The Cybersecurity Hub
Interacting globally, acting locally

This is a submission to secure the funding for the establishment of a Cybersecurity Hub. The Hub will contribute to developing a more skilled, more diverse cybersecurity workforce through improved collaboration between business, industry, tertiary and social sectors.

Executive summary

Combatting cybersecurity risks is a challenge shared by administrative, business and social sectors. Cybersecurity threats, attacks and breaches continue to increase in both volume and seriousness, and the gap between supply and demand in the cybersecurity workforce appears to be growing. This critical gap is being tackled in many different ways, from a rise in the number of tertiary institutions providing cybersecurity training, innovative awareness raising initiatives and multi-factor security authentication procedures for consumers, to a growing recent trend in industry to develop its own short courses for school leavers in order to bypass ineffective tertiary educational channels.

The Internet Standards, Security and Safety Coalition (IS3C), a United Nations Internet Governance Forum Dynamic Coalition, is taking a proactive, multi-faceted approach in addressing this challenge, by conducting research into the underlying causes of the gap in the supply and demand of skills and promoting greater awareness and understanding of existing cybersecurity standards. Given the multi-dimensional nature of cybersecurity, an essential first step is to bring together the stakeholders from across a wide range of sectors to develop an integrated strategy based on common goals, and to exchange knowledge, experience and practice. This is the primary purpose of the proposed IS3C Cybersecurity Hub which would function as a coordination centre for research and capacity building, and as an observatory to identify emerging challenges and new skills and knowledge requirements, and to develop the means for scaling up good practice.

The establishment of the Hub will be conducted in 3 phases. This document describes in detail the first phase, for which we are currently seeking financial support. In this phase, we plan to:

1. Undertake outreach to strategic partners worldwide to create a core advisory;
2. Create an online presence for the Hub;
3. Set the parameters for research into the curricula and outputs of tertiary institutions using a methodology based on a SWOT (Strengths, Weaknesses, Opportunities, and Threats) comparative analysis;
4. Develop an integrated strategy for the subsequent phases of the Hub's development;
5. Develop a risk mitigation strategy to ensure the sustainability of the Hub;
6. Final report and presentation.

In the second phase, the outreach programme will be broadened and consolidated, to attract new multi-stakeholder partners and reinforce visibility of the Hub within and beyond the IGF community. An observatory mechanism will be set up for the promotion and scaling up of good practice, with regular news briefs to inform and engage stakeholder members. Through the observatory, members will be able to share knowledge, experience and resources, making it easier for the tertiary education sector to find authentic learning resources to respond to the needs of their students and the ever-evolving needs of the cybersecurity sector.

In the later phases, the focus will turn to other levels of education, from early primary school upwards. One overarching aim of the Hub is to create more opportunities for children, as the youngest digital technology users, to become cyber secure by becoming more aware of technology-related risks and acquiring the necessary knowledge and skills to avoid or overcome those risks.

Table of Contents

Contribution of the Cybersecurity Hub to Sustainable Development

Within its first two years of operation, the Hub aims to make online courses available to a broader population in communities where tertiary cybersecurity education is not readily accessible or non-existent. The aim is not to reinvent the wheel but to repurpose and promote existing resources, contributing at the same time to achieving more diversity in the cybersecurity workforce. In this way, the Hub will contribute to the achievement of several of the UN's sustainable development goals such as quality education (SDG4), gender diversity (SDG5), economic growth in under-served countries (SDG8), and reliable infrastructure (SDG9).

Definition of concepts

The IS3C (Internet Standards, Security and Safety Coalition) is a multistakeholder dynamic coalition established under the United Nations' Internet Governance Forum. Its goal is to achieve the widespread, rapid deployment of existing, security-related Internet standards and ICT good practices to make online activity and interaction more secure and safer.

Since its inception in 2020, IS3C has delivered reports on IoT security by design, procurement and supply chain management and has produced two tools assisting experts to achieve positive deployment decisions from their superiors. Currently IS3C is developing guidance on next steps. The coalition's education and skills working group delivered its first report in 2021 (*https://is3coalition.org/docs-category/research-reports*). The overall objective of IS3C is to move from theory to practice, and translating the recommendations from this study into a multi-stakeholder action plan to be widely implemented. This is the goal of The Hub.

The Cybersecurity Hub will bring together IS3C experts and key stakeholder representatives from public, private and civil sectors from across the world to share knowledge and experience and scale up good practice for safer, more secure operation and use of the Internet. It will initially focus on the need for the tertiary sector to get up to speed to fill the growing demand for an efficient, diverse workforce. The Hub aims to improve knowledge of cybersecurity standards, promote meaningful partnerships between industry and tertiary education and encourage the take-up of cyber courses that integrate cutting edge cybersecurity knowledge and are based on ICT best practices.

The concept of IS3C's proposed Cybersecurity Hub has been presented to approximately 100 professionals, first at the 2023 EuroDIG meeting in Tampere, in IS3C's General Meeting in September, then at the 2023 UN Internet Governance Forum (IGF) in Kyoto and launched at the Riyadh 2024 IGF. Discussions with high level officials at these and other meetings suggest that the Hub would be more impactful if it were to work under the aegis of the IGF, as this would provide a neutral platform that would encourage the participation of a broad range of stakeholders.

The Hub will focus on three related aims:

1) Closing the knowledge gap between industry and tertiary cybersecurity education;
2) Raising awareness of career opportunities in cybersecurity amongst the general public, and at all levels of education and professional development;
3) Raising cybersecurity awareness in schools.

The Hub from the stakeholder perspective

Through interactive voting at the 2024 EuroDIG and IGF workshops, 53% of participants approved the key role of the Hub as being *to improve industry-education collaboration*, and 68% saw it as a means to improve *knowledge sharing between cybersecurity and tertiary education sectors.* One in three participants considered that it could also play a leading role in increasing the diversity of the cybersecurity workforce and facilitating mid-career changes.

One in three participants also thought the Hub could support the integration of cybersecurity in school curricula, from elementary school onwards. For almost 20% of participants, a Hub could be instrumental in encouraging cybersecurity-based gamification and simulation, hosting ethical hacking competitions to raise the awareness of the public at large about the importance of cybersecurity and fostering more informed, responsible use of digital technology by all users. For many participants, the Hub can help unite specialists through a common vision and values rather than through common interest, integrating a human rights approach as the basic standard.

Target groups for the Hub's functions

There are three main target groups in the initial development phase of the Hub: the **tertiary education sector,** the **industry-business sector and the Internet technical community.** The needs of, and benefits for, secondary target audiences such as governments, all levels of education, the public at large and SMEs will be analysed in a future IS3C report. SMEs could benefit considerably from the project as they have specific cybersecurity needs but often don't have the budget to meet them.

Tertiary education institutions: For the purpose of this document, this group includes both academia, and learners, i.e. tertiary pre- and post-graduates and/or employees who may be interested in a career shift. In keeping with findings from the initial IS3C study on education and skills, the Hub would improve collaboration between sectors and aim to align tertiary curricula more closely to the real career requirements of graduates to facilitate their entry into the cybersecurity workforce. Examples of good practice from the cybersecurity industry and other tertiary institutions, and a better knowledge and understanding of industry standards, would potentially offer more authentic learning resources to improve the quality of the education on offer. Tertiary institutions could also benefit from knowledge-sharing opportunities with industry, not only to be more rapidly informed about the possible security risks associated with emerging technologies, but also to become test-beds for new tools and techniques.

Awareness raising will be an important function of the Hub, and school leavers and employees looking towards a career shift would benefit from factual, regularly updated information on opportunities in the cybersecurity industry. The Hub could bring them into contact with potential employers in the sector, opening new possibilities for meaningful internships. Awareness raising could also help to overcome the discriminatory bias in the online dissemination of job offers, which is currently hindering the drive for a more diverse cybersecurity workforce.

The **cybersecurity industry** would benefit from a greater, more diverse interest in cybersecurity careers. Statistics show that it is becoming increasingly difficult to recruit staff in this sector. Interviews conducted with specialists in the previous study on the skills requirements of the cybersecurity industry (IS3C, 2022)[1] underline the importance of maintaining a diverse workforce by attracting more women and young people to the field. Improved education in tertiary institutions would raise the knowledge and skill level of trainees and employees, saving industry time and costs spent on the induction of new employees. The Hub would offer industry a privileged link with local or regional tertiary institutions, facilitating interaction with cybersecurity instructors and enabling its input on training modules in specialist or emerging areas, for example, linked to generative AI. Information on specific skills and specialist knowledge requirements could be published through the Hub to improve the reactivity of learning institutions, future-proofing the cursus they propose.

The good practice observatory to be established in the second phase of the Hub's development will aim to gather data on wide-ranging topics, from innovative training to new elements in internships and recruitment procedures. Several interviewees in the IS3C study pointed out the urgent need to find more cost effective internship and recruitment procedures, and this is an area where the Hub could make a considerable difference.

Implementation

Three work packages are foreseen in the initial phase, which ideally start in the first half of 2025.

1. Coordination (2 person months)

The project will be implemented by IS3C's Education and Skills working group (WG2), under the supervision of its chair, Janice Richardson (Luxembourg/Australia) and Vice-Chair Awo Amenah (Ghana), assisted by IS3C's coordinator Wout de Natris. A core Advisory Group will be appointed from the outset, to help **set the Hub's goals, to review progress, and to support the development of an integrated strategy** to guide the creation and functioning of the Hub in its various phases. The Advisory Group, which will contribute to the project on a voluntary basis, will comprise five members from different regions of the world representing the relevant professional sectors (academia, the tech industry, governments, student community and civil society). It will be led by a permanent chair who is not a member of IS3C, to ensure an objective overview. It will meet twice annually, with one online meeting and one meeting at the IGF.

IS3C's Education and Skills working group (IS3C WG2) will continually strive to bring new partners to the Hub and seek funding opportunities, with the support of the IS3C coordination team.

2. Communication (2 person months, plus design, printing and travel costs)

Initially, IS3C members will use their own extensive networks to raise the visibility of the Hub which will be presented on 1 or 2 pages of the IS3C website, managed by the web master of the site. The page(s) will include basic and membership information about the Hub. It will provide access to a survey form on cybersecurity training initiatives, regular news updates, research reports and an information leaflet, which will also be distributed at relevant events. IS3C WG2 will seek opportunities to present the Hub at a minimum of five international events, including but not limited to preparatory meetings for the UN IGF, regional IGFs such as the African IGF, EuroDIG and the Asia-Pacific Regional IGF (APrIGF), and the annual UN IGF event. Media tracking tools and Key Performance Indicators will be used to keep the communication on track.

3. Research preparation (3 person months)

This parameters of the research will be set by the team that completed the initial study in 2021-22 (https://is3coalition.org/docs/study-report-is3c-cybersecurity-skills-gap/), in collaboration with the Advisory Group. To scope the field, interviews will be conducted with at least six tertiary cybersecurity education instructors in different regions of the world. The aim is to define the content and to pilot a survey, to be implemented in phase two. This will incorporate a SWOT-style approach that will be distributed to at least 40 tertiary and vocational education establishments worldwide to analyse curricula, traineeship modalities, graduate employment statistics, etc. Focus will also be on identifying innovation and good practice. Supplementary tools developed by Insight SA in the framework of a research project with the EU agency, ETF (European Training Foundation) will be used as appropriate to enrich the information gathered.

4. Report and workshop (2 months)

A comprehensive report will be prepared to describe progress on the establishment of the Hub, including findings from the research piloting phase, parameters of research to be implemented in phase two and proposing recommendations for next phases. IS3C WG2 and research partners will apply for a workshop at the IGF to report progress on meeting its targets and set out the next steps for the Hub's development and activities.

Risk assessment, risk mitigation strategy

The aim of IS3C is to create a sustainable Hub that will contribute to improving cybersecurity education, in particular to address the growing shortages in the cybersecurity workforce, and the gap between the expectations of industry and cybersecurity courses taught in tertiary institutions. The risks related to conducting the first phase of work described in this document have been rigorously analysed and are listed below.

- **Risk of low interest in participation in the Hub**

The Hub is an evidence-based approach designed to respond to specific needs voiced by industry and education establishments in an IS3C study conducted in 2021-2022. The concept has since been endorsed by specialists attending IGF-related events, professionals in other IS3C working groups and participants attending a webinar organised by IS3C in May 2023. It has been discussed with members of the National Cybersecurity Coordination Centres set up within the EU. The level of interest has therefore been validated, and formal agreement from key stakeholders will be gathered during this initial phase of the project.

- **Risk of insufficient number of partners joining the Hub**

A period of one year has been foreseen to prove the potential impact of the Hub, during which we will implement outreach strategies to potential partners. The number of activities undertaken in year 2 and 3 will directly depend on the number of paying partners who subscribe. To date, most of the work has been on a voluntary basis, and there is a readiness to continue their work until financial equilibrium is reached.

- **The methodology of the study in tertiary institutions will not achieve the required results**

The methodology to be deployed for the upcoming study has been successfully used in the initial study (cited throughout this document) where a total of 66 countries were reached. It is a tried and tested methodology previously employed by the lead researchers in a study conducted for the Council of Europe involving 21,000 participants in 45 countries.[2]

- **Risk of ineffective outreach to target stakeholders**

A communication plan with Key Performance Indicators will be established before the commencement of phase one of the project, and rigorous media tracking processes will be used to match the outreach strategy to arising needs. Members of IS3C's Education and Skills Working Group have extensive experience in communication strategies (e.g. Safer Internet Day which was founded by the working group leaders and is now celebrated annually in 160 countries).

- **Risk that the deployment of the project does not comply to the specifications described herein**

A key role of the Hub's Advisory Group will be to follow progress and ensure that milestone targets are met. It will follow progress in order to formulate an integrated strategy for subsequent phases of the project. While not directly involved in the roll-out of the project, IS3C's leadership team will act as a neutral observer to ensure that deadlines and targets are met.

Key personnel

Janice Richardson: Educator, researcher, university lecturer (Australia and Europe), founder and CEO of Insight SA (Luxembourg), author of 16 books on the digital transformation (published by Kluwer, Springer, Council of Europe, UNESCO). Former coordinator of the EU-funded 31-country Insafe & the ENABLE networks (2004-16), she advises governments and institutions in Europe and Africa on the digital transformation, and sits on safety advisory boards of Meta, Instagram, Snapchat. Janice is chair of the *Education and Skills* working group and led the 2021-2022 study by IS3C.

Awo Amenah Amenyah (Ghana) : Founder and Executive Director of Child Online Africa, Awo leads a team of professionals and volunteers committed to influencing policies and changing practices to improve safety and security of young internet users in Africa. Her work has influenced the National Cyber Security Policy and Strategy in Ghana and the Africa Union's Agenda 2040. A DQ World Training Partner and Child Online Protection implementation partner for ITU, in 2019 she succeeded in bringing together 12 African countries alongside Ghana to celebrate an annual Safer Internet Day Africa campaign.

Veroniki Samara (Greece and Finland): PhD in computer science from the Technical University of Darmstadt, Germany, Veroniki is an author, educator and researcher, and has conducted numerous projects for the European Commission, the Council of Europe, Insight SA and other international organisations. She previously conducted applied research for leading companies including Digital Equipment Corporation, Siemens Nixdorf, ABB and the German Standardization Institute, assessing ISO standards, propose new vendor-independent concepts for data handling and exchange in prepress, and preparing studies for new tools in the multimedia office environment.

IS3C's leadership team

Wout de Natris - IS3C Coordinator
Wout coordinates the aims and activities of the IS3C stakeholder coalition and its eight currently active working groups. He is a self-employed consultant on Internet governance and co-owner of MKB Cyber Advies Nederland, focusing on enhancing cyber security for SMEs, currently working closely with the greenhouse agricultural sector. He conducted several studies into cyber security and on the efficacy of the IGF. He founded IS3C in 2020, following up on a study into the (lack of) deployment of security-related Internet standards in 2019.

Mark Carvell - IS3C Senior Policy Adviser
Mark is an independent consultant on Internet governance and is a Member of EuroDIG (the European regional Internet governance forum). From 2008 to 2019, he was Head of Internet Governance Policy in the UK Government's Department for Digital Culture, Media and Sport (DCMS) and represented the UK in international negotiations relating to digital policy and Internet governance, including the G7, ITU and the Council of Europe. He was the UK representative on ICANN's Governmental Advisory Committee (GAC) and was appointed Vice-Chair of the GAC in 2017. He is a former member of the IGF's Multistakeholder Advisory Group (MAG). Mark has also acted as an advisor to the Commonwealth Telecommunications Organization (CTO) on Internet governance policy.