with them.

Multiplier	Contact in the GEIGER consortium	Type of organisation	Country / area	Status of collaboration, joint activities
SRA	n/a	Network/ association	The Netherlands	Consortium member
Cluj IT	n/a	Cluster	Romania	Consortium member
SKV	n/a	Network/ association	Switzerland	Consortium member
NBA, The Royal Netherlands Institute of Chartered Accountants	SRA	Network/ association	The Netherlands	Regular consultation
Digital Trust Center	SRA	CERT	The Netherlands	Partnership established
BT Club of Entrepreneurs (powered by Transylvania Bank)	Cluj IT	Network/ association	Romania	Intermediation of surveys, organisation of events
Association of Owners and Handcrafts Cluj	Cluj IT	Network/ association	Romania	Intermediation of surveys
National Union of Owners from Romania	Cluj IT	Network/ association	Romania	Intermediation of surveys
Chamber of Commerce and Industry Salaj	Cluj IT	Network/ association	Romania	Dissemination of news, intermediation of surveys
Chamber of Commerce and Industry Bihor	Cluj IT	Network/ association	Romania	Dissemination of news, intermediation of surveys
Chamber of Commerce and Industry Satu-Mare	Cluj IT	Network/ association	Romania	Dissemination of news, intermediation of surveys
Chamber of Commerce and Industry Brasov	Cluj IT	Network/ association	Romania	Dissemination of news, intermediation of surveys
Romanian Chamber of Commerce System (41 organizations)	Cluj IT	Chamber of commerce and industry	Romania	GEIGER presented
Chamber of Commerce and Industry Bistrita	Cluj IT	Chamber of commerce and industry	Romania	Dissemination of news, intermediation of surveys, organisation of events
CLEMS	Cluj IT	Cluster association	Romania	Dissemination of news, intermediation of surveys
North-West Regional Development Agency	Cluj IT	NGO	Romania	Dissemination of news, intermediation of surveys
Centre Regional Development Agency	Cluj IT	NGO	Romania	Dissemination of news, intermediation of surveys

CDIMM Maramures	Cluj IT	NGO	Romania	Dissemination of news, intermediation of surveys
Member companies in Bistrita Nasaud County	Cluj IT	Local business environment	Romania	GEIGER presented
Swiss Cyber Security Days (SCSD)	TECH.EU	Event / platform	Switzerland	GEIGER presented
ISACA Switzerland	FHNW	Network/ association	Switzerland	Contact arranged
SCD-DNA	FHNW	Network/ association	Switzerland	GEIGER presented, interest in disseminating GEIGER
Swiss Cyber Forum	TECH.EU	Network/ association	Switzerland	GEIGER presented
Swiss Cyber Think Tank	FHNW	Think tank	Switzerland	GEIGER presented, partnership established
360inControl	FHNW	Business	Switzerland	GEIGER presented, partnership established
ENISA	FHNW, Tech.eu	EU Agency	Europe	Alignment done, collaboration ongoing
ECSO	FHNW, Tech.eu	Network/ association	Europe	Alignment done, plans for collaboration
Digital SME Alliance	Cluj IT	Network/ association	Europe	GEIGER presented, partnership established, collaboration ongoing
European Startup Network	Tech.eu	Network/ association	Europe	Contact initiated, GEIGER presented
Alliance4Europe	Tech.eu	Network/ association	Europe	Contact initiated, interest in disseminating GEIGER
Womenpreneur-Initiative	Tech.eu	Network/ association	Europe	Meeting to introduce GEIGER done, possible interest in communicating GEIGER to their audiences
European Family Businesses	TECH.EU	Network/ association	Europe	GEIGER presented
Accountancy Europe	SRA	Network/ association	Europe	Introduced Geiger, Accountancy Europe, will attend the Dutch kick-off meeting in January 2022
isacs.eu	FHNW, Tech.eu	Network/ association	Europe	GEIGER listed on their website
Cyberwatching.eu	Tech.eu	EU project	Europe	Collaboration ongoing
Cybersec4Europe	Tech.eu, FHNW	EU project	Europe	Alignment done, possible planning for collaboration
PUZZLE	FHNW, KSP	EU project	Europe	Alignment done
TRAPEZE	FHNW, KSP	EU project	Europe	Alignment done

CyberKit4SMEs	FHNW, TECH.EU	EU project	Europe	GEIGER presented, plans for collaboration
Ensuresec	TECH.EU, FHNW	EU project	Europe	GEIGER presented
ANSSI	TECH.EU	CERT	France	GEIGER presented
Association française des correspondants à la protection des données à caractère personnel AFCDP	FHNW	Network/ association	France	GEIGER presented
IHK (Industrie- und Handelskammer) Freiburg	PHF	Chamber of commerce	Germany	Workshop on GEIGER tool and education planned, article to be published on their website
Handwerkskammer Freiburg	PHF	Chamber of commerce	Germany	2 workshops on GEIGER tool and education planned, article to be published on their website
MSE alliances, e.g. catering	PHF	Network/ association	Germany	Materials in preparation
GI (Germany)	FHNW	Network/ association	Germany	Contact arranged
Digihub Südbaden	PHF	Network/ association	Germany	GEIGER presented, workshops in cooperation with Handelskammer open for members/clients interested in cybersecurity
Incubation centers (several)	PHF	Incubation center	Germany	Materials in preparation
EU CyberNet	TECH.EU	EU project	International	Partnership established
The International Software Product Management Association (ISPMA)	FHNW	Network/ association	International	GEIGER presented
CEGEKA	KSP	Business	Italy	GEIGER presented, interest in GEIGER education

Table 2: Listing of "multipliers" – associations, networks, and organisations collaborating with GEIGER for the project's dissemination, and/or endorsing the project

2.2.1.6 GEIGER educational ecosystem

The GEIGER educational ecosystem (GEE) describes the interaction of several stakeholders within the GEIGER cybersecurity education. Since MSEs can be considered as a socio-technological environment, the educational perspective builds upon a close connection between these stakeholders and the GEIGER tool.

The GEIGER education addresses several target groups: Ranging from IT-lay people, who will acquire only basics for cybersecurity, to potential Certified Security Defenders who acquire relevant skills to become a designated person for ensuring cybersecurity within their MSE or also other MSEs.

The GEIGER toolbox supports the education of MSE employees through direct application of the tool features in the MSE context as part of the GEIGER courses, as well as options for self-regulated learning features within the toolbox. Certified Security Defenders gain competences on using the GEIGER toolbox and communicating about cybersecurity and GEIGER within MSEs.

GEIGER courses will be offered by Education Providers, i.e. MSE associations, vocational schools or further relevant associations. Individuals, such as trained Certified Security Defenders on level 4 may as well offer GEIGER courses in formal settings.

Further, the GEIGER community will serve as a support and exchange network for Education Providers and Certified Security Defenders, as well as further individuals or organisations that are in close connection with or interested in GEIGER or cybersecurity. Further, learning materials including train-the-trainer resources will be provided.

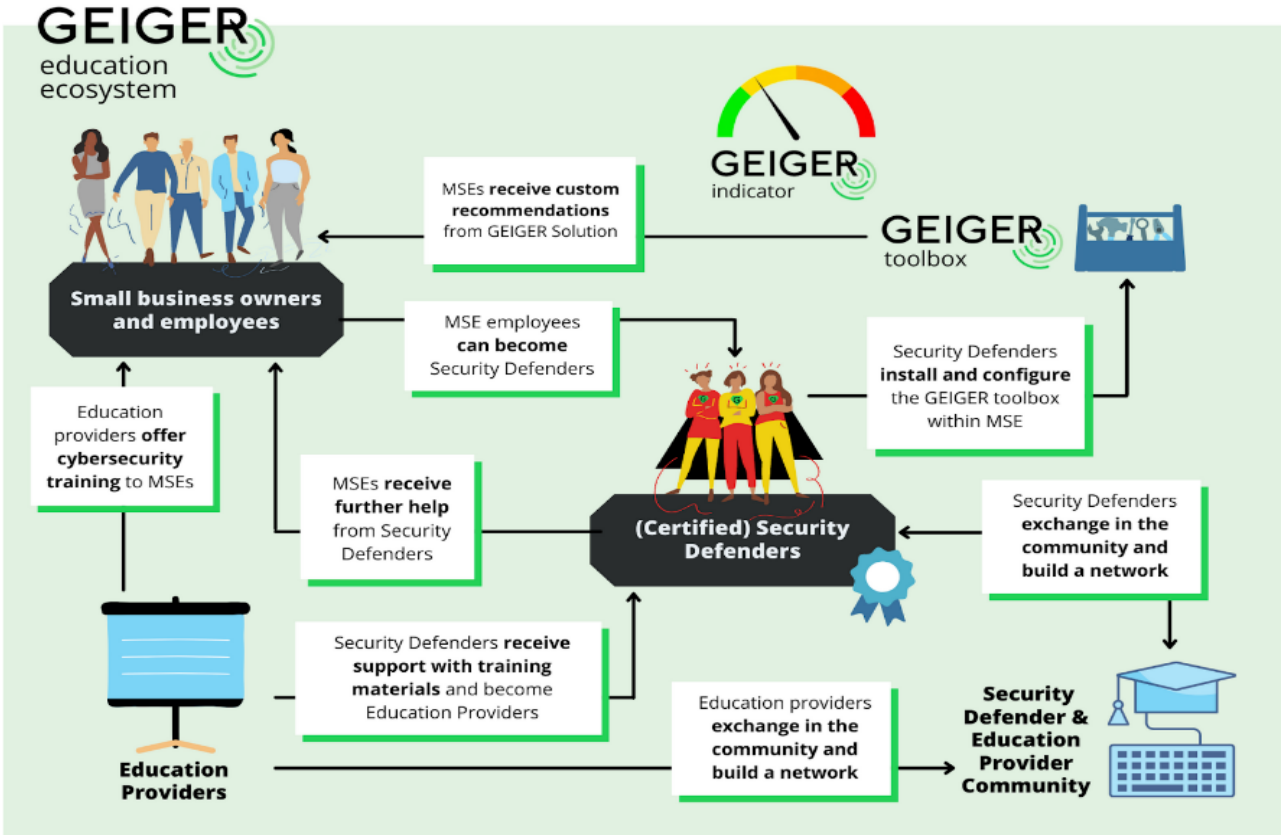

Figure 1: GEIGER Education Ecosystem

2.2.2 Tools and channels

A variety of communications channels and tools – digital, print, and face-to-face – is being used to efficiently reach each of our target audiences, and to communicate with them in a meaningful way.

The target audiences GEIGER aims at reaching are incredibly varying; they differ linguistically, geographically, and culturally, and they come from different backgrounds in terms of industries and fields of expertise, educational levels, and cybersecurity or IT skills. Due to this, setting up centralised communication channels will only get us so far in reaching our dissemination objectives, and in building a real impact. The communications of the GEIGER project relies heavily on the established channels of the consortium partners, through which GEIGER can be introduced to the target audiences in their own language, using messaging and vocabulary they are familiar with and that appeals to them. The range of actors with varying backgrounds and focuses in the consortium is a great help to this end. For example, the dissemination lead, Tech.eu, has a reach of approximately 70.000 viewers, mainly from the tech start-up ecosystem, for its website. SKV's 'Erfolg' newspaper has a circulation of 70.000 SME members, and SRA's quarterly magazine SRAadviseur a circulation of 4.400 and their daily newsletter 14.000 subscribers. Cluj IT reaches up to 300 local startups and entrepreneurs through its own digital member communications, as well as its ecosystem partners' channels.

During the first six months of the project (M1-M6), dedicated digital communications channels and tools as well as visual style for GEIGER were set up. They are introduced in detail in the *D5.1 Impact plan (p. 22)*. From M7 onward, the range of channels and tools was extended with a newsletter mailing list ad subscription

form, and a survey platform. As restrictions to organise physical events have been gradually lifted, participation in them has also offered an important channel to reach out to our audiences and establish partnerships – new in the context of this project, and superior in its efficiency in terms of establishing connections, compared to remote events.

As the focus of the outreach has been until M18 in connecting with multipliers and other stakeholders on a local level and securing partnerships with them, activating the communications via centralised mass mailing list has not been a priority. The infrastructure for sending out the GEIGER newsletter mailings has been established, and it is managed with an open source mailing tool Mailman, hosted by FHNW, to the highest standards of the protection of the personal data of the subscribers. Anyone interested in the GEIGER project and solution can sign up, and subscriptions have been encouraged on the GEIGER website, social media, and face-to-face communications with all stakeholders. The mailing tool has been so far tested and templates prepared, and the first mass mailings are planned to go out to the full list of subscribers in preparation of the GEIGER Beta Launch in June 2022. In the context of the European and national launch events, the possibility to sign up will be further promoted, and a growing list of subscribers will give us a tool to approach the interested stakeholders on a regular basis with updates and calls to action. The plan for the concept of the GEIGER newsletter has been described in detail in *D5.1 Impact Plan*, p.25.

In order to gather feedback from the end-users and multipliers, a survey platform was set up for the needs of the exploitation planning, validation and dissemination of the project. The Questback platform, hosted by FHNW and content managed by Tech.eu, was chosen for this purpose. The platform has been until now used for a net promoter test on the GEIGER value proposition (T5.3 Exploitation Planning). The aim of the net promoter test is to gather feedback from a wider range of small businesses on the value proposition formulated with the help of the MSEs in the consortium. The survey form has been tested in the context of the Romanian use case, and similar surveys for the Swiss and Dutch use case are in preparation. The details of the net promoter test are described in the chapter on *4.1 Exploitation Planning Roadmap*.

The project's participation in events is described in detail in chapter *2.2.4 Events*.

2.2.3 Communication materials

To facilitate presenting the GEIGER project and solution in a consistent and unified manner, both in terms of visual style and contents, T5.1 is tasked with preparing communication materials, print and digital, that support them in their efforts of approaching stakeholders. T5.1 lead Tech.eu coordinates the drafting and production of the print materials, collaborating with the consortium partners, and provider them with guidelines and advice in the use of the produced materials.

The table below lists the communication materials – ready to distribute materials, templates, as well as guides and manuals that have been produced until M18 as part of the GEIGER dissemination kit.

Date	Description	Purpose
9/2020	Logo + variations	ready to distribute
9/2020	Meeting minutes template	template
9/2020	Style guidelines	guide/manual
9/2020	Deliverable template	template
9/2020	Presentation template (ppt)	template

09/2020	Photo, video and audio consent form for events (+ information on the project's processing of personal data)	ready to distribute
10/2020	Introduction flyer	ready to distribute
10/2020	Communications Handbook	guide/manual
01/2021	Introduction poster (one-pager)	ready to distribute
01/2021	Introduction presentation (short)	template
02/2021	Introduction of project phases for partners	ready to distribute
02/2021	Communications guide to approach partners/multipliers	guide/manual
05/2021	Introduction presentation (extended)	template
09/2021	Introduction flyer, v2.0	ready to distribute
09/2021	Roll-up (English and Dutch versions)	ready to distribute
09/2021	Stakeholder involvement roadmap poster	ready to distribute
09/2021	Memorandum of Understanding (MoU) for multiplier partnerships	template
11/2021	Pitch deck, v1.0	template

Table 3: Listing of the contents of the GEIGER dissemination kit until M18

Two presentation slide decks have been prepared for the use of the consortium, to present the project in meetings and events. The short version gives an overview of the project, consortium, and the GEIGER solution. The extended version goes into the detail of the different areas. Both presentation templates can be adapted to meetings and events targeted to a certain audience, according to their centres of interest, and T5.1 is supporting the consortium members in the adaptions.

In preparation for FIC2021 event in Lille, France, in September 2021, the introduction flyer, initially drafted in October 2020, was updated and printed. We also drafted and printed a roll-up with the GEIGER branding and listing the consortium members' logos, and produced a batch of webcam covers for laptops with the GEIGER branding, to be distributed as give-aways that support the awareness on GEIGER as well as awareness on the importance of protecting one's privacy.

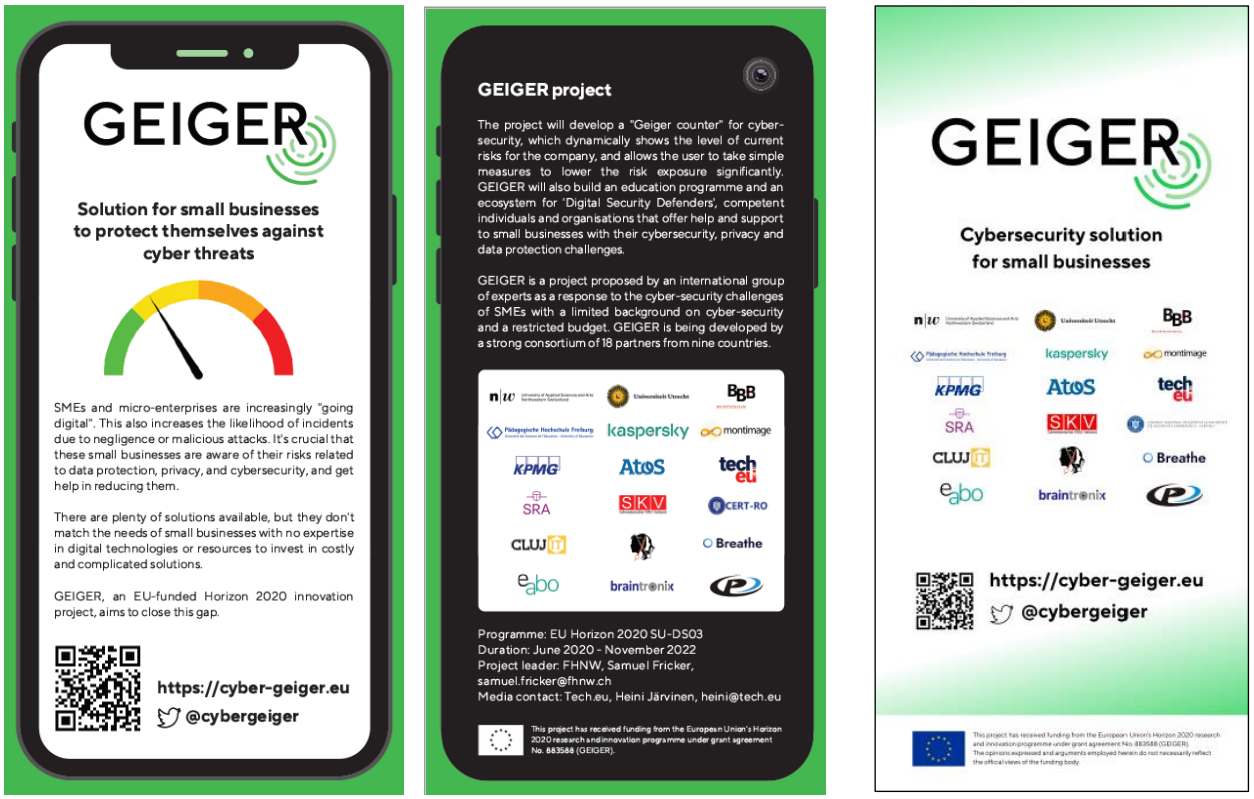

Figure 2: An updated GEIGER flyer and a roll-up were printed for the FIC2021 event.

To facilitate the outreach towards potential multipliers, T5.1 drafted a communications guide for consortium members for approaching multipliers. It laid out the dissemination objectives of the stage of the project, as well as the responsibilities and task division of the consortium members. It included the reference to the supporting communication material kit, and a step-by-step checklist to help consortium members to structure their work approaching the potential multipliers.

We drafted a document 'Introduction of project phases for partners', to familiarise stakeholders with the possibilities to get involved in the GEIGER project. This document was later refined into a visual one-pager, 'Stakeholder involvement roadmap poster', ideal for presentations as well as printing. It has been used in alignment and introduction meetings with a variety of stakeholders, and it has also been printed and distributed in one-to-one meetings as well as at large-scale events such as FIC2021 and European Cyber Week.

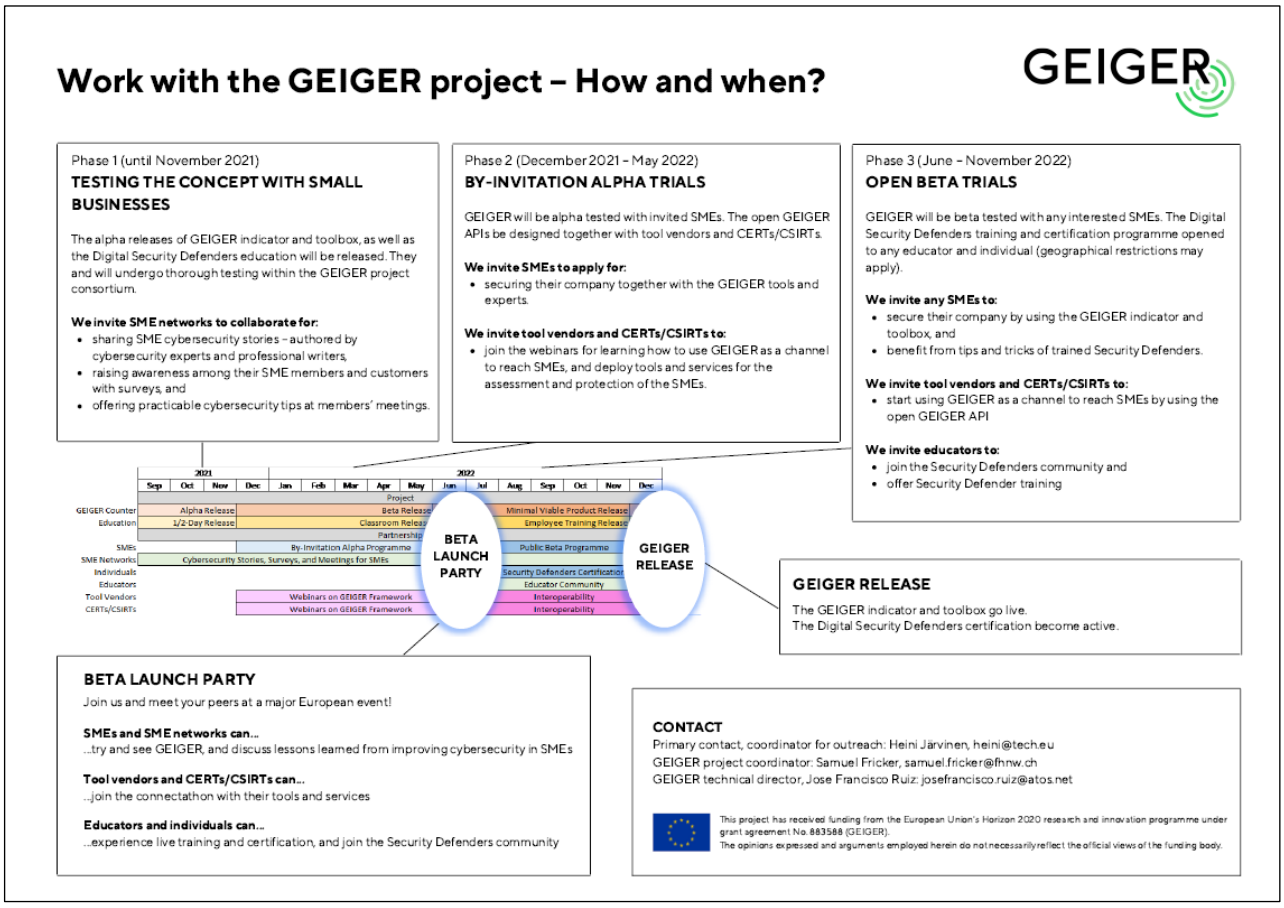

Figure 3: The stakeholder involvement roadmap presents the possibilities for the different stakeholder groups to work with GEIGER.

As part of our multiplier outreach, we drafted a template for a Memorandum of Understanding (MoU). The aim of this document is to help formalising our partnerships with multipliers. A communication kit and guidelines for the consortium members to make the best use of the MoU are preparation.

In addition to the communication materials created for dissemination and ecosystem building purposes, T5.1 has supported the content creation for the GEIGER user interface (UI) in WP2, in the role of the 'GEIGER curator'.

Audio-visual material with the consortium member Loredana has been filmed during the GEIGER retreat in October 2021, and the editing is ongoing. These short video clips will be used in events and distributed via social media to present the MSE perspective to the project, and to offer small businesses an approachable touching point to the GEIGER.

2.2.4 Events

Awareness on the GEIGER solution and the project and its activities is being raised during relevant events. This is done by the organisation of events such as workshops, as part of the project's core activities, by the participation in external events for example as exhibitor at trade fairs or speaker in a panel or a conference, and the by collaborating with event organisers in order to co-organise panel discussions or workshops within an external event.

Due to the COVID-19 crisis, the majority of the physical events during M1-M14 of the project were cancelled, postponed, or converted into online or hybrid events. This has constituted a major challenge for awareness-raising on the project, and in particular for networking to build relevant contacts and alliances through event participation.

Despite the COVID-19 restrictions limiting the possibilities of participation in events, GEIGER consortium has been, since the beginning of the project, actively involved in events online. During the last few months of this reporting period (M7-M18), physical events started to take off. We took full advantage of them to present

GEIGER to our stakeholders, and to connect and further build our relations with multipliers, peer projects, decision makers, tool providers, and other stakeholder groups. M16 also marks the first time a large number of consortium members met in real life, after nearly a year and a half of collaborating almost exclusively online, in the context of the first GEIGER retreat in Braunwald, Switzerland.

During M7-M18, GEIGER consortium was present in total in 18 conferences, 10 workshops, 3 webinars, 1 brokerage event, 1 trade fair, 1 matchmaking event, and 2 other events. Many of these events are international and gather a significant range of stakeholders. In addition to that, we participate in 23 meetings to present GEIGER to stakeholders, and to align with them in different areas of the project. The table below lists the events during M7-M18 in which GEIGER was presented.

Date	Consortium member	Event name	Location	Type of event	Target audience
12/2020	FHNW	Virtual UK Cyber Security Seminar for Swiss Industry 4.0 Advanced Manufacturing	Online	Conference	Industry
01/2021	MI	Webinar on phishing threat (Phish Threat Sophos)	Online	Webinar	Industry
02/2021	FHNW, KSP, TRAPEZE	GEIGER-TRAPEZE Meeting	Online	Meeting	Peer projects
02/2021	CERT-RO	Preparatory meeting for European Cybersecurity Month	Online	Meeting	ICT professionals
02/2021	FHNW	7. F&E-Konferenz zu Industrie 4.0	Online	Conference	Industry
02/2021	FHNW	Trinational Cybersecurity Days 2021	Online	Conference	MSEs
02/2021	FHNW	Trinational Cybersecurity Days workshop, DPIA	Online	Workshop	MSEs
02/2021	PHF	Trinational Cybersecurity Days workshop, Cybersecurity concerns of small businesses	Online	Workshop	MSEs
02/2021	FHNW	ATI Event on Cyber Reslilience of SME	Online	Meeting	MSEs
02/2021	FHWN, PHF, ENISA	GEIGER-ENISA SME Education Call	Online	Meeting	Policy / institutions
02/2021	FHNW, MI, PUZZLE	GEIGER-PUZZLE Meeting	Online	Meeting	Peer projects
02/2021	PHF	GEIGER Workshop for MSEs and multipliers within Handwerkskammer	Online / Freiburg, Germany	Workshop	MSEs
02/2021	PHF	GEIGER Workshop for MSEs and multipliers within IHK (Industrie und Handelskammer)	Online / Freiburg, Germany	Workshop	MSEs
03/2021	FHNW	SATW Swiss TecLadies	Online	Workshop	Students
03/2021	FHNW	P2PKOS Societal Challenge 7 "Secure Societies", 2nd project to policy kick-off seminar	Online	Meeting	Policy / institutions
03/2021	FHNW, ATOS, UU	GEIGER-NCSC	Online	Meeting	Policy / institutions
03/2021	FHNW	Ringvorlesungen «EUROPA! Wir sind mittendrin – schauen wir hin!»	Online	Webinar	Students
03/2021	FHNW	SPM Summit Europe 2022 (The ISPMA Conference)	Frankfurt, Germany & Online	Conference	Industry, academia
04/2021	FHNW	SWISS ENGINEERING – Cyber Security	Online	Conference	Industry
04/2021	KSP	ChannelCity	Online	Webinar	Industry
04/2021	TECH.EU	Brokerage Event - EIT Digital 2022	Online	Brokerage Event	Industry
04/2021	KSP	CSIT 2021 - 8th International Conference on Computer Science and Information Technology	Copenhagen, Denmark	Conference	Industry

04/2021	FHNW, PHF, ENISA	GEIGER-ENISA SME Education Call	Online	Meeting	Policy / institutions
05/2021	FHNW	SATW TecDays	Online	Meeting	Students
05/2021	PHF, FHNW, ATOS, TECH.EU	SPARTA project exchange	Online	Meeting	Peer projects
05/2021	Cluj IT, Tech.eu, e-abo, PHF, CERT-RO	Cluj Innovation Days 2021 SME cybersecurity panel	Online	Conference	MSEs
06/2021	FHNW	Transfer Hochschultag	Switzerland, Online	Other event	Academia, students
07/2021	SRA	SRA IT Kring voor kleine kantoren	Online	Meeting	MSEs
07/2021	PHF	Digital MSE ICT Matchmaking Event Business Without Borders	Online	Matchmaking event	MSEs
07/2021	TECH.EU	Womenpreneur Initiative introduction meeting	Online	Meeting	MSEs
08/2021	UU	ECIS 2021 Doctoral Consortium	Online	Conference	Academia, industry
08/2021	UU, PHF, FHNW, MI, ATOS, TECH.EU	ARES Conference	Online	Conference	Academia
08/2021	UU, PHF, FHNW, MI, ATOS, TECH.EU	ARES Conference - International Workshop on Security and Privacy for SMEs, SME-SP 2021	Online	Workshop	Academia
08/2021	FHNW, MI	GEIGER Coding and Integration Workshop	Paris, France & Online	Workshop	Industry
09/2021	TECH.EU, MI, FHNW	The International Cybersecurity Forum (FIC)	Lille, France & Online	Trade fair	Industry
09/2021	FHNW, MI	Digital SME & NetworldEurope SME WG Workshop on 5G, Edge Computing and IoT	Online	Workshop	Policy / institutions
09/2021	PHF	Meeting IHK Freiburg	Freiburg, Germany	Meeting	Industry, MSEs
09/2021	PHF	Meeting Handelskammer Freiburg	Freiburg, Germany	Meeting	Industry, MSEs
09/2021	FHNW, TECH.EU	CyberKit4SMEs introduction meeting	Online	Meeting	Policy / institutions, peer projects
09/2021	FHNW	Seminar Datenschutz FHNW	Basel, Switzerland	Workshop	Students
09/2021	Cluj IT	The Swiss Contribution – Transition towards a More Digital and Greener Society	Luzern, Switzerland & Online	Workshop	Industry, Administration, Education
10/2021	PHF	Association of European Economics Education (AEEE) Conference 2021	Freiburg, Germany	Conference	Academia, education
10/2021	GEIGER	GEIGER retreat	Braunwald, Switzerland	Meeting	GEIGER consortium
10/2021	CERT-RO	Annual International Conference "New Global Challenges in Cyber Security" - #CERTCON 11	Bucharest, Romania and Online	Conference	Industry, academia, institutions/policy
10/2021	FHNW, TECH.EU	Digital SME Alliance meeting on SME Categorisation	Online	Meeting	Policy / institutions
10/2021	TECH.EU	EU Cybernet introduction meeting	Online	Meeting	Policy / institutions, peer projects
10/2021	FHNW, TECH.EU	ECSO alignment call	Online	Meeting	Policy / institutions, industry
10/2021	TECH.EU	EU CyberNet Annual Conference 2021	Brussels, Belgium & Online	Conference	Industry, policy / institutions, peer projects
10/2021	FHNW	Axiams SOC Opening	Basel, Switzerland	Other event	Industry
10/2021	SRA	SRA IT meetings	Online, NL	Meeting	Accountants

10/2021	SRA	GBNED | Cybersecurity toegepast op uw kantoor	Presentation	Meeting	Accountants
11/2021	TECH.EU	Belgian Cyber Security Convention 2021 & networking event	Brussels, Belgium & Online	Conference	Industry
11/2021	TECH.EU	European Innovation Council (EIC) Summit	Brussels, Belgium & Online	Conference	Industry, policy / institutions, MSEs
11/2021	MI	European Cyber Week	Rennes, France	Conference	Industry
11/2021	MI	Cyber Security & Cloud Expo 2021 Europe – Enabling a secure future	Amsterdam, The Netherlands	Conference	Industry
11/2021	Cluj IT	Orizont Europa și transformarea digitală	Online	Conference	Academia, industry
11/2021	MI	APSSE – presentation about SME cybersecurity	Online	Conference	Academia, industry
11/2021	TECH.EU	Dataconomy Media GmbH	Brussels, Belgium	Meeting	Media, industry
11/2021	TECH.EU	Swiss State Secretariat for Education, Research and Innovation (SERI) introduction meeting	Brussels, Belgium	Meeting	Policy / institutions

Table 4: List of events in which information on GEIGER was disseminated during M7-M18

Below, we describe some of the highlights of the event organisation and participation of the GEIGER consortium and its members.

The Trinational Cybersecurity Days 2021 took place on 18-20 February, online. The GEIGER project was introduced on the first day by members of the GEIGER consortium Bettina Schneider (FHNW), Petra Maria Asprion (FHNW), and Edgardo Montes de Oca (MI). The central discussion around the project unfolded during the Saturday's workshops "Share and exchange: Cybersecurity Challenges for small businesses" and "Data Protection: Conduct a data protection impact analysis". The workshop covered topics on challenges that small businesses are facing, and that can be tackled by awareness and training. Naomi de Marinis, together with Jessica Peichl, PHF, conducted one of the workshop. Naomi is the very first GEIGER Certified Security Defender. She studies in her third year of apprenticeship as a barber (Coiffeuse EFZ) at BBB Berufsfachschule Baden, and also works as an apprentice at Hair & Nails Butterfly.

Figure 4: Naomi de Marinis, is the very first GEIGER Certified Security Defender.

On 5 May 2021, GEIGER participated in an online panel discussion 'Developing SME Cybersecurity Resilience in Europe', organised by Cyber Security for Europe. The panel explored issues relating to developing SME's awareness of cybersecurity in order to improve resilience and responses to cyber attacks. Technical Coordinator of the GEIGER project José Francisco Ruiz from Atos Spain presented GEIGER during the panel.

The Cluj Innovation Days 2021 took place on 18-21 May, with the theme of *'The future economy of Europe. Going green & going digital'*. The GEIGER project was introduced on the third day by members of the GEIGER consortium, Heike Klaus (E-ABO), Jessica Peichl (PHF), and Iulian Alecu (CERT-RO), in a panel discussion 'Cybersecurity: needs and challenges of SMEs in a growing digital world', moderated by Heini Järvinen (TECH.EU).

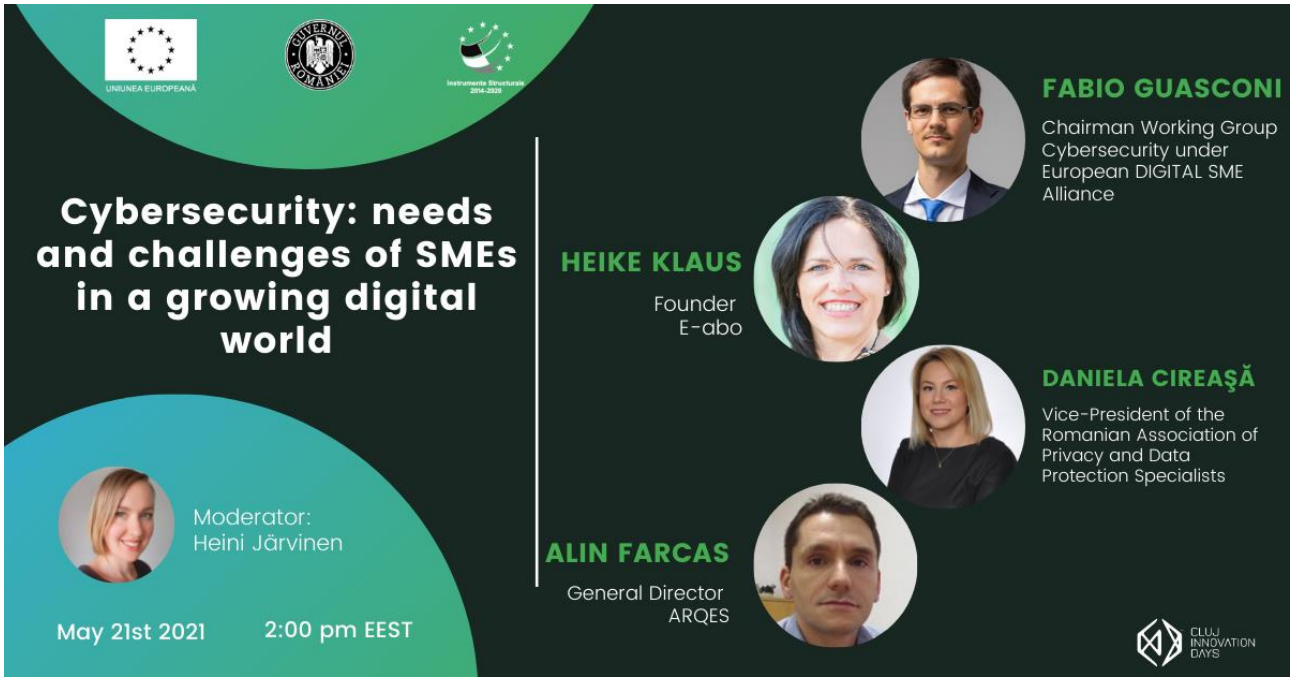

Figure 5: GEIGER was introduced in a Cluj Innovation Days panel discussion 'Cybersecurity: needs and challenges of SMEs in a growing digital world'.

On 18 August 2021, GEIGER partners organised a scientific workshop called *SME-Security and Privacy* that was held in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021). The workshop was a great success that allowed the GEIGER consortium to present a total of four joint papers, and to build synergies with the H2020 PUZZLE project.

The International Cybersecurity Forum (FIC 2021) took place on 7-9 September 2021 in the Grand Palais of Lille, France. FIC is the leading European conference and trade fair on cybersecurity. During the three-day event, the GEIGER team, Heini Järvinen (Tech.eu), Samuel Fricker (FHNW), and Wissam Mallouli (MI), presented the project at a dedicated stand at the EU Pavilion area, together with other Horizon 2020 projects CyberSec4Europe, SPARTA, ECHO, and CONCORDIA, as well as ENISA. We met and discussed with an impressive number of participants and event partners, to raise interest around small businesses' cybersecurity challenges, and to build bridges with various stakeholders of the project.

Figure 6: GEIGER was presented at the EU Pavilion of the International Cybersecurity Forum (FIC) 2021.

On 16 September 2021, Samuel Fricker, the coordinator of the GEIGER project, presented the talk 'Solutions for SMEs to Help Market Access and Uptake or Increase Efficiency' at the '5G, Edge Computing and IoT - Security Requirements for Robust Solution' online conference hosted by the European Digital SME Alliance and NetworldEurope. Samuel highlighted the opportunity of serving digitally dependent and digitally based small businesses with cybersecurity technologies developed by digital enabler SMEs. The meeting was useful to trigger policy discussion on the classification of SMEs and how they are served with cybersecurity.

Events play an important role in connecting with stakeholders and building the ecosystem(s) around the GEIGER solution, in particular during the last phases of the project where we aim achieving their active engagement. The following table lists the events for the remaining 12 months of the project that the consortium will organise, co-organise, or in which GEIGER is going to be present and presented. This is a preliminary list of the events confirmed until today, and will be completed as new opportunities arise.

Date	Consortium member	Event name	Location	Type of event	Target audience
12/2021	PHF	GEIGER Workshop for MSEs and multipliers within Handwerkskammer Freiburg	Online	Workshop	MSEs
01/2021	SRA	Kick-off meeting Geiger pilot (validation & demonstration)	Utrecht, The Netherlands	Meeting	Accountants, MSEs
01/2022	TECH.EU	CPDP2022 Data Protection & Privacy in Transitional Times	Brussels, Belgium & Online	Conference	Industry, policy / institutions
02/2022	FHNW	3rd Trinational Cybersecurity Days Basel 2022	Basel, Switzerland	Conference	MSEs
02/2022	FHNW	RiskIN Conference	Zurich, Switzerland	Conference	Industry
03/2022	BBB	SME event in the context of the Swiss use case	Baden, Switzerland	Conference / workshop	SMEs
04/2022	TECH.EU, FHNW	Swiss Cyber Security Days (SCSD)	Zürich, Switzerland & Online	Conference	Industry, policy / institutions
05/2022	KSP	Cybertech Europe	Rome, Italy	Conference	Industry
06/2022	GEIGER	GEIGER EU Launch	Lille, France	Workshop, trade fair, conference	Industry, policy / institutions, peer projects

06/2022	GEIGER	GEIGER Romanian Launch	TBD	TBD	MSEs
06/2022	GEIGER	GEIGER Dutch Launch	Rotterdam, The Netherlands	TBD	MSEs
06/2022	GEIGER	GEIGER Swiss Launch	TBD	TBD	MSEs

Table 5: List of events planned for GEIGER dissemination M19-M30

2.2.5 Publications

The content drafted for GEIGER project's non-scientific publications constitute the backbone of the framing and storytelling around the GEIGER project and GEIGER solution. They build on the key messages defined in *D5.1 Impact Plan* (chapter *2.5 What: Key messages*) as well as the work conducted on the GEIGER value proposition (see chapter 3.1 Exploitation Planning Roadmap), and contribute to reaching our desired audiences with the messaging that appeals to them, and to building up and giving the direction to GEIGER's public image. These publications include the news published on the GEIGER website, as well as through multiplier channels such as their websites, blogs, magazines, and newspapers, and mass media publications.

Publications in scientific journals and conferences allow the results of the GEIGER project to be presented and disseminated to researcher communities. The aim of these publications is to collect expert feedback, gain visibility, facilitate identifying further partnerships, and build the reputation of the project and its consortium members.

2.2.5.1 Themes and stories

To ensure the relevance and the quality of the content created for the dissemination of the project, T5.1 initiated a working group, "editorial team". It was kicked off in May 2021 (M11). The work is coordinated through the organisation of monthly meetings, as well as *ad hoc* meetings and exchanges in smaller groups to continue work on the planned publications and content.

The editorial team is composed of consortium members with different backgrounds and expertise, to contribute with different perspectives and ideas. The goals of this working group are a) to collaborate on defining the themes and types of content that support the dissemination goals of each stage of the project, and to establish an "editorial calendar" based on these themes and types of content b) to coordinate the production of the content to propose for collaboration with multipliers (e.g. to be published in their magazines and newsletters), c) to fact-check the produced content, and d) to reach out to their contacts (potential multipliers) to test the proposed ideas and to get feedback on them.

These objectives serve to boost the project's outreach towards potential multipliers, and help reaching their audiences with an impactful message, which in turn will enable us to reach our end goal of interesting SMEs in the GEIGER solution, and encouraging them to test it out.

Until M18, the editorial team has produced content around the theme of the wave of Flubot smishing attacks in Switzerland, experienced by the consortium member, small business owner and hairdresser Loredana Bartels. An article describing her experience and presenting tips for SMEs to avoid similar smishing attacks was published by the Swiss consortium use case multiplier SKV in its newspaper 'Erfolg', on the GEIGER website, and on the Cyberwatching.eu platform, and used as one of the key themes for GEIGER's #CyberSecMonth social media campaign in October 2021. The story and the supporting visual material are available for the consortium members to be used for translations and adaptations, and to be published through their own channels, or to be proposed to the multipliers they collaborate with. As a result of the editorial team planning, an article around a Romanian SME that suffered a ransomware attack is in preparation, and will add to the GEIGER project's dissemination "content back" with another relatable story targeted to SMEs.

2.2.5.2 Mass media

Mass media offers a great potential to reach the part of our primary target audience, as a significant percentage of the population is typically employed by SMEs.

While targeted media, such as trade magazines are an obvious channel to approach narrowly defined SME audiences within a specific industry or field, mass media, in particular national and local television, radio and newspapers, offers the possibility to reach out to those small business owners and staff who aren't regularly following these (or any) professional publications.

The content produced as a result of the planning done by the editorial team is also the basis of our proposed content for mass media. This content can be adapted for example into editorial and opinion pieces, press reports, or short videos, in cooperation with the consortium members and media outlets the use case countries or at the European level. Taking into account the diverse languages, cultures, varying media landscapes, and other particularities of each country, the close cooperation within the pilot use cases and benefitting from their understanding of the local environments and existing media connections is critical in order to guarantee the success of this approach.

For the important milestones of the project, such as the Beta launch and the launch of the spin-off, the dissemination lead Tech.eu will coordinate the drafting of joint press releases, including the appealing framing and the storyline, and support the consortium members in their efforts to approach and collaborate with their local media.

2.2.5.3 Social media

The social media accounts for the GEIGER project - Twitter, Facebook, LinkedIn, Instagram, YouTube - were set up during M1. They have been used since then to communicate milestones of the project, and to promote news and event highlights published on the GEIGER website as well as consortium members' event organisation and participation. During October 2020 and October 2021, in the context of the European Cybersecurity Month (#CyberSecMonth), the EU's annual campaign dedicated to promoting cybersecurity, we also ran awareness campaigns around the themes chosen by ENISA for each year's campaign, combining them with open polls inspired by the GEIGER value proposition net promoter test, as well as contents linked to how to protect oneself against smishing attacks.

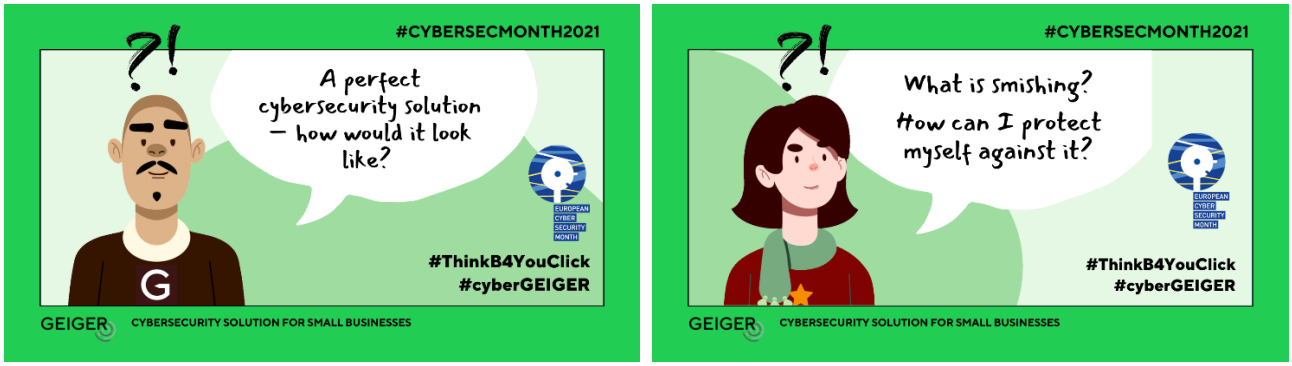

Figure 7: An awareness campaign was ran via GEIGER social media channels in the occasion of the #CyberSecMonth.

As pointed out in our communication strategy, GEIGER's social media channels are not considered the key channel towards our principal target audience. However, they are an efficient way to build visibility and nurture relations within some of the other important stakeholder communities – namely the EU level actors in both areas of SMEs and cybersecurity, and the European and international cybersecurity community. To this end, the GEIGER social media channels have been used to share and promote relevant content published by stakeholders such as peer projects, EU institutions, and cybersecurity community actors, to follow and participate in the public debate around the themes of the project, and to approach potential collaborators via personalised direct messages. In order to use our resources dedicated to dissemination and communication efficiently, we have selected the key social media channels for active use, based on the estimated likelihood of the reach towards our target audiences on each platform. On the rest of the platforms, GEIGER has a minimal static presence (i.e. profile or company page), referring to the actively used platforms and the project website.

The actively used channels until M18 are Twitter and LinkedIn. They are popular among both the "EU bubble" as well as cybersecurity community, and thus allow us to establish a solid digital presence and reach these

stakeholder groups. Facebook has been used in the context of the GEIGER project in a limited manner, mainly reusing the content initially drafted for LinkedIn (as the formats suitable for these channels are rather very similar), to keep the efforts put into managing this channel low. Instagram and YouTube have not been actively used until M18. They are channels that are often used for entertainment purposes, and have a potential for reaching individuals, including SME owners and employees, in their personal capacity (vs. professional context) and thus interest them in the topic of cybersecurity on an emotional level. The relevance to the GEIGER project of activating these channels will be revisited in the preparation of the project stage in which large-scale visibility among MSEs will become our key objective, and when the visuals presenting the concrete GEIGER tool user interface and functionalities – necessary for creating suitable content adapted for these (audio-)visually oriented channels – will be available.

2.2.5.4 Overview of non-scientific publications

The following table lists the non-scientific publications on the GEIGER website and through multiplier channels during M7-M18.

Date	Published by	Title/description	Type of publication
12/2020	SKV	SKV Newsletter December 2020	Newsletter
1/2021	CCI BN	Camera de Comert si Industrie Bistrita-Nasaud newsletters / publications	Newsletter
1/2021	Atos newsletter	Atos participation in GEIGER	Newsletter
1/2021	Kaspersky newsletter	Introducing GEIGER	Newsletter
1/2021	Atos Research and Innovation newsletter	Sibiu Innovation Days 2020 Day 1 Panel 2 Cybersecurity	Newsletter
1/2021	General-Anzeiger (local newspaper)	Introducing GEIGER	Press article
2/2021	cyberwatching.eu	PROJECT OF THE WEEK - GEIGER	Blog
2/2021	cyberwatching.eu	GEIGER: Providing new tool for small businesses to fight cyberattacks	Blog
2/2021	SKV	Cyberwatching.eu: "GEIGER" ist project der woche!	News & Events
2/2021	GEIGER	GEIGER is the Cyberwatching.eu "Project of the week"!	News & Events
2/2021	GEIGER	Event report: HOME RUN - 2nd Trinational Cybersecurity Days Basel 2021	News & Events
3/2021	cyberwatching.eu	Cybersecurity risk management: How to strengthen resilience and adapt in 2021 – Insights and recommendations from research and innovations projects and entities	Other
3/2021	GEIGER	Call for papers for ARES Conference workshop on small businesses' security and privacy is open!	News & Events
3/2021	cyberwatching.eu	Cybersecurity risk management: How to strengthen resilience and adapt in 2021	Blog
3/2021	GEIGER	Call for papers for ARES Conference workshop on small businesses' security and privacy is open!	News & Events
4/2021	Atos	Description of the work done so far in GEIGER project	Newsletter
4/2021	GEIGER	Tracking app – and digital security – for parents of children with asthma	News & Events
5/2021	GEIGER	Cluj Innovation Days 2021, cybersecurity needs and challenges of SMEs	News & Events
6/2021	CERT-RO	GEIGER - project description	Website landing page
6/2021	Cyberwatching.eu	Project Radar	Listing
7/2021	GEIGER	Happy birthday, GEIGER!	News & Events
7/2021	Cyberwatching.eu	Happy birthday, GEIGER!	Blog
8/2021	GEIGER	SME-SP workshop in the ACM ARES 2021 conference	News & Events
8/2021	SRA	GEIGER: Praktische oplossing voor cyberveiling in het mkb	Press article
8/2021	SRA	Webpage GEIGER / Landing page	Website landing page
8/2021	TRAPEZE	Collaborations	Listing
9/2021	GEIGER	International Cybersecurity Forum #FIC2021	News & Events
9/2021	ENISA	SecureSME – How to secure your employees and business from cyberattacks	Listing
9/2021	CyberSec4Europe	Related projects	Listing

9/2021	GEIGER	European Digital SME Alliance and NetworldEurope SME WG Workshop on 5G, Edge Computing and IoT	News & Events
9/2021	SKV	Was ist Smishing, und wie kann man sich davor schützen?	Press article
10/2021	GEIGER	What is smishing, and how to protect yourself against it?	News & Events
10/2021	Cyberwatching.eu	What is smishing, and how to protect yourself against it?	Blog
10/2021	GEIGER	#CybersecMonth: How to tackle smishing?	News & Events
10/2021	Cyberwatching.eu	#CybersecMonth: How to tackle smishing?	Blog
11/2021	EU CyberNet	Stakeholder community	Listing

Table 6: List of non-scientific publication though GEIGER, consortium member, and partner channels

Below, we describe some of the highlights of the non-scientific publications in which GEIGER was presented.

As a follow-up to a webinar organised by Cyberwatching.eu, 'Cybersecurity risk management: How to strengthen resilience and adapt in 2021', in which Max van Haastrecht from Utrecht University, GEIGER consortium member, gave a lightning talk to introduce the GEIGER project, the concept of the GEIGER Indicator, and its benefits for small businesses, a publication containing insights and recommendations was published and distributed through the Cyberwatching.eu channels.

Figure 8: Recommendations composed of the contents of the webinar included a section presenting GEIGER as a cybersecurity risk management tool.

In February 2021, a collaboration with Cyberwatching.eu project resulted in GEIGER being presented as the 'Project of the week' on the Cyberwatching platform. It was accompanied by a blog article with a short presentation of the project, and another blog article with a longer description, and an article was published on the GEIGER website to highlight this collaboration.

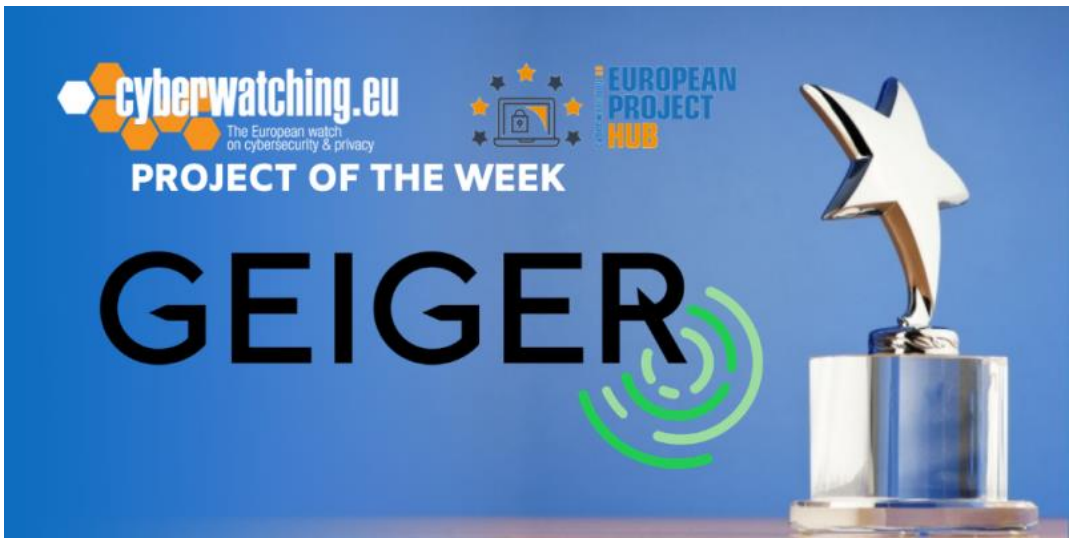

Figure 9: GEIGER was highlighted as a 'Project of the week' on Cyberwatching.eu platform in February 2021.

An accountant association and GEIGER consortium member SRA published an article with an expert interview of Frank Grimberg, FHNW, in their member magazine 'SRAadviseur'. SRA is one of consortium multiplier in the Dutch pilot use case, and the article presents to SRA's membership the GEIGER project, challenges around cybersecurity, and the role accountants could have in tackling these challenges their client MSEs are facing. The original article was published in Dutch, and the English version is being prepared, to be published via GEIGER website, and other translations/adaptations are under consideration, to be used in the Swiss and Romanian GEIGER pilot use cases.

AUTOMATISERING

GEIGER: PRAKTISCHE OPLOSSING VOOR CYBER-BEVEILIGING IN HET MKB

De digitale transformatie maakt cyberbeveiliging steeds belangrijker. Voor kleinere bedrijven is dit extra ingewikkeld. GEIGER, een innovatieproject gefinancierd door de EU, moet hier een oplossing voor bieden. In Nederland komen er een pilot en een opleidingsprogramma gericht op accountants, uitgevoerd door SRA. Wat houdt GEIGER in en wat moet het opleveren? Een eerste kennismaking.

FRANK GRIMBERG
We vergelijken cybercriminaliteit met radioactieve straling. Je ruikt en ziet het niet, maar het is wel gevaarlijk.

TONY VAN OORSCHOT
"GEIGER is specifiek bedoeld voor het mkb, om kleinere ondernemers bewust te maken van de risico's die ze lopen op het gebied van cyberbeveiliging."

Iets voor u?

PILOT

SRA start in het derde kwartaal met de pilot van het educatieprogramma, rekening houdend met de seizoensrijdte op de kantoren en onder uitstekende begeleiding. Geïnteresseerd? Meld u dan aan bij Tony van Oorschot, tvanoorschot@sra.nl.

34 SRAadviseur

SRAadviseur 35

An article published in the Swiss SME association and consortium member SKV's newspaper 'Erfolg' focused on the recent wave of Flubot phishing attacks that many businesses in Switzerland experienced. One of the consortium MSEs, Coiffure Loredana, had experienced the Flubot attack, and the article included her interview, creating a relatable case for small business owners and employees. The article was published originally in German, and the English version of it was published shortly after that on the GEIGER website, and on Cyberwatching.eu platform.

Figure 11: The consortium multiplier, Swiss SME association SKV published an articles in their member newspaper 'Erfolg', presenting GEIGER to their audiences.

To create a stable to-go resource for any cybersecurity questions or issues to its members, SRA launched a landing page dedicated to GEIGER. The page presents the role accountants can have in in helping MSEs address their cybersecurity risks, gives the possibility to learn more about the project and GEIGER education, and offers a contact point for any further questions.

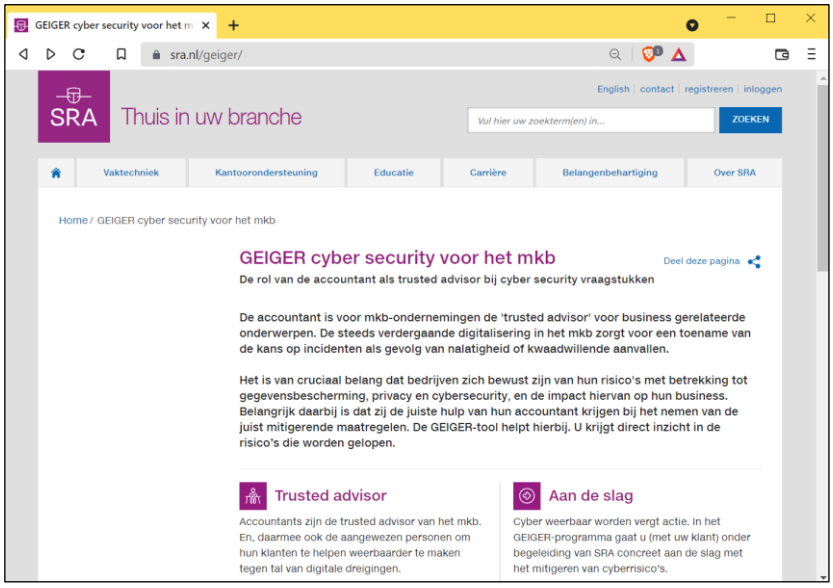

Figure 12: SKV's landing page dedicated to GEIGER presents the role accountants can have in in helping MSEs address their cybersecurity risks.

To assure the presence of the project on as many channels as possible, GEIGER seeks to be part of the relevant listings on relevant platforms. In addition to being listed or presented on the consortium members' websites, GEIGER is listed on Cyberwatching.eu Project Radar, TRAPEZE 'Collaborations' page, CyberSec4Europe 'Related projects' page, CyberNet Stakeholder community page, and ENISA's page 'SecureSME – How to secure your employees and business from cyberattacks' that offers resources for small

businesses to tackle cybersecurity risks. Opportunities to list GEIGER on further website and catalogues are being continuously investigated.

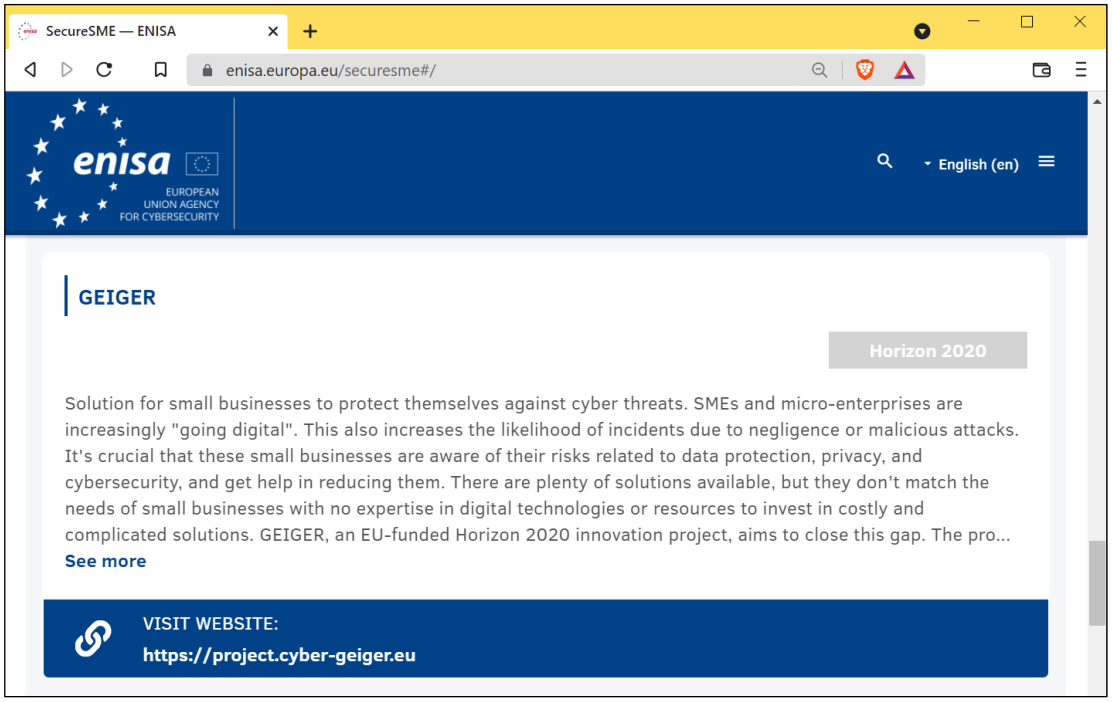

Figure 13: GEIGER is listed on ENISA's SecureSME resource page for small businesses.

2.2.5.5 Scientific publications

The results of the GEIGER project are presented and disseminated through publications in scientific journals, as well as conferences and workshops. The aim of these publications is to collect expert feedback about the quality and soundness of the work being done within the framework of the project. The project also gains visibility among researcher communities through these publications, and facilitates identifying further partnerships and building the reputation of the project and its academic consortium members.

Until today, GEIGER consortium members have submitted 11 articles that were accepted for presentation/publication. Three of these papers are results of collaboration within the GEIGER consortium, and several additional joint papers are in planning for the remaining 12 months of the project. The table below lists the papers submitted until M18:

Date	Consortium member	Title	Link
07/2020	FHNW	SMEs' Confidentiality Concerns for Security Information	https://arxiv.org/abs/2007.06308
08/2020	UU	Can We Survive without Labelled Data in NLP? Transfer Learning for Open Information Extraction	https://www.mdpi.com/2076-3417/10/17/5758
05/2021	UU	SYMBALS: A Systematic Review Methodology Blending Active Learning and Snowballing	https://doi.org/10.3389/frma.2021.685591
07/2021	UU	Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics	https://doi.org/10.3390/app11156909
08/2021	PHF	Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro- and Small Enterprises	https://dl.acm.org/doi/abs/10.1145/3465481.3469198
08/2021	UU, FHNW, MI	A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs	https://dl.acm.org/doi/10.1145/3465481.3469199

08/2021	FHNW, TECH.EU	Classifying SMEs for Approaching Cybersecurity Competence and Awareness	https://dl.acm.org/doi/10.1145/3465481.3469200
08/2021	ATOS, MI, UU	GEIGER: Solution for small businesses to protect themselves against cyber-threats	https://dl.acm.org/doi/10.1145/3465481.3469202
09/2021	CLUJ IT	Domain Analysis with TRIZ to Define an Effective "Design for Excellence" Framework	https://link.springer.com/chapter/10.1007/978-3-030-86614-3_34
10/2021	UU	Open-CyKG: An Open Cyber Threat Intelligence Knowledge Graph	https://doi.org/10.1016/j.knosys.2021.107524
10/2021	CLUJ IT	Requirements Analysis in Disruptive Engineering Solutions Using the Paradigm of Living Systems	https://doi.org/10.3390/app11219854

Table 7: List of scientific papers accepted for presentation/publication in the context of the project

To assure the relevance, quality and high-impact visibility of the upcoming scientific publications, the second GEIGER retreat will focus on the planning and drafting of the upcoming publications among the GEIGER consortium members. This retreat is planned for early February 2022, and will likely take place in in Cluj-Napoca, Romania, and be hosted by Cluj IT.

2.2.6 Crisis communication plan

In order to be prepared to mitigate public criticism or accusations targeted to the project, and to be able to react in a controlled manner in a crisis situation, T5.1 has drafted a GEIGER crisis communication plan.

This document, intended for internal use of the consortium, introduces a set of step-by-step guidelines to prepare the consortium for an emergency or unexpected event that threatens the reputation of the project or the consortium, include steps to take when a crisis emerges, and instructions regarding how to communicate with the public.

The plan includes the crisis communication points of contact (POCs) – the consortium members responsible for leading and coordinating the actions in a crisis situation – as well as contact details of subject matter experts from the GEIGER executive board, who are available to advise POCs regarding best approach to the management of the crisis and the contents of the consortium statement.

The crisis communication plan also lists the most probable and foreseeable scenarios, such as situations in which the project or a consortium member is being attacked by press or public interest groups, and presents tips to proactively develop the positive reputation of GEIGER by leading the narrative.

The crisis communication plan aims at guaranteeing, in case a crisis emerges, a timely response and publication of information, and ensuring that a uniform message is shared across all platforms.

2.2.7 Overview of dissemination activities

The following table replicating the dissemination and communication objectives from the EC portal gives an overview of the number of the dissemination activities during M7-M18 of the project.

KPI	Value	Explanation
Organisation of a Conference	2	Conferences organised or co-organised by GEIGER consortium members, in which the project was presented
Organisation of a Workshop	8	Workshops organised or co-organised by GEIGER consortium members, in which the project was presented
Press Release	0	Press releases sent out by GEIGER consortium members to national or international media outlets, mentioning the project and raising awareness around it
Non-scientific and non-peer-reviewed publication	36	News articles, blogs, introductions, or other long-format texts introducing or mentioning GEIGER that were published in non-scientific publications, including newsletters and member magazines, by GEIGER consortium members, multiplier organisations/networks, media outlets, news agencies, or any other organisations

Exhibition	1	A booth or stand in an exhibition area of a conference, trade fair, or other event (physical or virtual) where GEIGER was presented
Flyer	4	Short-format introduction and information materials (print or digital) produced for the GEIGER dissemination
Training	0	Trainings organised by the GEIGER consortium or its members around the GEIGER Solution
Social Media	174	Social media posts done via GEIGER's or consortium members' social media accounts, throughout all social media platforms, mentioning GEIGER
Website	0	Websites developed and maintained for the purposes of the GEIGER project
Communication Campaign	1	Campaigns through social media, TV, radio, printed mass media, or targeted press to raise awareness around GEIGER coordinated by GEIGER consortium or its members
Participation to a Conference	18	GEIGER consortium member's participation as speaker, moderator, or attendee in a conference (physical or online), where information on GEIGER was disseminated
Participation to a Workshop	10	GEIGER consortium member's participation as speaker, moderator, facilitator, or attendee in a workshop (physical or online), where information on GEIGER was disseminated
Participation to an Event other than a Conference or a Workshop	8	GEIGER consortium member's participation in any other event than a conference or workshop (e.g. webinar, physical or online), where information on GEIGER was disseminated
Video/Film	0	Videos, films and other audio-visual communications materials produced by the GEIGER consortium or its members to raise awareness around the project and its themes
Brokerage Event	1	GEIGER consortium member's participation in a brokerage event (physical or online), where information on GEIGER was disseminated
Pitch Event	0	GEIGER consortium member's participation in a pitch event (physical or online), where information on GEIGER was disseminated
Trade Fair	1	GEIGER consortium member's participation in a trade fair where information on GEIGER was disseminated
Participation in activities organised jointly with other EU project(s)	1	Activities jointly organised or coordinated with peer projects, including (but not limited to) joint publications, campaigns, and events
Other	24	Other meetings such as meetings with peer projects.

Table 8: Overview of dissemination and communication activities linked to the GEIGER project

2.2.8 Impact tracking

The numbers indicating our progress towards the listed KPIs is being tracked throughout the duration of the project, to evaluate the success of the dissemination and communications efforts of the GEIGER project. Based on this tracking, we evaluate whether our efforts in each area have been successful and sufficient. The detailed plan for tracking has been introduced in *D5.1 Impact Plan* (chapter *1.1 Impact tracking*).

From M1 until M6, the dissemination efforts of the consortium members, such as publications, event organisation and participation, and outreach towards multipliers, were tracked via shared spreadsheets in the project cloud (NextCloud) to collect the relevant data on the past activities and the future planning. Even though the regular reminders we sent to the consortium members, the results of this tracking weren't covering the entire consortium, and details from a number of consortium members had to be collected in individual exchanges.

Based on the feedback from the consortium, T5.1 designed and implemented a monthly online questionnaire to facilitate the collection of the tracking data. The platform used for the questionnaire is LimeSurvey, a free and open source online survey web app which allows composing a surveys, and sending them with individual, one-time use tokens that permit each consortium member to fill in the questionnaire once per month. The monthly questionnaires have proven to be more efficient than the shared spreadsheets, and improved the completeness of the collected data. To make sure no dissemination activity goes untracked, targeted follow-up with the key consortium multipliers is being conducted from time to time.

In order to form a complete image of the impact reached through not only the consortium member activities, but also the joint publications and activities with multipliers, tracking numbers linked to them is critical. To this end, questions mapping these activities have been added to the monthly questionnaire, and the

consortium member responsible for the contacts towards each multiplier are encouraged to cover the tracking of the activities coordinated with them.

2.3 Planning M19-M30

2.3.1 Ecosystem bootstrapping, partnerships with the stakeholders

In order to reach the desired impact, GEIGER aims at building mutually beneficial long-term partnerships with the key stakeholders. The most important stakeholder group from the dissemination perspective is MSEs, the end-users of the GEIGER solution. We aim at reaching them mainly through multipliers, their trusted sources of information, support and services, and building and exploiting partnerships with these multipliers continues to be one of the strong focuses of our outreach strategy until M30.

However, to create a functioning solution and an ecosystem that is able to support it, a range of other stakeholders are to be considered. These are for example CERTs/CSIRTs that contribute to the up-to-date threat landscape and information sharing within the GEIGER solution, cybersecurity providers whose tools and services will be integrated to the GEIGER app, education providers that contribute to both the awareness raising around cybersecurity among their students and to educating and training Digital Security Defenders, as well as Security Defenders who will be part of the support network offered by GEIGER to its users.

All these groups are critical to the success of the GEIGER spin-off and thus the positive impact to the society to which GEIGER aims at contributing. A preliminary mapping of the stakeholder and audience groups, as well as their prioritisation in our outreach, has been described in D5.1 (chapters 1 Introduction and 2.4 Who: Target Audiences). This chapter elaborates the status of the key partnerships that have already been secured and that we aim at securing by the end of the project lifetime.

2.3.1.1 GEIGER multipliers & MSE ecosystem building

Until M18, the GEIGER consortium members have initiated and formalised partnerships with a number of key stakeholders, both at the national and European level. The multipliers approached until today have been listed in *Table 2* of this deliverable.

The outreach towards new potential multipliers continues throughout the rest of the duration of the project, and in addition to that, we will increasingly initiate joint dissemination activities to the engaged multiplier partners. The key elements of this process include 1) the GEIGER consortium members flagging opportunities for potential actions or campaigns towards the multipliers with whom they are in contact, 2) the consortium member and T5.1 collaborating to build targeted contents, communications materials and actions, and 3) the consortium member proposing the materials or activities to the multipliers for publication or implementation. The proposed materials and activities can include for example print or digital publications or surveys thought multiplier channels, joint workshops or workshops organised by the GEIGER consortium member and targeted to the audiences of the multiplier, presenting GEIGER in the multiplier events, organisation of joint events, or any other form of collaboration that can help reach the audiences of that multiplier. The materials and activities are often first "tested" by the consortium multipliers, after which they can be easily adapted to the needs of any external multipliers.

In preparation of the GEIGER Beta launch, the relations to the multipliers are being deepened, and collaboration to reach out to their audiences is starting. The relevant multipliers at the European level will be involved in the EU level launch party (see *2.3.2 Preparation of the launch party*), and at the national level to the local launch events. Publications and activities to raise awareness around cybersecurity and to promote the participation in the local launch events will be coordinated and planned in collaboration with them.

A template Memorandum of Understanding (MoU) to formalise the partnerships has been drafted by T5.1 and made available to the consortium members, and an accompanying communication kit is in preparation.

2.3.1.2 GEIGER Education Ecosystem

At the current project stage, each of the educational stakeholder groups – MSEs, Certified Security Defenders, and Education Providers – is represented by pilot users within the three use case scenarios.

The use case Education Providers Berufsfachschule Baden (Switzerland), Cluj IT (Romania) and SRA (The Netherlands) have identified their target groups and outlined course structures accordingly *(cross-reference to D3.2, Chapter 2.2).* Cluj IT and SRA are in close contact with a pool of associated MSEs which will be participating in the pilot courses starting in March 2022. For the BBB use case, the main target groups are vocational students in non-IT and IT classes. Students who become Certified Security Defenders will apply their acquired competences in practice mainly with companies they are working at.

Within these use case scenarios, the main pool of Certified Security Defenders has been identified within the BBB use case, covering a number of student classes. Further Certified Security Defenders will be trained within the pool of IT-MSEs among the Cluj IT-Cluster. In all use cases, additional Educated Security Defenders will be trained on lower levels of the GEIGER Curriculum.

Further details of the planning and status of the GEIGER training is laid out in *D3.2 Intermediate Training Report*.

The GEIGER community has been set up as an online platform. In a first step, the platform has been opened consortium-wide. Within the setting of the GEIGER courses, the pilot users within the use cases will enter the community, as well as organisations in close contact with the GEIGER consortium. After a first feedback workshop with the target group of young Certified Security Defenders a cycle of iterative community building work will start, including member coordination, as well as setting up information and materials on the platform (for further details on the development and structure of the GEIGER Community see *D3.2*).

Further Education Providers will be contacted within the reach of the consortium, and dissemination continues among use case countries for further Education Providers suitable for nationwide spreading of information. For this purpose, dissemination materials have been prepared and first demos of learning features can serve for hands-on sessions, for example Kaspersky's CyberSafety Management Games (CSMG) and Montimage's app-based anti-phishing cyber range.

2.3.2 Preparation of the launch party

The key objectives of these launch events are to gain significance for the project at the EU level, and to mobilise local stakeholders.

The planning includes three stages of loosely linked events that are building on each other:

1) In the first stage, an EU-level launch will be organised. This will be done in the context of the International Cybersecurity Forum FIC2022 that will take place in Lille, France, on 7-9 June 2022. The goals of this event are to gain top-level endorsement and media visibility, and bring the technology actors linked to the project together to work on the interoperability of the GEIGER tools. We will build on our experience of presenting GEIGER in the previous edition of the event in September 2021. To bring the visibility and the impact to the next level, in addition to the dedicated booth in the expo area, a full programme of keynotes and talks by high-level actors in Europe, panel discussions, demo sessions, and other activities around the GEIGER solution and the project will take place in the FIC2022 expo area, followed by a social evening event in another venue in the proximity. To address the technology actors and interoperability, a connectathon area to work on the GEIGER API is being planned within FIC2022. Cybersecurity provider SMEs (digital enablers) are abundantly present in the FIC event, and during in the 2021 edition a number of them have shown strong interest in participating in the upcoming GEIGER connectathon.

2) In the second stage, local launch events will take place in the pilot use case countries, the Netherlands, Switzerland, and Romania. These events aim at showcasing GEIGER with local multipliers, and launch joint planning for activating SMEs in the local level, to eventually secure the participation of a sufficient number of SMEs to the validation and demonstration work (WP4). The detailed concept and planning is being discussed with the consortium members driving the planning of these local events in each use case country,

and the timing, programme, and the communications to attract attention and participants will vary, to maximise the reach towards the local audiences and the impact of these events.

3) In the last stage is linked to the validation and demonstration work, and is led by WP4. It includes local execution of large-scale trials, and repeated local follow-ups with multipliers, monitoring and managing SME activation.

2.3.3 Recruitment of MSEs for the pilot studies

To create impact and prepare for exploitation of the project results, it is critical to ensure MSE participation in the validation and demonstration of the GEIGER solution. In the Dutch pilot use case, accountancy firms (service providers to MSEs and small businesses) have already been involved in the requirements engineering work of WP1 (M1-M6). The involvement of MSEs is planned to increase stepwise in the validation and demonstration).

The validation is being performed by WP4, starting from M13, and it includes interactive user testing and frontrunner Certified Security Defenders (CSD) education evaluation. Approximately 45-50 MSEs (15-20 in each use case country) will contribute to this validation work in the alpha phase, which is planned for months M19-M23. Towards the end of month M24 the GEIGER minimum viable product (MVP) is intended to be available. This month marks the start of validation with beta users. The intention is to involve between 360-1200 MSEs in this phase, to achieve a statistically significant evaluation of the GEIGER solution in operational environments. To reach this large number of MSEs, recruitment of beta users must start early. Therefore, WP4 has already initiated first efforts to recruit beta users. From M22 onwards these efforts must increase (e.g. through local events) to ensure that an adequate number of beta users are recruited by M24. Beta testing will continue until M29, when the final validation results will be used to motivate the GEIGER business model. The results of the MSE recruitment for demonstration will be reported in detail in D5.3 (M30).

The “multipliers” in the consortium (SKV, SRA, ClujIT, as well as BBB that has a considerable multiplier capacity among its audiences) are recruiting these MSEs via their direct interactions and established communications within their networks. Recruiting MSEs for validation is closely intertwined with the communication and dissemination activities around the GEIGER solution and cybersecurity towards the use case multipliers’ audiences, as a minimum level of awareness of the existence of cyber risks is a prerequisite to the interest in their participation. As the validation work in this first phase is for a large part qualitative and demands a level of time and efforts from the MSEs side, securing their participation relies on benefitting from the consortium multipliers’ existing good relations with their members and small businesses in their networks. T5.1 supports the use case multipliers in building the tailored framing and messaging for each target audience and preparing communication materials to be used in the outreach.

2.3.3.1 Switzerland

In the Swiss pilot use case, the key channels used for recruiting MSEs for validation are communications through the SKV website and the regional partner websites, SKV's social media channels and newsletter, visibility in the association media, including Newspaper 'Erfolg', and organisation of and participation in events and workshops. Additionally, we make use of the extensive network of the Swiss pilot use case leader BBB to involve MSEs. BBB will train and certify security defenders, who have direct connections to MSEs through their internship programme. In months M19 and M20 the list of MSEs participating in the alpha phase is to be constructed. This means that enough MSEs will have been recruited by the time the GEIGER integrated prototype becomes fully available for testing.

2.3.3.2 The Netherlands

In the Dutch use case, SRA acts as the pilot use case leader, educator, and multiplier. Dutch accountants will be educated to become security defenders, and can then assist their client MSEs in installing, configuring, and using the GEIGER application. Additionally, accountants’ offices are often themselves MSEs, meaning they fall within the target audience of the GEIGER solution.

In the Dutch use case, the key channel used for recruiting MSE for validation are the accountants within the SRA membership. Using the SRA magazine, newsletters and meetings, awareness around the GEIGER project

has been raised among them. The list of participating SMEs depends on the accounting firms who will participate in the project. This list will be completed by the end of M21. Next to the accountants who already have signed up for the kick-off event, all SRA-members will be invited to participate in the pilot.

A kick-off event was intended to take place on the 18 November 2021. Due to Dutch COVID-19 measures, the event had to be postponed. We decided not to organise a replacement event online, since a judgement was made that this would not offer sufficient possibility to motivate the accountants who are lined up to join the alpha phase of the validation. A total of 6 accounting firms had indicated interest in participating. If each of them is able to interest three MSE clients on average, this will likely yield enough participating MSEs – the goal for the Dutch use case being 15-20 participants in the alpha phase.

A challenge for the recruitment has been the fact that (Dutch) accountants are currently very busy solving COVID-19 related issues. This means that a large extent of their capacity is being used to tackle the their clients' COVID-19 regulation compliance, which is likely discourage them to take on new challenges. This means the GEIGER tool should be available in at least an integrated prototype level for the 'alpha' accountants, to give them an additional push to get involved in the GEIGER project. This implies that the Dutch alpha validation timeline is likely to start in M21 and run past the original end of the alpha phase in M23. Although such deviations are not ideal, the modular design of the WP4 validation planning allows them.

2.3.3.3 Romania

In the Romanian use case, the key channels used for recruiting MSEs for validation are Cluj IT's digital channels towards its members, as well as its ecosystem partner channels (see chapter 1.2.1 Multiplier outreach & collaboration, ecosystem building).

In September 2020 Cluj IT contacted more MSEs to collect data about their interest on cybersecurity practices and education. Over 180 answers have been received. From these MSEs, over 90 showed their interest to participate in further training programs, as well as testing and validation activities. During the summer of 2021, we have conducted a second investigation. This time, out of 300 MSEs, only 35 responded, and 28 expressed their interest to be involved in the testing and validation activities. In this latter exercise MSEs were contacted via email, with the kind request to fill a survey, and this explains the rate of about 10% responses. We will activate a new exercise in December 2021, to be close to the moment of starting the training programs.

In principle, all companies that accepted to participate in the training program also accepted to test the GEIGER prototype. So at this stage, we count to approximately 120 SMEs. The target for Romanian use case is 15-20 MSEs for the validation, thus we have a buffer in the case some of the MSEs will cancel their involvement.

To respect GDPR, in the first exercise we asked to be provided only the email addresses. In the moment of starting the training program and testing of prototypes, MSEs will be contacted again to provide additional data and to delegate the persons who will participate in these actions. In the second exercise, we asked the respondents to provide the name of their company, name of the contact person, and email. Based on the second outreach, a list of 28 MSEs willing to participate in the GEIGER validation has been composed.

The demonstration will be performed by WP4, with a large number of MSEs in the three use case countries. As indicated before, this involves an early alpha phase, where 15-20 alpha users interact with the GEIGER solution in an operational environment. Given the relatively small group of MSEs at this stage, we can perform experiments on-site and intensively interact with the users to gather their experiences. The beta phase of validation comprises the period from M24 onwards. Here, we intend to reach a larger number (360-1200) MSE users. We will still collect feedback on the functioning of the tool, but interactions will be less frequent and less intense. For use case partners and alpha users still using the GEIGER tool in this later phase, we will be able to collect information and insights on the effects of continued use.

The use case multipliers, as well as partnerships built with external multipliers such as SME/start-up associations, chambers of commerce, industry, trade and professional associations and networks for dissemination of the project (T5.1) will be made use of when recruiting these MSEs. In the context of the

Swiss use case, an event to start recruiting MSEs in a large scale for this phase is in planning for March 2022 by BBB.

2.3.4 Dissemination linked to exploitation

To prepare for dissemination linked to exploitation and manage the related dissemination work, the GEIGER project reaches out to relevant stakeholders with targeted messaging at appropriate timings.

At the end of M18, 8 associations or chambers in 3 member states, and 2 associations in Switzerland, have confirmed their intent to recommend GEIGER among their members (KPI I2.1.4.3), 7 education providers to offer GEIGER education (KPI I2.1.4.4), 4 CERTs/CSIRTs to interoperate with GEIGER (KPI I2.1.4.5), as well as 6 tool providers to integrate their tools with GEIGER (KPI I2.1.4.6), and an additional 20+ tool providers that have shown strong interest in learning more about this possibility. We have also secured the support and collaboration of the key actors at the EU level, to facilitate the communications linked to the roll-out of the GEIGER solution.

Reaching out to stakeholders relevant for the exploitation happens hand in hand with building the multiplier contacts for dissemination of the project, as largely the same networks are important for both areas. In the next months of the project (M19-M24), SME and professional associations, start-up and entrepreneur networks, cluster organisations, digital innovation hubs (DIHs), chambers of commerce, and any other networks giving access to our primary target audience and end-users, MSEs, are the most relevant groups of stakeholders.

We have established partnerships with several European level networks and umbrella organisations, such as Accountancy Europe and Digital SME Alliance, and other actors critical to the success of raising awareness of the project at the EU level, such as The European Cyber Security Organisation (ECSO), and the European Union Agency for Cybersecurity (ENISA). Important partnerships have been also established in the pilot countries, including The Royal Netherlands Institute of Chartered Accountants (NBA) and Digital Trust Center in The Netherlands, Swiss National Cybersecurity Centre in Switzerland, and several NGOs, associations and chambers of commerce in Romania, including the Chamber of Commerce and Industry Bistrita, Chamber of Commerce and Industry Salaj, Chamber of Commerce and Industry Bihor, Chamber of Commerce and Industry Satu-Mare, Chamber of Commerce and Industry Brasov, BT Club of Entrepreneurs (powered by Transylvania Bank), Association of Owners and Handcrafts Cluj, CLEMS cluster, CDIMM Maramures, National Union of Owners from Romania, North-West Regional Development Agency, Centre Regional Development Agency, Coiffure Suisse, and Schweizer Yogaverband.

In the coming months, we continue to initiate new contacts, and deepen the existing partnerships by coordinating joint activities and publications, drawing lessons from the joint activities with the consortium multipliers. We aim at formalising the partnerships with multipliers and other relevant stakeholders, such as CERTs, with the mutual MoU (see chapter 1.3.1 Ecosystem bootstrapping, partnerships with the stakeholders').

2.4 Management of key success factors and risks

KPIs under T5.1 reflect the aim at raising awareness and interest of GEIGER solution and ecosystem, and stimulating the target audiences' desire to adopt GEIGER. The communication tools and actions are tailored to correspond to the needs of each geographic and demographic target audience, in collaboration with the partners with local and field-specific expertise, and the impact of the activities is being evaluated throughout the duration of the task to initiate corrective action early whenever necessary.

The table below gives an overview of the KPIs linked to dissemination, their status at M18, as well as the key actions and explanations on their operationalisation.

KPI	Description	Status at M18	Key actions & explanation on operationalisation
I2.1.1.1, I2.1.5.1	>500'000 MSEs will be aware of the GEIGER Indicator as a dynamic risk monitoring	definition ongoing	Delay in launching the active outreach towards multipliers and in launching the newsletter subscription form. The progress of this KPI is under the set goals. Mitigating actions to improve the progress on this KPI:

	instrument, and ≥1'000 industry-diverse MSEs that know the GEIGER Indicator.		• New GEIGER 'editorial team' composed of consortium members from different areas of expertise (kick-off May 2021): coordination of planning, production, and quality control for the communication materials towards multipliers. • Enhanced collaboration on testing the communication content with the consortium multipliers.
I2.1.1.2	>50'000 MSEs will have tried the personalised GEIGER Indicator for their own specific MSEs by registering on GEIGER Solution	planned (M19-M30)	1) Communications through all channels to familiarise the potential end-users with the GEIGER interface and functionalities 2) Targeted training & workshops on the use of the GEIGER tools
I2.1.4.1	≥1'000'000 impressions of the GEIGER Indicator as measured by the number of impressions of media channels.	defined, in progress	300'348 impressions. Activities: 1) Mass media impressions 2) Targeted media impressions 3) Social media impressions (via GEIGER and partner channels) 4) Impressions in events (consortium partners' participation as speakers)
I2.1.4.2	≥100'000 small enterprises have a GEIGER account, allowing them to predict their risk with the personalised GEIGER Indicator and benefit from the GEIGER toolbox.	planned (M19-M30)	Requires MVP of the GEIGER Indicator/Toolbox. Planned activities: 1) Integration of an easy procedure to create a GEIGER account to the GEIGER website 2) Targeted 'Call to Action' communications towards subscribers and followers
I2.1.4.3	≥20 MSE associations or chambers of commerce in ≥50% of the member states will have confirmed their intent to recommend the GEIGER Framework among their member enterprises.	defined, in progress	Mapping and listing the ones already on board. Initiating contacts with potential ones. 1) Mapping the MSE associations and chambers of commerce in the EU member states represented by the consortium members 2) Facilitating the outreach by creating introduction material, best practices and MoU template
I2.1.4.5	≥50% of the CERTs/CSIRTs in member states will have confirmed their intent to interoperate with the GEIGER Framework	defined, in progress	3 have already confirmed: CERT-RO in Romania, NCSC in Switzerland, DTC in The Netherlands 1) Establishing contacts in the early stages of the project 2) Collaboration and involvement of the CERTs/CSIRTs in the development of the framework

Table 9: KPIs linked to T5.1

2.5 Summary and Conclusions

This section gave an overview of the status of the implementation of the dissemination and communications plan for the GEIGER project. It also listed the achievements, actions completed, and communications materials produced during the reporting period (M7-M18).

The key take-aways of this section are:

1) The GEIGER consortium have done excellent work building the foundations for the mass outreach towards MSEs by engaging relevant multipliers, including SME associations and networks, chambers of commerce, umbrella organisations, peer projects, institutions and public bodies, and mass media. In preparation of the beta launch, the relations to these multipliers are being deepened, and collaboration on joint dissemination activities to reach out to their audiences is starting. This will

allow us to maximise our reach towards the potential GEIGER end-users in the phase 4 of the project (M25-M30).

2) In addition to MSE ecosystem building, T5.1 will continue facilitating and supporting the consortium's outreach towards all other stakeholders groups (including education providers, Digital Security Defenders, CERTs/CSIRTs, and cybersecurity providers), to secure partner commitment for the establishment of the GEIGER startup and sustainable exploitation of the results after the end of the project.

3 T5.2 Standardisation and Liaison with Policy

Until Month M06 of Task 5.2 and reported in Section 3.6 of D5.1, the GEIGER consortium has identified several potential areas for contributions standards and policy. For each area, GEIGER planned development in WP2 (GEIGER Technical Framework) and in WP3 (Security Defenders Education Framework) based on identified standards and contributing back for areas where significant gaps were identified in the standards.

- C1 Security Defenders Curriculum
- C2 Open GEIGER API for Interoperability with Cybersecurity Tools
- C3 Open GEIGER API for MISP-based Interoperability with CERTs
- C4 Protection of MSEs whose Business depends on Social Networks and Cloud-based Services under non-European Ownership

During the period of Months M07-M18, the GEIGER consortium entered a dialogue with European agencies, associations, and standards-defining organisations (SDOs). They included ENISA's initiative targeting SMEs, the European Digital SME Alliance working on skills and recommendations for SMEs, the Small Business Standards (SBS) SDO working on recommendations for SMEs, and the European Cyber Security Organisation (ECSO) working on labels and recommendations for SMEs. This dialogue opened several additional opportunities for potential contributions.

- C5 SME Guide on Information Security Controls
- C6 SME Classification
- C7 Open GEIGER API for xAPI-based Interoperability with Education Tools

During the period of Months M07-M18, the GEIGER work focused on evaluating, adapting, and implementing identified standards, respectively designing and implementing the curriculum and GEIGER API. Also, work has been performed for contributing to standardisation and policy. The following subsections describe the status.

3.1 C1 Security Defender Curriculum

The definition and standardisation of the security defender education will allow organisation interested in offering cybersecurity education for laypeople to join the overall educational initiative of GEIGER. The growing education provider community will contribute to building capacity for helping SMEs in cybersecurity. Schools, like represented by the GEIGER partner BBB, and associations, like represented by the GEIGER partners SRA for accountants and CLUJ IT for innovation ecosystems are examples of organisations expected to adopt the security defender curriculum. Also, a curriculum established as a standard will enable certification of any course participant who wants to do a certified security defender examination.

No already existing clearly applicable standard could be identified for designing and implementing the security defender curriculum. Hence, GEIGER aims at developing an own educational curriculum for human certification, obtaining the support for it by stakeholders, and integrate it as a component into other already existing curricula.

GEIGER is in contact with the following organisations for raising awareness and contributing to standardisation in the context of the security defender curriculum:

- ENISA SME initiative: dialog on awareness-raising and educational approaches. ENISA support is important for the positioning of the GEIGER results in Europe.

- ICT Berufsbildung Schweiz: contribution of cybersecurity curriculum for apprentice education in the ICT domain. The support of this professional association is evidence for the relevance and adequacy of the Security Defenders curriculum in the education of ICT-centred professionals.
- Coiffeur Suisse: contribution of cybersecurity curriculum for apprentice education in the hairdressing domain. The support of this professional association is evidence for the relevance and adequacy of the Security Defenders curriculum in the education of ICT-agnostic professionals.

3.1.1 Achievements M7-M18

GEIGER has adapted the Security Defenders curriculum for compatibility with the ICT Berufsbildung curricular scheme. ICT Berufsbildung Schweiz is a standards-defining organisation (SDO) for ICT education in Switzerland. So far, the focus of the GEIGER work has been on the levels 1 and 2 of the GEIGER educational framework described in D3.1.

The highly regulated system of dual vocational education, as experienced in the Swiss use case, implies different aspects of standardisations regarding the curricular structure. 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[1]). 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' (*see also D3.1*).

Figure 14: Learning Objectives related to basic cybersecurity measures in MSE environments (in German).

shows the learning objectives related to basic cybersecurity measures in MSE environments for ICT Berufsbildung Schweiz. Since the SDO is regulating education in the German-speaking part of Switzerland, the learning objectives are specified in German.

[1] https://www.ict-berufsbildung.ch/

Kompetenz	Typische Cybersicherheitsmaßnahmen für Kleinunternehmen umsetzen

Handlungsziele	
HZ1	Informationen über aktuelle Bedrohungen, insbesondere von Kleinunternehmen, und mögliche Gegenmaßnahmen auffinden und wiedergeben können. Häufige Sicherheitslücken erkennen können.
HZ2	Gängige Mechanismen für sichere IT-Prozesse und empfohlene Massnahmen für gängige Applikationen im eigenen Betriebsumfeld umsetzen können.
HZ3	Prinzipien des Schutzes personenbezogener erläutern und gängige Schutzmechanismen umsetzen können.
HZ4	GEIGER-App handhaben können.
HZ5	Wissen mit anderen Personen im eigenen betrieblichen Umfeld diskutieren können.

Objekt	IT-System von Kleinunternehmen,insbesondere unter Einbindung der GEIGER-Umgebung

Leistungsziel-Definition

LZ-Nr.	Leistungsziel	Selbsteinschätzung				Selbsteinschätzung				Kompetenzstufe			Typ	HZ / HKB
		Einschätzung meiner Kompetenz vor der Bearbeitung des Moduls				Einschätzung meiner Kompetenz nach der Bearbeitung des Moduls				Verstehen, reproduzieren, jemandem erklären, erläutern	auf ein neues Problem anwenden können	analysieren, weiterentwickeln, synthetisieren, beurteilen	*Minimalziel, erweitertes Ziel, Expertenziel*	*Handlungsziel und Handlungskompetenzbereich nach ICT-Berufsbildung CH*
		--	-	+	++	--	-	+	++	K1	K2	K3		
LZ1	Ich kann Quellen auffinden, die aktuelle Sicherheitslücken publizieren.													HZ1
LZ2	Ich kann die gängigen Cyberattacken für mein betriebliches Umfeld beschreiben.													HZ1
LZ3	Ich kann erläutern, wer welche Zugriffsrechte im IT-System meines Betriebes hat.													HZ1
LZ4	Ich kann beschreiben, was ich nach einer Cyberantacke tun kann.													HZ1
LZ5	Ich kann sichere Passwörter generieren.													HZ2
LZ6	Ich kann gängige Sicherheitssoftware installieren.													HZ2
LZ7	Ich kann typische Phishing-Mails erkennen und löschen.													HZ2
LZ8	Ich kann die automatische Ausführung von Programmen, Macros etc. deaktifieren.													HZ1
LZ9	Ich kann Datenbackups einrichten bzw. einen Backupplan umsetzen.													HZ1
LZ10	Ich kann automatisches Updaten einrichten.													HZ1
LZ11	Ich kann Cybersicherheits- und Datenschutzzwischenfälle dokumentieren.													HZ2/3
LZ12	Ich kann die zentralen Prinzipien der europäischen Datenschutzgrundverordnung / Schweizer Bundesdatenschutzgesetz erklären.													HZ3
LZ13	Ich kann erklären, was personenbezogene Daten sind und warum sie geschützt werden sollen.													HZ3
LZ14	Ich kann Datenschutzrisiken in meinem Betrieb identifizieren und typische Prozesse zur Maximierung des Schutzes ausführen.													HZ3
LZ15	Ich kann erläutern, welche Daten von mir und meinem/n Endgerät/en in der GEIGER-Umgebung gespeichert sind.													HZ3
LZ16	Ich kann die Grundfunktionen der GEIGER-Umgebung erläutern.													HZ4
LZ17	Ich kann einfache Empfehlungen der von GEIGER-Umgebung generierten Empfehlungen umsetzen und die Person benennen, an die ich mich für weitere Hilfe wenden kann.													HZ4
LZ18	Ich kann Weiterbildungsangebote aus der GEIGER-Umgebung nutzen.													HZ4
LZ19	Ich kann mit Kolleg:innen und Fachpersonen Cyberrisiken und Zwischenfälle in unserem Betrieb diskutieren.													HZ5
LZ20	Ich kann mit Kolleg:innen gängige Verhaltensweisen zur Cybersicherheit erläutern.													HZ5

Figure 14: Learning Objectives related to basic cybersecurity measures in MSE environments (in German).

The competences described in Figure 14 mainly cover basic cybersecurity measures in MSE-environments defined by the GEIGER curriculum and aligned in the prescribed format. It further covers basic knowledge on how to use GEIGER, i.e., the toolbox and self-regulated learning features. Further, the scheme covers communication about cybersecurity with colleagues.

BBB as educational institution is currently planning on providing learning materials as Open Educational Resources that can be exploited for the purpose of GEIGER. Provided learning content will be adapted within the learning features, and further learning materials such as presentational slides etc.

The course provided by ICT Berufsbildung may serve as basis for the GEIGER course on level 3 and 4, covering the curricular specifications. GEIGER-specific learning content will have to be added.

3.1.2 Planning M19-M30

In a next step, the comprehensive curricular scheme adaption for Level 3 will be designed and implemented. Also, ICT Berufsbildung Schweiz will be involved as a stakeholder in GEIGER validation to pave the way for recognition and inclusion of the Security Defenders education in their educational standard.

3.2 C2 Open GEIGER API for Interoperability with Cybersecurity Tools

The definition and standardisation of the GEIGER API for cybersecurity tools will allow GEIGER to expand monitoring and protection capabilities through interoperability with sensor and shields offered by third-party vendors of cybersecurity tools. With such an Open API approach, GEIGER will be able to tap into the 10 billion € spending in cybersecurity and offer vendors in that market a channel to reach relevant SMEs with the vendor-offered sensors and shields.

No already existing clearly applicable standard could be identified for designing and implementing the interoperability by cybersecurity tools that would allow the exchange of sensor data and recommendations. Hence, GEIGER aims at developing an own open API and obtaining the support for it by stakeholders, including important tools providers.

3.2.1 Achievements M7-M18

GEIGER has designed and implemented a proof-of-concept version of the GEIGER API as part of the GEIGER integrated prototype. The API covers the declaration of sensors provided by a tool being integrated into the GEIGER Framework, the exchange of sensor values, the declaration of recommendations supported by the tool for improving the sensor values, the launch of the tools within such a recommendation context, and the setting of tool configuration. The detailed documentation of the GEIGER API is provided in D2.2.

Also, GEIGER has started to disseminate the GEIGER API to win supporting cybersecurity tools providers. More than 16 external tools providers have registered their interest to join webinars about the GEIGER API and participate in a Hackathon for connecting their tools to the GEIGER framework ("Connectathon").

3.2.2 Planning M19-M30

In a next step, the GEIGER API will continue to be validated with the cybersecurity tools included in the GEIGER consortium as part of WP4. The lessons-learned and feedback will be used to mature the design and implementation of the GEIGER API as part of WP2.

Also, a webinars series will be launched in WP5 allowing interested cybersecurity tools providers to get more information about the API and how to use it for interoperating with the GEIGER platform. The webinar series will culminate in the Connectathon for trying out the API and becoming part of the GEIGER ecosystem. Any feedback and recommendations collected during these efforts will be forwarded to WP2 for further maturing the design and implementation of the GEIGER API.

3.3 C3 Open GEIGER API for MISP-based Interoperability with CERTs

The definition and standardisation of the GEIGER API for cybersecurity tools will allow GEIGER to expand monitoring and protection capabilities through interoperability with sensor and shields offered by third-party vendors of cybersecurity tools. With such an Open API approach, GEIGER will be able to tap into the 10 billion € spending in cybersecurity and offer vendors in that market a channel to reach relevant SMEs with the vendor-offered sensors and shields.

MISP could be identified as a standard for exchanging information with CERTs. MISP allows to specify cyber incidents and indicators of compromise (IOC) in a machine-readable format for information exchange and automated processing. The exchanged data will be used by the CERTs for threat intelligence and by GEIGER as an input for calculating the GEIGER indicator values. GEIGER aims at implementing MISP in collaboration with the partner CERT CERT-RO, the Swiss NCSC for the Swiss use case, and the Digital Trust Center for the Dutch use case.

3.3.1 Achievements M7-M18

GEIGER has designed and implemented a proof-of-concept version of the MISP-based GEIGER API for interoperability with CERTs as part of the GEIGER integrated prototype. The API covers the schema and encoding of incident and IOC information together with examples. Also, the API allows the declaration of a

CERT's taxonomy of security incidents to support translation from and to the GEIGER taxonomy of security incidents. The detailed documentation of the MISP-based GEIGER API is provided in D2.2.

Lessons-learned: during the design and implementation of the MISP-based GEIGER API and the discussions with the currently partnering CERTs, two challenges have emerged.

Firstly, CERTs use differing taxonomies of security incidents, and interoperability depends in the harmonisation of incident categories. To account for the current lack of harmonisation, GEIGER has implemented an internal translation mechanism. The mechanism is inspired by the Morphing Mediation Gateway proposed by the Wise-IoT project[2].

Secondly, Indicators of Compromise (IOC) are a non-trivial concept. Agreement with CERTs is required to scope the analysis of incidents performed and the information captured in an IOC. Each category of compromise may require an individual agreement, allowing adaptation to the information needs of the specific category.

3.3.2 Planning M19-M30

In a next step, the MISP-based GEIGER API will continue to be validated with the CERTs partnering with the GEIGER project as part of WP4. Within WP5, the GEIGER partners and the partnering CERTs will continue their dialogue on specifying IOCs that are of high interest for GEIGER and the CERTs. As part of WP2, the design and implementation of the API will be adapted to support the agreed IOC categories.

Also, GEIGER will initiate the dialogue with the Computer Incident Response Center Luxembourg (CIRCL) who are the developers and maintainers of the MISP standard. The meetings have been agreed with CIRCL. The scope will be to address the challenges encountered by GEIGER in the adoption of the MISP standard and exploring opportunities to contribute back to standardisation by drawing on the MISP-based GEIGER API implementation.

3.4 C4 Protection of MSEs whose Business depends on Social Networks and Cloud-based Services under non-European Ownership

As detailed in D5.1, the use of foreign social networks and cloud-based services implies risks for SMEs. SMEs that depend on social networks and cloud-based services are exposed to the threat of blocking or deletion of her accounts and the consequent unavailability of data, infrastructure, and funds. There is a need for clear policies regarding how such incidents are to be handled to avoid negative impacts on the business of the concerned SMEs and ensure compliance of these SMEs with the GDPR and other applicable laws

3.4.1 Achievements M7-M18

GEIGER has drafted a policy brief that describes the account blocking threat experienced by the SMEs. Figure 15 shows the draft. The policy brief has been submitted to the Research Executive Agency of the European Commission and presented at the P2PKOS project-to-policy kick-off seminar on March 22-23, 2021.

[2] http://wise-iot.eu/wp-content/uploads/2017/03/D2.4-Semantic-Interoperability-Components-R1-1.0.2.pdf

European Commission

Digital Security

At a glance

Title: GEIGER Cybersecurity Counter
Type of action: IA
Topic: SU-DS03-2019
Grant Number: 883588
Total Cost: 4'739'716.61
EC Contribution: 3'999'162.50
Start Date: June 01, 2020
End date: November 30, 2022
Duration: 30 Months
Project Web Site: www.cyber-geiger.eu
Key Words: Cybersecurity, Micro and Small Enterprises (MSEs), Awareness, Risk Assessment, Security Defenders Education, MSE Support Ecosystem

Project Coordinator: Samuel Fricker
Project partners:
Fachhochschule Nordwestschweiz (FHNW)
Universiteit Utrecht (UU)
Fores Media Ltd (TECH.EU)
Kaspersky Lab Italia Srl (KSP)
Pädagogische Hochschules Freiburg (PHF)
Mintimage EURL (MI)
SOMEKH CHAIKIN Partnership (KPMG)
Stadt Baden (BBB)
ATOS IT Solutions and Services Iberia SL (ATOS)
Schweizerischer KMU Verband (SKV)
Haako GmbH (HAAKO)
Centrul National de Raspuns la Incidente de Securitate Cibernetica (CERT-RO)
Asociatia Cluj IT (CLUJ IT)
E-ABO GmbH (E-ABO)
Braintronix SA (SCB)
Public Tender SRL (PT)
Semenwerkende Registeraccountants en Accountants Administratieconsultenten (SRA)
Bartels Loredana (CL)

GEIGER

The challenge

>24M European micro and small enterprises (MSEs) process private data and are not prepared for cyber-attacks. The scale, value, and sensitivity of personal data in the cyberspace are increasing, and citizens are uncertain about who monitors, accesses, and modifies their personal data –with consent or by attack as a result of breach.

Project Objectives

- To develop an easy-to-understand security indicator reflecting the risk level of an MSE or a community thereof.
- To develop an open toolbox with recommendation, protection, and education tools adapted to MSEs.
- To develop an information security and analysis platform connecting MSEs and their competent CERTs.
- To initiate and develop an education ecosystem, where competent security defenders can help MSEs

Concept and approach

Expected Results – indicate TRL if applicable

- GEIGER Framework, incl. ISAC platform and MSE toolbox: TRL7
- Security Defenders Education Ecosystem at TRL7

Target end users

- 100K MSEs that lack cybersecurity and data protection skills and emotionally cope with that lack
- Associations wanting to improve cybersecurity and data protection among their member MSEs.
- Apprentices (vocational training), entrepreneurs, and accountants wanting to help MSEs
- CERTs/CSIRTs wanting to disseminate recommendations for new threats, while understanding the MSEs community better
- Security and data protection tool developers wanting to reach and better service MSEs

Main project events

CPDP 2021, Trinational Cybersecurity Days 2021, Cybertech Europe 2021, Cluj Innovation Days 2021

Research Executive Agency

RECOMMENDATIONS

N/A at this stage.

GENERAL SCENE SETTER

Europe's 25 million micro and small enterprises (MSEs) are not sufficiently protected against negligent behaviour and malicious cyberattacks. More than half of MSEs experience breaches or attacks, and more than half of those that are severely hacked are forced to close within six months. This problem is significant as they represent almost 90% of European enterprises. Besides the relatively few digital enabler start-ups, the large group of digitally dependent and digitally based MSEs are confronted with that problem. GEIGER works with these MSEs and collaborates with CERTs/CSIRTs to raise awareness and with vocational schools and professional associations the create capacity for helping these MSEs.

The GDPR guarantees access, rectification, erasure, and portability rights for data subjects. Micro and Small Enterprises (MSEs) use social networks and cloud services managed under jurisdictions outside the EU to store and process personal data from customers and users. Network and cloud service operators block MSE accounts for diverse reasons but continue to process the data. This "account blocking" hinders the intermediary MSE to comply with the data subjects' rights. The operators' use of non-European courts is a blocking barrier for the MSE wanting to settle a conflict. Most MSEs in that position cannot comply with the GDPR and face massive business risks as a consequence.

The GEIGER project aims at working with 100'000 MSEs during the project lifetime. The work at this scale enables surveys to know the prevalence of issues like the account blocking problem and understand the perception of the MSEs about potential solutions. The GEIGER project is interested in collaborating with P2PKOS and open up the work with the GEIGER MSE community. GEIGER looks forward to formulating and helping disseminate a policy brief with clear recommendations.

THE MAIN TEXT

The GEIGER project has observed the account blocking problem while eliciting requirements from the MSEs. Most MSEs exchanged personal messages and photos with customers using leading social networks and messengers. Other MSEs used cloud services to collect and manage payments from her customers. The MSEs experiencing account blocking did so due to diverse reasons. Some, for example, due to false denouncements, trolls, or imperfect monitoring algorithms, others due to forgotten passwords in combination with changed branding. The lack of legislation that would have protected them implied no clear way for resolving the situation and being forced to give up the case with acceptance of non-compliance and painful business impact.

A technical solution is unlikely to resolve the problem of being prevented from executing the data subjects' right for data access, rectification, erasure, and portability. For that reason, the GEIGER project proposes to contribute to the development or adaptation of a policy framework imposing obligations on social network and cloud operators, while offering the rights to European MSEs necessary for avoiding and mitigating the account blocking problem. One recommendation could be to extend the GDPR framework with the right to backup data stored in the social network or cloud service.

POLICY IMPLICATIONS

Elements added to the GDPR should be targeted to shape adequate rights and obligations of MSEs as intermediaries between the data subject and the storage provider and processor. Ways would need to be found to guarantee access to data so that the GDPR guarantees can be executed even in the face of conflicts between parties in the data value chain. GDPR court cases should be monitored to understand the conflict constellations and understand ways to settle them.

We consider the debate among stakeholders and the public as well as the organisation of a co-ordinated approach to adapting regulations to be essential in addressing the challenge. The benefit will be a massive risk reduction for micro and small enterprises and improved compliance with the rights of data subjects.

CONCLUSIONS

N/A at this stage.

Research Executive Agency

Figure 15: Policy Brief concerning the account blocking threat experienced by SMEs that use non-European social networks and clouds.

3.4.2 Planning M19-M30

In a next step, GEIGER will collect the opinion of SMEs that participate in the GEIGER trials concerning the account blocking threat. The SMEs' judgements and recommendations will be used to conclude the policy brief that will be submitted in its final form to the Research Executive Agency of the European Commission.

3.5 C5 SME Guide on Information Security Controls

The recommendations offered by the ISO 27K standard are closely related to the risk-reduction recommendations offered by GEIGER to SMEs. ISO 27K-based recommendations have been selected and adapted for SMEs in a joint effort by the European Digital SME Alliance and the Small Business Standards SDO. GEIGER was joining this effort, contributing as a with the in-depth expertise that was developed during the project work so far. The resulting SME Guide will offer an overall 27K-based framework within which the GEIGER risk-reduction recommendations will be positioned.

3.5.1 Achievements M7-M18

GEIGER has contributed to the SME Guide on Information Security Controls. The guide has been approved by standards workgroup of the European Digital SME Alliance and Small Business Standards. This marks the successful conclusion of the work on C5.

3.6 C6 SME Classification

The classification of SMEs in categories that allow differentiating cybersecurity support needs of these SMEs will allow GEIGER to target SMEs with specific dissemination actions and value propositions. The empirical work on cybersecurity in SMEs performed by GEIGER allowed to better understand the factors that explain SMEs' cybersecurity needs and identify limitations of current classification schemes. Based on this background, GEIGER joined the Digital SME Alliance in establishing a refined classification scheme that is easy to measure and is effective in separating important classes of SMEs that require different cybersecurity support activities.

3.6.1 Achievements M7-M18

GEIGER has initiated collaboration with the European Digital SME Alliance concerning the classification of SMEs. Several online meetings have been performed for identifying relevant taxonomies and statistical work.

3.6.2 Planning M19-M30

A workshop, survey, and public event are planned for publishing a refined classification of SMEs that are useful for digitalisation in general and cybersecurity in particular.

3.7 C7 Open GEIGER API for xAPI-based Interoperability with Education Tools

The definition and standardisation of the GEIGER API for education tools will allow GEIGER to expand capabilities for raising awareness and training employees with educational tools offered by third-party vendors, including Cyber Ranges. With an Open API approach, GEIGER will be able to expand its offering and allow tool vendors to reach relevant SMEs with their offering. The GEIGER consortium found the xAPI standard adequate to implement this aspect of the GEIGER API.

To allow for interoperability of the GEIGER Toolbox with the different training features included in the GEE (e.g., online tasks for single learners or courses from different educational institutions), the competences of the full GEIGER curriculum are written in form of (minimized) xAPI-statements. xAPI is a meta-data-model for tracking learning achievements of a particular learner independent of learning contexts (traditionally such models, e.g., SCORM, focus on learning objects within specific learning management system).

A complete xAPI-statement usually consists of:

'actor'	'verb'	'object'	'result'	'context'
i.e. the specific learner	e.g. what the learner has done with a learning object	e.g. a learning object or objective	e.g. a score in concern of a learning object	e.g. the learning situation or a curricular reference

For the purpose of outlining the GEIGER curriculum, the statements are minimized to: 'verb' and 'object', assuming the 'actor' as the specific learner within the MSE and 'result' and 'context' as information, that might be collected within specific contexts and tools. An xAPI-statement within the GEIGER curriculum thus might e.g., comprise:

- <verb> = 'installed'
- <object> = 'anti-malware application'

These two elements present the actual learning objective, i.e. the targeted competence, usually consisting of an operator and a subject matter. These minimized statements can thus easily be translated into other curricular formats. Thus, this Cybersecurity Curriculum for MSEs provides the opportunity to be exploited on a larger scale, i.e., fill the salient gap yielded by neglecting the dominance of IT-lay persons in MSEs (see also https://doi.org/10.1145/3465481.3469198).

3.7.1 Achievements M7-M18

The xAPI statements within the curriculum have been finalised. Also, the design of the xAPI-based GEIGER API has been drafted and made available to the GEIGER partners that develop and integrate learning tools into the GEIGER framework. The detailed xAPI statements are reported in D3.2, the definition of the API in D2.2.

Also, the GEIGER consortium has initiated contact with the xAPI community, in particular with the organisations Advanced Distributed Learning (ADL) who coordinate the community and Rustici Software, a key developer of the xAPI standard. In these discussions, GEIGER informed about the adoption of the xAPI and agree on an agenda for sharing lessons-learned and contributing back to the xAPI standard. More details on the dialogue is provided in D3.2.

3.7.2 Planning M19-M30

In a next step, learning tools that are available within the GEIGER toolbox will be adapted to implement the xAPI-based GEIGER API within WP2 to ensure a standardised reporting of learning data, also when interacting with Learning Management Systems such as Moodle. The presentation of the xAPI-based GEIGER API will be included in the webinars series for tool vendors that are interested in joining the GEIGER ecosystem.

Within WP4, the API will be used for validating the interoperability between the GEIGER framework and the learning tools. The trials will include the Connectathon planned for testing interoperability with third party tools. Any lessons-learned and recommendations will be fed back to WP2 for planning the evolution of the API.

Also GEIGER agreed with ADL and Rustici to continue the dialog on lessons-learned with xAPI and explore opportunities to contribute back to standardisation with recommendations.

3.8 Management of key success factors and risks

The table below gives an overview of the KPIs linked to standardisation and liaison with policy, their status at M18, as well as the key actions and explanations on their operationalisation.

KPI	Description	Status at M18	Key actions & explanation on operationalisation
I2.1.2.8	1 open API with API access governance policies for querying	2 open APIs implemented (alpha)	Open GEIGER API for cybersecurity tools: alpha version implemented, being validated.

	incidents and submitting information	1 open API designed	Open GEIGER API for MISP-based interoperability with CERTs: alpha version implemented, in discussion with CERTs Open GEIGER API for xAPI-based interoperability with education tools: design specified. Development and validation continue as part of WP2 and WP4. First public availability of the APIs planned for the connectathon (part of Launch Party). Final release planned for period M25-M30.
I2.1.2.9	4 contributions to standardisation work or Memorandum of Understandings with related initiatives for harmonising external GEIGER Framework interfaces and the security defenders education. ≥2 contributions to standardisation	5 standards-related activities ongoing 1 policy-related activity ongoing	Security Defender Curriculum: alpha version being validated under the observance of standards defining organisations ICT Berufsbildung Schweiz and Coiffure Suisse. Submission of contributions planned for period M25-M30. SME Guide on Information Security Controls: contributions submitted to Small Business Standards. Standard is being finalised. SME Classification: Submission of contributions planned for period M19-M24. MISP Contributions: Dialogue ongoing. Submission of contributions planned for period M25-M30. xAPI Contributions: Dialogue ongoing. Submission of contributions planned for period M25-M30. 1 draft policy brief submitted to REA. Final version planned for period M25-M30.

Table 10: KPIs linked to T5.2

3.9 Summary and Conclusions (FHNW)

The activities related to standardisation and liaison with policy have progressed according to plan. The technical work of WP2 and WP3 benefit from the identified standards. There are good opportunities to strengthen GEIGER results via contributions to standardisation. KPIs will be met, respectively are expected to be exceeded.

4 T5.3 Exploitation Planning

The exploitation plan in the GEIGER project refers to the utilisation of results in further research and innovation activities, other than those covered within the timeframe of the GEIGER project, in developing, creating, and marketing a product and providing a service, and in standardisation activities.

In this respect, we have considered as possible exploitation activities the followings:

- Transfer of GEIGER results in a start-up using a Joint Venture model, and run a disruptive business (the intended main line for exploitation)
- License trade secrets within the GEIGER project to third parties in the case the first activity will not succeed (contingency plan)
- Sell some results to a third party to integrate into its technology (contingency plan)
- Transfer of know-how in consulting programs for SMEs /MEs (e.g., Cluj IT, BBB, etc.) (diversification plan)
- Transfer of know-how in training programs for SMEs /MEs (e.g., Cluj IT, FHNW, PHF, UU, etc.) (follow up and consolidation plan)
- Integrate some results within technologies developed by the technical partners in the project (e.g., ATOS, MI, etc.) to enhance their own solutions (in the frame of IP, strategic partnership plan in relation with the main line of exploitation)
- Use cyber-GEIGER by partners (follow up and consolidation plan)
- Publish in scientific papers (diversification plan)
- Use in academic education (e.g., FHNW, PHF, UU, etc.) (follow up and consolidation plan)
- Use in future research (follow up and consolidation plan)

- Transfer of know-how to create or improve standards (e.g., FHNW, Cluj IT) (diversification plan)

We have also started the process to define an IP exploitation agreement to stipulate what and how the aggregated results (e.g., GEIGER toolbox, know-how generated by other partners, etc.) can be used by each partner at the end of the project.

4.1 Exploitation Planning Roadmap

The roadmap for exploitation planning and management considers the innovation methodology adopted in the project. Because we confront with a disruptive innovation in the GEIGER project, the lean innovation methodology was adopted.

According to this methodology we consider that users must be part of the co-creation process from the very early stages of solution design and development. In this respect, specific actions have been considered from the first six months of the project, within WP1, which is responsible with the definition of requirements. Further, end users must be involved in the value proposition design and testing. This happened in several iterative sessions, organised online. The beta result is shown in *Figure 8*. It put the basis for testing to a wider set of end users. The strategy is to test in the three GEIGER use case countries in the first phase of calibration. For piloting, the first country was Romania. It will be followed by the tests in Switzerland and the Netherlands.

In Romania, we used the survey approach, contacting end users via our multiplier partners. From 300 SMEs we contacted, 35 (approximately 10%) provided feedback. Conclusions are positive, meaning that companies showed interest in the GEIGER solution. This early test is also important to indicate the potential size of the local market. In this respect, for Romania, considering the early promoter test completed through the survey, we would count on 50.000 small businesses to be future customers of GEIGER. Our expectations are higher in the more developed countries, such as Germany, Switzerland, the Netherlands, Belgium, France, and Spain.

The figure below explains the Beta version of the value proposition.

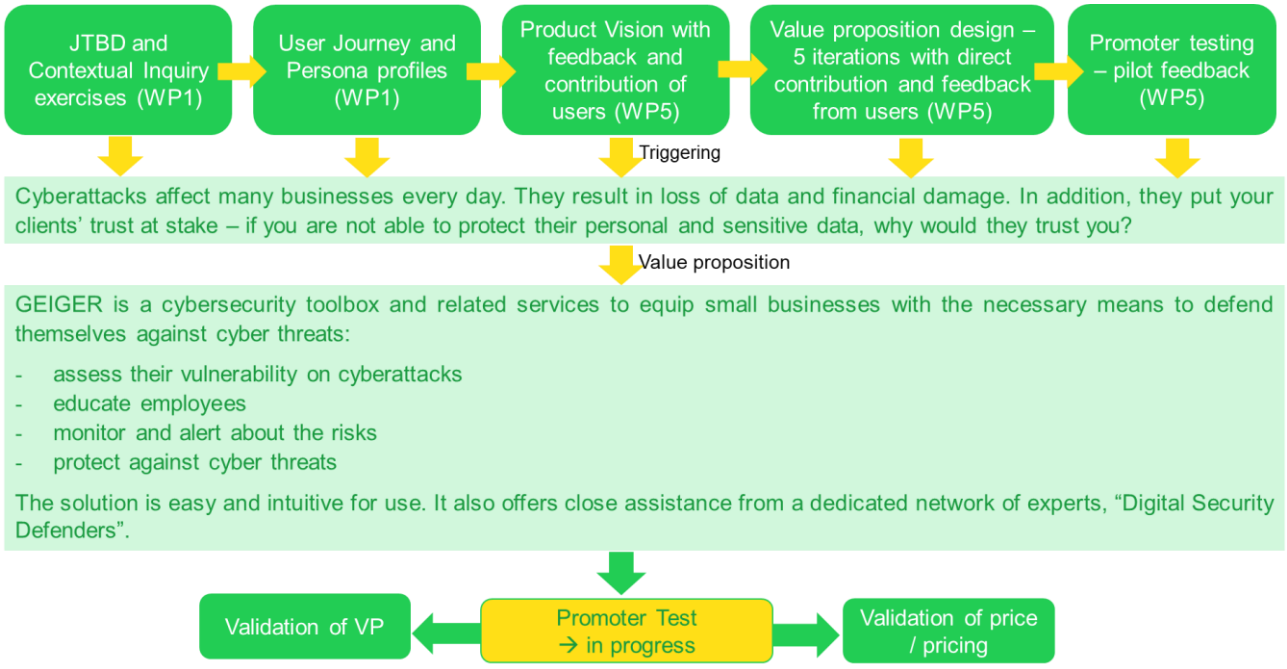

Figure 16: Beta version of the value proposition

The value proposition and actions have been also tested with five expert product managers who operate in the USA market. The feedback was very positive, but with a recommendation to simplify the current vision statement ("*To create an affordable, super-intuitive, rapid and easy customizable solution for tool-assisted cybersecurity assessment, training, and protection of digitally dependent or digitally based micro-enterprises from any sector of activity*"). We have also tested with these experts the main values, obstacles, methods, and metrics.

The roadmap for actions related to exploitation planning is shown in the Figure below.

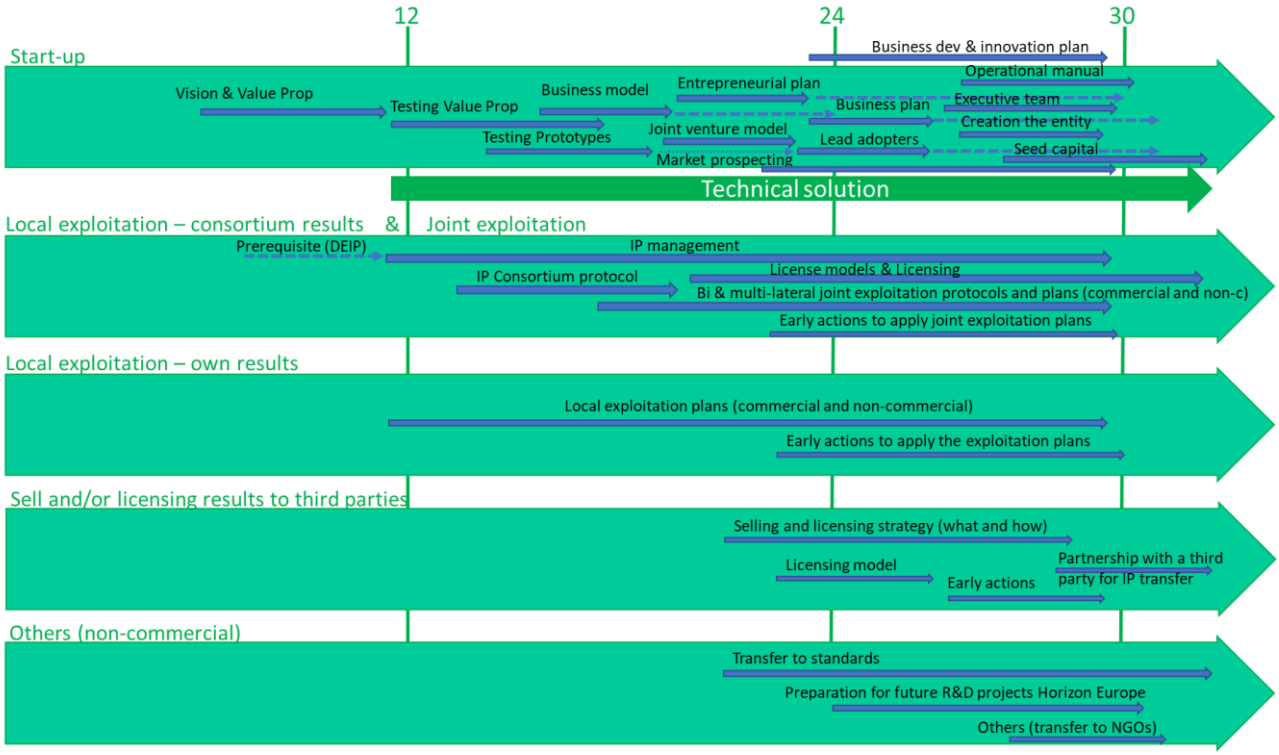

Figure 17: Roadmap for exploitation planning

As the roadmap indicates, in order to increase the chances for technology transfer to the startup (spin-off), several actions must be undertaken much earlier than they are usually considered in the traditional models. WP4 will be responsible for testing various versions of the solution (prototypes) in order to provide feedback on user experience and functionalities. However, this is not sufficient, because the startup's success will count in equal measure by the effectiveness of the business model associated to the startup.

4.2 Agreements and Documents

4.2.1 Joint Venture Agreement

Discussions we conducted during M15-M17 with experts in innovation management, including those from AT Kearney through Horizon 2020 Booster Programme, indicate that we need to set up a clear IP exploitation agreement and an early identification of the partners that want to join the business initiative after the end of the project.

The investigation we did in the first half of 2021 indicated that partners in the consortium are mostly focused on local exploitation (see *Table 10*). Therefore, we have started to prepare a model for joint venture agreement, as well as a model for IP exploitation agreement. Both documents are crucial for the next demarches to set up the startup. The draft versions have been discussed in an internal meeting with the consortium members, but the process is still at the beginning. It was concluded that a dedicated retreat must be organized to clarify all aspects related to the startup foundation. This action will be scheduled for the beginning of 2022, possibly combined with the retreat with an academic focus (see *2.2.5.5 Scientific publications*). We have also identified a potential consultant in IP management to assist the consortium in preparing the final forms of the two documents.

The table below presents the results of the first iteration to collect expressions of interest for the exploitation of the results of the GEIGER project within the consortium. We have started since May 2021 to collect data about IP from the consortium members. This process will be open until the end of the project, because the most consistent results that will be subject to IPR will be generated after M18. A clear proportion of IP from each partner cannot be valued at this phase of the project. Because this process is crucial, the task force

created in the project to deal with start-up foundation will start to investigate partners about their interest to join the start-up, and in which form. It has established a meeting in the first part of February 2022 with the purpose to fix this issue.

Member	IPR (patents). In the case you can report some results about patenting please provide details in the line "Others:"	Release of feasibility demo or prototype. In the case you have a positive answer, please provide details in the section "Others:"	Did you already release in the project a product, a service, a new process, a new method? Provide details for any of the cases, if available.	Innovation introduced in your organization. Innovation means new products, new practices, new processes, new services, new business models, new technologies, etc. Please provide details in the section "Others:" [if applicable]
Cluj IT	No application, no intention to apply	No release, no intention to release	No	We introduced the MIRO platform for internal working sessions in various projects.
haako gmbh	We did not apply for patents in relation to GEIGER	We are a use case partner and do not "build" anything on our own	No	We plan to adopt GEIGER, but no internal innovation
Montimage	We expect to apply in the future for patents in relation to GEIGER; End-point protection and user control	Going to release a prototype to the end of the project; going to release a feasibility demo to the end of the project 1) cyber-range related to phishing emails; 2) vulnerability scanning tool based on Kaspersky SDK	1) MMT-IDS; 2) Pentesting service (part of security audit)	We already introduced in our organization innovations in the context of GEIGER; 1) support the computation of the global risk indicator; 2) train professionnals using cybergames
Coiffure Loredana	We did not apply for patents in relation to GEIGER	Haven't published anything yet	No	We intend to introduce innovations in our organization as a result of GEIGER
e-Abo GmbH	We did not apply for patents in relation to GEIGER	Not applicable	No	No
PHF	We did not apply for patents in relation to GEIGER	Release a protoype to this moment in relation to GEIGER	Curriculum based on xAPI (advancement against SCORM)	n.a.
Kaspersky	We did not apply for patents in relation to GEIGER	Going to release a prototype to the end of the project; going to release a feasibility demo to the end of the project	No	We intend to introduce innovations in our organization as a result of GEIGER
BRAINTRONIX SA	We did not apply for patents in relation to GEIGER	No	No	Keeping a closer watch over the cyber-security in our organization and thoughts of improvement
Atos	We did not apply for patents in relation to GEIGER	Going to release a feasibility demo to the end of the project - According to the needs of the project we can release a demo of the risk assessment functionality	No	We intend to introduce innovations in our organization as a result of GEIGER
Public Tender Srl	We did not apply for patents in relation to GEIGER	No	No	We will use the results of Geiger
Utrecht University	We did not apply for patents in relation to GEIGER	We released a protoype to this moment in relation to GEIGER, We are going to release a prototype to the end of the project	GEIGER Indicator algorithm; GEIGER Validation method for Software Solutions	No not in our organisation
SKV Schweizerischer KMU Verband	We did not apply for patents in relation to GEIGER	No, not applicable	No, we didn't	We intend to introduce innovations in our organization as a result of GEIGER

BBB	We did not apply for patents in relation to GEIGER	We are going to release a feasibility demo to the end of the project, cyber security defender course	No	We intend to introduce innovations in our organization as a result of GEIGER, We try to implement the cyber security defender education into the curriculum of computer scientist apprentice and as a optional topics course for all of our apprentices.
SRA	We did not apply for patents in relation to GEIGER	Yet to be decided	No	We intend to introduce innovations in our organization as a result of GEIGER
KPMG	We did not apply for patents in relation to GEIGER	The modules and functionalities to be developed by KPMG will be part of the overall project prototype to be developed until the end of the project.	Not yet, modules will be developed essentially during during the next period of the project.	We intend to introduce innovations in our organization as a result of GEIGER, 1. Incident Reporting tool for SMEs&MEs and initial cyber threats identification and data protection/privacy risks assessment based on chatbot communication with the SME&ME. 2. Security Information Exchange tool to exchange information with CERTs/CSRITs. 3. Improved identification capabilities for risks, threats and potential compliance issues in an SME/ME ecosystem.
Tech.eu	We did not apply for patents in relation to GEIGER	We aren't going to release a prototype or a feasibility demo	No	We intend to introduce innovations in our organization as a result of GEIGER
CERT-RO	We did not apply for patents in relation to GEIGER	No	No	We intend to introduce innovations in our organization as a result of GEIGER

Table 11: The first iteration for collecting expressions of interest for exploitation

4.2.2 Mutual NDA

Mutual non-disclosure agreement (NDA) is an important IP management document. Because in the meetings we intend to organise in the next period for establishing the strategy of the future startup, a mutual NDA will be signed by participants. This is related to the good practices, such that to consolidate the confidentiality related to any critical issue of the business success.

4.2.3 Code of Honour

The code of honour is an additional document to the mutual NDA, to strengthen the IP management framework. The draft model of this code is elaborated. All documents and related actions are intended for early institutional construction of the transfer of results. They will polish the communication and will indicate the clear commitment for moving forward with the GEIGER innovation. This institutional construction is also necessary for future discussions with potential investors or partners.

4.3 Business model

Business model is one of the most important pieces for successful technology transfer of the GEIGER's results into a start-up. To design an appropriate business model, we have tested in two stages the psychological price in a pilot market (Romania). This could be considered a reference, being an emerging market. Tests have been done with a "theoretical prototype" described in terms of key jobs to be done. The first test indicated a reference price of 200 euro as annual subscription. The second test, more elaborated, indicated a reference price of 170 euro as annual subscription.

A wider pallet of business models for digital innovations have been analysed and discussed with experienced product managers from USA. A freemium model, even if very popular, was not recommended by experts because it has less than 10% level of attrition. They indicated that instead, a free trial model of 14-60 days

would be more successful, followed by a customised approach for pricing. For pricing and monetisation, also some other business models were analysed.

The conclusion is the start-up will have to run more business models that address different services and different customers and end-users, such as advertising, subscriptions, marketplace, transactions, razor-razor blade, micro-transactions, and XaaS. The are several major findings up to this date in terms of value perception by customers of the GEIGER solution. They indicate that a simple model cannot work. The model which will be investigated and detailed is an original one, called "outcome-driven business model", which takes elements from XaaS, razor-razor blade, marketplace, subscriptions, and advertising.

Up to this date, we have elaborated the first draft of the business model. The beta version for consultation will be released in early December 2021.

4.4 Action Plan

4.4.1 Booster Programme

H2020 Booster Programme was accessed by the GEIGER consortium. We activated the programme in October 2021. The consulting team comes from AT Kearney, and two meetings with them already took place. The first one was directed towards calibrating our expectations from the experts. The second one was an applied meeting, where the first indications were delivered. The third meeting is scheduled for December 2021.

We have collected valuable information from former similar cases in terms of the exploitation of the project results and the establishment of a start-up, including where our focus should be, where and how to tackle the location for the future start-up, as well as which must be the priority actions.

4.4.2 Accelerated GEIGER spin-off launch

To accelerate the launching of the GEIGER start-up/spin-off, we concluded that various actions must be undertaken much earlier than typically in traditional research projects. We have tested the GEIGER with some venture investors and open the door to attend a pitching event in early December 2021 in Helsinki. Based on this experience, to which will be added other conclusions from the design of business model, and from other lessons learned (and already documented) from different previous pitching contexts, we are going to work out the materials for early pitching of GEIGER and for aligning the GEIGER solution with the business model. It will be a spiral process of prototyping-testing-evaluating-learning-refining.

4.5 Summary and Conclusions

The preparation for exploitation was accelerated relative to the scheduled program. This was indicated by the lean innovation model we have adopted. The decision was good because the pilot tests showed the need to calibrate the initial hypothesis.

From a focus on differentiation by technology (e.g., GEIGER indicator), the focus must move on the business model, and the construction of a novel ecosystem, supported by technology, but with a strong niche on market education and activation of non-consumers or less-demanding consumers into mid-end consumers.

The next phase will cover the clarifications of involvement for each consortium's partner, foundation of the business model and its calibration based on internal and expert feedback, activation of end-user testing of the technical solution, and investigation of the potential customers about the value perceived from the proposed business model. We are ready to further adjust the business model based in the feedback. We also foresee the need to add new functions into the technical solution because of the constrains or requests imposed by the business model. Participation to pitching events, investigation of possible locations for the start-up, finalisation of signature of documents for IP exploitation and management in relation to the startup by stakeholders are other actions for the next three months (M19-M21).

5 Conclusion

In this Intermediate Impact Report, we presented the status of the implementation of the project's dissemination and communication plan, as well as the planning to reach the desired impact through efficient and purposeful dissemination activities. We also gave an overview already given and expected contributions to standardisation and policy definition, as well as the roadmap and action plan towards the long-lasting impact beyond the duration of the project that we aim at achieving by the sustainable exploitation of the project results and the rollout of GEIGER across Europe.

This deliverable D5.2 guides the WP5 work during the next phases of the project. D5.2 is the second deliverable for the dissemination, standardisation, and exploitation planning activities of the GEIGER project. The plans will keep evolving throughout the project's remaining lifespan and will be updated and adjusted on a regular basis with any new relevant outcomes that may impact our dissemination and communication, standardisation, and exploitation planning strategies. The outcomes achieved by executing these strategies will be documented in the third and last deliverable of this work package, D5.3 Final Impact Report (M30).