

Strengthening Cybersecurity and Digital Payment Literacy for Swiss SMEs Expanding into South Africa: A Train-the-Trainer Approach

**Franka Ebob Enow Ebai¹, Petra Maria Asprion¹,
Lebogang Mosupye-Semenya², Ntswaki Matlala², and Sergi Gubin¹**

¹University of Applied Sciences and Arts Northwestern Switzerland FHNW, School of Business, Institute for Information Systems, Basel, Switzerland

²Johannesburg Business School, South Africa

ABSTRACT

Small and medium-sized enterprises (SMEs) increasingly rely on secure digital infrastructures when entering international markets. However, understanding country-specific cybersecurity regulations and digital payment systems remains a significant challenge, and existing Swiss internationalisation programs provide limited training in these areas. To address this gap, this study proposes a conceptual Train-the-Trainer model, which has not yet been empirically validated, designed to equip Swiss business trainers with expertise in cybersecurity and digital payment systems in Switzerland and South Africa. The proposed program consists of a seven-week training framework aimed at developing a pool of trainers capable of transferring this specialized knowledge to Swiss SMEs. By strengthening trainers' competencies, the model supports SMEs in navigating regulatory and technological environments during market entry. The initiative is expected to generate direct benefits for business trainers and SMEs while also contributing to broader local, national, and regional capacity-building outcomes.

Keywords: Train-the-trainer, Digital payment systems, Cybersecurity, Internationalisation

INTRODUCTION

SMEs pursuing growth beyond domestic borders often encounter complex digital payment systems (DPSs), characterised by diverse digital ecosystems, evolving cyber-risk landscapes, varying cybersecurity regulations, compliance structures, and data protection standards. International expansion, therefore, goes beyond market access to navigating socio-technical systems, where a combination of technological factors and societal factors determine market access. This is the case of Swiss SMEs that want to expand to South Africa for new market opportunities. While the country is economically appealing to Switzerland as one of Africa's lion economies (Federal Department of Foreign Affairs [FDFA], 2021), Swiss SMEs must navigate complex regulatory environments and payment infrastructures, amongst other challenges that differ from those in Switzerland. The country's payment ecosystem for

instance, is characterised by the presence of physical banks and increasing digital payments like TymeBank and MTNMoMo following the rise of smartphone usage, cryptocurrencies and need for speedy cross-border value exchange (Thunes Financial Services LLC, 2026). Additionally, the region faces cyber threats that can undermine the sustainability of Swiss businesses operating in South Africa. For example, around 17'849 ransomware detections were reported in 2024 (Interpol, 2025). All these present unique experiences and challenges to foreign companies, newly entering the country. Swiss SME, planning to go into South Africa must therefore be equipped with digital payment knowledge, regulatory requirements and cyber-risks in South Africa.

While 99% of companies in Switzerland are SMEs (State Secretariat for Economic Affairs [Seco], 2025), and are integral to national innovation and economic performance, they have limited systemic support for cyber risk adaptation in internationalisation programs. Our initial review of official Swiss internationalisation support frameworks (Innosuisse and Switzerland Global Enterprise (S-GE)) revealed a lack of topics related to DPSs and cybersecurity. Market entry programs by Innosuisse in collaboration with Swissnex for Swiss startups interested in internationalisation in the US, Brazil, and India focus on topics such as incorporation, hiring, immigration, regulatory approval, pitch training (Swissnex, n.d.), tailored market research, and business matchmaking (Swissnex, 2026). S-GE export consulting services mainly include market evaluation and market analyses, development of internationalisation strategies, business partner search, and tax consulting (Switzerland Global Enterprise [S-Ge], n.d.). Further, S-Ge Academy which primary trains staff from Swiss Business Hubs abroad, business investment promotion, and embassies mainly offers courses that centre on export and trade promotion, client and SME consulting, and investment promotion (S-Ge, n.d.). Our review further revealed that existing international support trainings do not cover DPSs in Africa, particularly in South Africa, or cybersecurity regulations in Switzerland and South Africa.

Besides topics such as market research, networking, taxation in internationalisation programs, knowledge on DPSs, related regulations and cybersecurity is important. Cybersecurity is critical for secure and trusted digital flows, and countries' cybersecurity measures have an implication for international trade (International Institute for Sustainable Development [IISD], 2025). Moreover, educating businesses and business trainers on cyber risks and how to mitigate is one way of supporting businesses which want to newly enter the African regions (African Union, 2020). Based on these insights, this study introduces a novel conceptual perspective that interconnects cybersecurity, digital payments, and SME internationalisation, thus addressing the importance of facilitating secure cross-border expansion. We propose a Train-the-Trainer (TtT) model in which knowledge on DPSs and cybersecurity in South Africa and Switzerland is transferred to trainers, who then pass it on to Swiss SMEs.

The main research question is: How can a Train-the-Trainer model be designed to strengthen cybersecurity and digital payment literacy among Swiss SME internationalisation trainers supporting market entry into South Africa?

In terms of the methodological approach, the TtT model proposed in this study was developed through a review of the existing literature on SME internationalisation support, cybersecurity capacity building, and the existing TtT approaches. The adopted approach facilitated the identification of gaps in existing Swiss internationalisation support programmes and provided insights into how knowledge of cybersecurity and digital payment systems can facilitate the internationalisation of Swiss SMEs. Furthermore, lessons from previously implemented TtT models informed the design of the proposed model.

Following this introduction are the theoretical background, the proposed TtT model, and a concluding discussion.

THEORETICAL FRAMEWORK

This section depicts three sections of literature: SME internationalisation support, cybersecurity capacity, and TtT capacity-building approach. It provides an understanding of how knowledge of cybersecurity and payment systems can support Swiss SMEs' internationalisation.

Internationalisation and Existing Support Programs

Internationalisation is central to the growth of Swiss SMEs; this entails having a presence abroad, scaling up and expanding to other countries (Yakovlieva & Orlenko, 2025). The core benefits from internationalisation include access to emerging markets, increased market integration and achieving global growth (European Commission, n.d.), as well as increased sales and an expanded target audience (Yakovlieva & Orlenko, 2025). The topic is also of relevance to Swiss SMEs as one-third of these businesses are actively involved in international markets and generate more than three-quarters of their revenue abroad (Haute École de Gestion [HEG], 2024). Specifically, about 9.2% of Swiss companies have a presence in North, East, West, and Central Africa, and approximately 9.6% of Swiss businesses are present in South Africa. The main internationalisation challenges include compliance with local regulations, dealing with local competition, adapting to cultural differences and customer habits (Yakovlieva & Orlenko, 2025), which also entails considering and adapting to a country's payment ecosystem and the potential customer's preferred methods of payment (WARC, 2024). This is important as digital payment methods vary by country (Stripe, 2023). Cybersecurity is also a challenge as organisations face growing organisational cyber risks (World Economic Forum (WEF), kein Datum) and countries' varying cybersecurity policies and data protection standards.

There are established institutions in Switzerland to support SMEs to overcome these internationalisation challenges. Swiss Business Hub Southern Africa operating as part of the Embassy of Switzerland supports Swiss SMEs interested in exploring opportunities in Southern and Eastern Africa. They offer market analysis, legal clarification, business partner search, business trip and trade faire presence (The Federal Council, 2024). Switzerland Global Enterprise provides export consulting, events and webinars, and business

travel support. Their past webinars have covered topics like Egypt's industrial transformation, rules to protect the Swiss brand, and tariffs (Switzerland Global Enterprise [S-Ge], 2024).

Further, Swiss African Business Circle (SABC) organises events that bring Swiss and African stakeholders together to explore synergies (Swiss-African Business Circle [SABC], n.d.). On the training side, Swiss Africa Business Innovation Initiative (SABII) operated until 2024, enabling Science-based Swiss startups to explore market opportunities in regions like Nigeria, Ghana, Kenya and South Africa (Sareco, n.d.). Swissnex also offers trainings on facilitating Swiss founders' international expansion. While not focused on the African country, their Start up Camps support Swiss founders to implement their go-to-market strategy, build local networks and win first local customer in countries like Brazil, India, China and Japan (Swissnex, n.d.).

SMEs and Cybersecurity Capacity

Cybersecurity research consistently identifies SMEs as vulnerable actors, facing diverse cyber-risks. A review of about 40 scholarly publications from 2022 onwards showed that SMEs have a weak cybersecurity posture because they often underestimate cyber risks and overlook the implementation of required cybersecurity measures (Chidukwani, Zander, & Koutsakis, 2022). SMEs' cybersecurity weaknesses may also stem from inadequate resources and cybersecurity and lack of cybersecurity awareness (Benjamin et al., 2024). This is also a challenge to tech-companies; a lack of cybersecurity knowledge hinders them from developing secure digital products (Lindkvist, Hoglund, & Djebbar, 2025). Their other challenges include financial and prioritisation constraints.

This is relatable to SMEs in Switzerland: one in three SMEs has already experienced a cyberattack (State Secretariat for Economic [seco], 2026). As of 2024, 4% of 25 companies reported experiencing cyberattacks in previous years (Digital Switzerland, 2025). Yet more Swiss SMEs than before feel less confident in their cybersecurity capacity. To overcome these challenges, SMEs must acknowledge they can be targeted (Tetteh, 2024) and combine technological and procedural measures with employee training (Lindkvist et al., 2025; Chidukwani et al., 2022).

Train-the-Trainer Model as a Capacity-Building Approach

The TtT Model enables less experienced business trainers to gain new skills and learn a new topic (Centre for Disease Control and Prevention [CDC], n.d.) (SessionLab, 2024), building a pool of trainers who can transfer knowledge to others (CDC, n.d.). It has been implemented successfully in fields like healthcare, education, and the clean energy sector. Related to cybersecurity education, the TtT approach has been used to transform faculty, researchers and students into future trainers to close the cyberinfrastructure and data skill gap (Purwant et al., 2025). The approach followed six phases including, a pre-training, running of the TtT (Summer Institute), continuous

learning engagement through virtual meetings, trainers running a local training, trainers do an outreach, and gaps identification, and building of the training content for the onboarding of new members. Furthermore, a TtT framework educated trainers who then supported struggling readers in 16 English primary schools. The model followed key stages: trainer recruitment, pilot school selection, programme delivery, and process evaluation (Cockerill et al., 2025). In the clean energy sector, a TtT programme for hydrogen safety responders across ten European countries involved analysing current safety provisions, developing and testing training materials, integrating them into national programmes, and evaluating and disseminating the results (Brennan et al., 2024). A TtT programme was also developed for recovery college trainers in mental health and collaborative living. It demonstrated how training can be delivered and disseminated in other settings, involving three stages: trainer recruitment, delivery of training modules, and ongoing support (Vallarino et al., 2026).

The TtT approach has proven effective. In some studies, trainers reported increased confidence in delivering training content (Cockerill et al., 2025; (Cockerill et al., 2025; Purwant et al., 2025). In another study, TtT models improved knowledge, skills or practice for the trainers and even for the trainees (Nexø et al., 2024).

Overall Synthesis and Existing Gap

Our review of the existing internationalisation support programs in Switzerland shows an absence of focus on payment ecosystem, related regulations and cybersecurity. Moreover, SMEs, including those in Switzerland already face cyber threats which also pose a risk to their internationalisation plans to South Africa, and they need to be familiar with the region's DPSs. Additionally, some studies (Ojala et al., 2026; African Union, 2020; Hasan et al., 2021) have already demonstrated the relevance of training to improve cybersecurity awareness. While this was not in the context of training trainers (TtT), it still validates that training can be used to build cybersecurity competencies. Thus, to complement already existing offers in Switzerland, particularly focused on South Africa, we propose and demonstrate a structure of a TtT model aimed at enhancing trainers' knowledge on cybersecurity, regulations and digital payments.

RESULTS

To answer our main research question, we depict a TtT model, the target group and training design. We also showcase expected contributions that the model can attain once it has been implemented. The empirical validation of the model will be done in future research.

Description of the Proposed Train-the-Trainer Model

The proposed TtT model is designed to strengthen the capacity of trainers in Swiss internationalisation / market entry programs by equipping them

with knowledge on DPSs and cybersecurity in the context of Switzerland and South Africa. We plan to validate the model with at least 20 trainers who will subsequently transfer the acquired knowledge to Swiss SMEs by integrating relevant content into their training curricula and advisory activities. The overarching objectives of the TtT model include:

- Enhance trainer literacy in DPSs, related regulations and cyber risk management.
- Enable integration of these topics into broader entrepreneurship and internationalisation curricula.
- Foster cross-cultural networks among trainers, SMEs, and experts, cultivating resilient and inclusive digital engagement.

To operationalise the TtT model, we draw on selected elements of TtT approaches in prior studies (Vallarino et al., 2026; Brennan et al., 2024; Cockerill et al., 2025) to develop a five-stage process consisting of:

- **Stage 1:** Program Design and Setup (Vallarino et al., 2026; Cockerill et al., 2025). This includes program and curriculum design, setting up a digital learning platform and trainers' recruitment.
- **Stage 2:** Content Preparation and Review (Brennan et al., 2024). Experts from Switzerland and South create and peer review the content to ensure high quality.
- **Stage 3:** TtT sessions (Vallarino et al., 2026; Cockerill et al., 2025; Brennan et al., 2024). After content review, pilot TtT sessions will be conducted over a 7-week program with experts from both countries.
- **Stage 4:** Pilot Evaluation (Cockerill et al., 2025). This involves running a survey to evaluate content effectiveness and assess pilot impact.
- **Stage 5:** Integration in trainers' curricula (Brennan et al., 2024). Business trainers will be supported in integrating the TtT content in their trainings and advisory activities.

Target Participants and Training Design

The target group of the TtT model and related sessions are business trainers involved in existing Swiss entrepreneurship and internationalisation programs. To enrich the exchange of perspectives and experiences, business trainers from South Africa will also participate in the program. The TtT training will be delivered by program coordinators and guest speakers, including cybersecurity experts, professional lecturers, and entrepreneurs from Switzerland and South Africa. To make the program as practical as possible, each session will combine an input lecture, a guest speaker contribution, and a practical activity in which participants work on a dedicated task. In the final session, participants will present the results of their supporting work. The organizers will then facilitate a discussion to gather feedback and reflect on participants' experiences in the program. Table 1 outlines an overview of the proposed curriculum.

Table 1: Proposed curriculum.

Week	Topics	Participants Activities
1-2	- General introduction to the course, objectives and expectations; - General information cybersecurity-related risks including ZA& CH; - Intro to payment ecosystems and their relevance (overview) - Simulation of a cybersecurity risk to a payment system: ZA& CH	-Participants get-to-know each other (ZA & CH) -Pairing of participants -A project assignment is shared (TBD)
3-4	Part 1: - Discussing Payments systems in ZA (2-3 types) - Having Guest speaker (s) from ZA - Relating the payment systems discussed to cybersecurity regulations, compliance - Case studies of attacks ZA Part 2: - Discussing Payments systems in CH (2-3 types) - Having Guest speaker (s) from CH - Relating the payment systems discussed to cybersecurity regulations and compliance in CH	Participants partake in class activities and discussions in pairs
5	-Panel discussion with experts from CH and ZA in relation to cybersecurity and payment systems	Participants partake in Q & A with the panel experts
6	Bringing topics discussed together A cross-comparison of CH and ZA, highlighting differences, similarities and opportunities	
7	Final presentations of participants discussed -Lessons learned and participants' feedback	Participants present their results.

Expected Contributions

By successfully running the proposed TtT's session, we expect to contribute to the quality and competitiveness of the Swiss internationalisation programs and Swiss entrepreneurship ecosystem in general. We mainly expect results as impact at the local, regional, and national levels. The results at the local level include:

- Swiss business trainers become knowledgeable on innovative DPSs, regulations, and cybersecurity across Switzerland and South Africa.
- Swiss business and entrepreneurship programs integrate the developed content into their curriculums.
- Swiss business trainers develop new networks through the program, an added value to their own learners.

At the regional level, we expect that business programs and professional training programs in different Swiss regions adopt the course curriculum and integrating it into their educational structure.

At the national level, we expect that Swiss SMEs that are trained by participating trainers with our course package are well-prepared for the risks they may face as they expand to the African region.

DISCUSSION

Gaps in existing Swiss internationalisation programs regarding topics such as DPSs, regulations and cybersecurity highlight the need to enhance trainers' existing knowledge and skills. Rather than recruiting trainers outside the current programs, we propose a TtT program for those who already possess market entry expertise and have established contacts with SMEs. Evidence of the effectiveness of the TtT model has already been documented in the literature. The TtT model is a reliable way to upskill business trainers in a particular area, thereby increasing the pool of available trainers. The planned stages in the proposed TtT model in this study match some stages in previous studies. The recruitment of trainers aligns with the approaches described in Cockerill et al. (2025) and Vallarino et al. (2026), while the content preparation phase corresponds to the approach in Brennan et al. (2024). Process evaluation aligns with Cockerill et al. (2025) and the integration of the knowledge into trainers' curricula corresponds with Brennan et al., (2024) and Vallerino et al., (2026). Incorporating the material into trainers' courses demonstrates the sustainability of the proposed intervention. While we intend to apply the TtT model for a different target group, similar positive results as those reported by Hollis et al., (2022) and Cockerill et al., (2025). For instance, business trainers may report a better understanding of the link between DPSs and cybersecurity regulations, as well as high confidence and readiness to cascade this knowledge to SMEs. In turn, SMEs may report a better understanding of DPSs, related regulations and cybersecurity. Beyond these impacts, the initiative also contributes to increasing cybersecurity awareness and expanding the pool of individuals with cybersecurity skills.

CONCLUSION AND LIMITATIONS

This study presents a TtT model aimed at equipping business trainers in existing Swiss market entry and internationalisation programs with knowledge of DPSs, regulations and cybersecurity. The main limitation of this study is that the presented TtT model has not yet been empirically validated through field implementation or quantitative testing. Thus, the results and impact discussed remain theoretical and require future evaluation. However, an implementation of the model is planned between December 2026 and February 2027. The lack of extensive research on all internationalisation programs and their content in Switzerland, including online programs is another limitation.

Future research should therefore focus on piloting the TtT model, assessing its actual effectiveness and impact in practice, and evaluating how successfully trained business trainers transfer knowledge on DPSs, regulations and cybersecurity to SMEs. Such evaluation would provide empirical evidence of the model's impact and its potential for replication in other internationalisation support programs.

REFERENCES

- African Union. (2020). *The digital transformation strategy for Africa (2020–2030)*. <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>
- Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, 19, 134–153. <https://doi.org/10.30574/gjeta.2024.19.2.0084>
- Brennan, S., Brauner, C., Davis, D., Backer, N. D., Dyck, A., García-Hernández, C., ... Vladimir, M. (2024). European hydrogen train-the-trainer framework for responders: Outcomes of the HyResponder project. *International Journal of Hydrogen Energy*, 79, 448–455. <https://doi.org/10.1016/j.ijhydene.2024.07.038>
- Centers for Disease Control and Prevention (CDC). (n.d.). *Understanding the training of trainers model*. https://www.cdc.gov/healthy-schools/media/pdfs/17_279600_TrainersModel-FactSheet_v3_508Final.pdf
- Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2022.3197899>
- Cockerill, M., O’Keeffe, J., Thurston, A., Ozkaya, C., Holland, J., & Taylor, A. (2025). The development of a train-the-trainer approach in reciprocal reading instruction in England’s primary schools. *Education Sciences*, 15(2), 183. <https://doi.org/10.3390/educsci15020183>
- Digital Switzerland. (2025). *Cybersecurity losing priority among Swiss SMEs despite unchanged threat landscape*. <https://digitalswitzerland.com/news/cybersecurity-losing-priority-among-swiss-smes-despite-unchanged-threat-landscape>
- European Commission. (n.d.). *SME internationalisation beyond the EU*. https://single-market-economy.ec.europa.eu/smes/growing-and-scaling-sme/improving-smes-access-markets/sme-internationalisation-beyond-eu_en
- Federal Department of Foreign Affairs (FDFA). (2021). *Sub-Saharan Africa strategy 2021–2024*. https://www.eda.admin.ch/eda/en/fdfa/fdfa/publikationen.html/content/publikationen/en/eda/schweizer-aussenpolitik/Subsahara_Afrika_Strategie_2021-2024
- Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58.
- Haute École de Gestion (HEG). (2024). *Swiss International Entrepreneurship Survey (SIES)*. <https://www.heg-fr.ch/en/research-and-mandates/projects/swiss-international-entrepreneurship-survey-sies/>
- Hollis, J. L., Seward, K., Kocanda, L., Collins, C. E., Tully, B., Brett, K., ... MacDonald-Wicks, L. (2022). Evaluating a train-the-trainer model for scaling-up Healthy Conversation Skills training: A pre-post survey using the Theoretical Domains Framework. *Patient Education and Counseling*, 105(10), 3078–3085. <https://doi.org/10.1016/j.pec.2022.06.011>
- International Institute for Sustainable Development (IISD). (2025). *Cybersecurity and international trade*. <https://www.iisd.org/publications/report/cybersecurity-international-trade-policy>
- INTERPOL. (2025). *New INTERPOL report warns of sharp rise in cybercrime in Africa*. <https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa>

- Lindkvist, A., Hoglund, E., & Djebbar, F. (2025). Cybersecurity practices, challenges and posture in small and medium enterprises: A survey study in Sweden. *European Conference on Cyber Warfare and Security*, 24, 838–847. <https://doi.org/10.34190/eccws.24.1.3579>
- Nexø, M. A., Kingod, N. R., Eshøj, S. H., Kjærulff, E. M., Nørgaard, O., & Andersen, T. H. (2024). The impact of train-the-trainer programs on the continued professional development of nurses: A systematic review. *BMC Medical Education*. <https://doi.org/10.1186/s12909-023-04998-4>
- Ojala, A.-L., Sipola, T., & Saharinen, K. (2026). Cybersecurity awareness and hygiene development in Finnish vocational education: Staff perceptions, training gaps and diverse learning pathways. *Information & Computer Security*, 34(1), 66–85. <https://doi.org/10.1108/ICS-12-2024-0311>
- Purwant, W., Yang, M., Jiang, P., Moots, S. C., Sosonkina, M., & Wu, H. (2025). T3-CIDERS: Train-the-trainer and community building to increase cyberinfrastructure adoption in cybersecurity research and education. *Practice and Experience in Advanced Research Computing*. <https://doi.org/10.1145/3708035.3736021>
- Sareco. (n.d.). *SABII – Swiss Africa Business Innovation Initiative*. <https://www.sareco.org/portal-business/>
- SessionLab. (2024). *What is the train-the-trainer model and how to use it?* <https://www.sessionlab.com/blog/train-the-trainer-model/>
- State Secretariat for Economic Affairs (SECO). (2026). *Cybersecurity*. <https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/Cybersecurity.html>
- State Secretariat for Economic Affairs (SECO). (2025). *Figures on SMEs: Companies and jobs*. <https://www.kmu.admin.ch/kmu/en/home/concrete-know-how/facts-and-figures/figures-smes/companies-and-jobs.html>
- Stripe. (2023). *Stripe report finds businesses are racing across borders with digital trade*. <https://stripe.com/en-pt/newsroom/news/global-digital-trade>
- Swiss-African Business Circle. (n.d.). *Connecting Switzerland & Africa*. <https://sabc.ch/>
- Swissnex. (2026, March 26). *China*. <https://swissnex.org/china/services/startups/>
- Swissnex. (n.d.). *Enabling Swiss startups to go international*. <https://swissnex.org/services/startups/>
- Swissnex. (n.d.). *Startup camps: Boston & New York*. <https://swissnex.org/boston/work/startups/startup-camps/>
- Switzerland Global Enterprise (S-GE). (n.d.). *Academy*. <https://www.s-ge.com/en/academy?ct>
- Switzerland Global Enterprise (S-GE). (n.d.). *Export consulting*. <https://www.s-ge.com/en/services/export-consulting?ct>
- Switzerland Global Enterprise (S-GE). (2024). *Information webinar: Internal compliance program (ICP) in global trade*. <https://www.s-ge.com/en/publication/recordings/depublicationwebinar-aufzeichnungen2024eventwebinarwebinar-icp?ct>
- Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems*, 25, 235–246. https://doi.org/10.48009/1_iis_2024_120
- The Federal Council. (2024). *Swiss Business Hub Southern Africa*. <https://www.eda.admin.ch/swiss-business-hub-southern-africa>
- Thunes Financial Services LLC. (2026). *The rise of digital payments in South Africa*. <https://www.thunes.com/insights/learn/digital-payments-in-south-africa/>

- Vallarino, M., Briand, C., Lord, M.-M., & Sauvageau, A. (2026). Logic model for a train-the-trainer program ensuring alignment with recovery college principles and values. *Mental Health and Social Inclusion*, 30(1), 101–113. <https://doi.org/10.1108/MHSI-02-2025-0057>
- WARC. (2024). *How localising digital payments unlocks internationalisation opportunities*. <https://www.warc.com/en/article/how-localising-digital-payments-unlocks-internationalisation-opportunities-c7cae1cab6d04483a2f3dfb3f5aa819c>
- World Economic Forum. (2025). *Cybersecurity*. <https://www.weforum.org/stories/2025/05/cybersecurity-cyber-risk-national-policy/>
- Yakovlieva, V., & Orlenko, O. (2025). Modern challenges for companies in the context of business internationalization. *International Journal of Psychology and Strategic Communication*. <https://doi.org/10.61030/CVDT2672>