International Law Office®

TECH, DATA, TELECOMS & MEDIA - SWITZERLAND

Implementation of 2018-2022 national strategy for the protection of Switzerland against cyber risks – quarterly report

13 November 2020 | Contributed by Walder Wyss

On 19 October 2020 the Federal Council's Cyber Committee adopted a report on the advancement of the 2018-2022 national strategy for the protection of Switzerland against cyber risks (2018-2022 NCS) and its gradual implementation. The report focuses mainly on the progress made in supporting small and medium-sized enterprises (SMEs) and promoting research and training.

Overall, the report concludes that much progress has been made in the implementation of the 2018-2022 NCS and that, in general, the process is on track. More specifically, the report notes that one-third of the 247 measures under the NCS have been achieved. The next two years should see an acceleration in the adoption of the remaining measures.

The 2012-2017 NCS did not target SMEs and, as a result, there was little nationally coordinated action to support them in the area of cybersecurity. The implementation of the 2018-2022 NCS has achieved several milestones in that respect. For example, in 2018 ICTswitzerland (a private umbrella organisation for the digital economy) developed a cybersecurity quick test for SMEs to provide smaller companies with a self-assessment tool. The test allows companies with little knowledge of information and communications technology (ICT) and cybersecurity to quickly and easily determine whether their technical, organisational and human measures are enough to protect them against cyber risks. Moreover, ICTswitzerland, in collaboration with the Swiss Academy of Engineering Sciences and the business community, have published a guide designed to help SMEs achieve a minimum level of cybersecurity. In addition, the Swiss Association for the Cybersecurity Label – a private association of market actors – has created a label enabling SMEs to indicate their ICT security commitments to potential business partners.

Progress was also reported in the fields of education and training, where several achievements were made (eg, the creation of a cyber defence campus at both the Swiss Federal Institute of Technology Lausanne and ETH Zurich in September 2019 and November 2019, and where a master's degree in cybersecurity can now be obtained). Further, a federal diploma of higher education in cybersecurity is now available to holders of federal certificates of capacity with experience in the ICT field.

The report also summarises practicable solutions with regard to norms relating to objects connected to the Internet, minimum ICT standards and a possible obligation to declare cyber incidents reaching a certain threshold and on which the Federal Council is due to decide before the end of 2020.

For further information on this topic please contact Jürg Schneider, Hugh Reeves or Ashley Robinson at Walder Wyss by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com, hugh.reeves@walderwyss.com or ashley.robinson@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

The materials contained on this website are for general information purposes only and are subject to the disclaimer.

AUTHORS

Jürg Schneider

Hugh Reeves

Ashley Robinson