

Press release

Bern, 8 December 2020

Home office surge in Swiss SMEs: Opportunities taken – cyberrisks underestimated

gfs-zürich surveyed 503 CEOs of small companies about the effects of the coronavirus crisis on digitalisation and cyber security in Swiss SMEs

Thanks to modern infrastructure and location-independent activities, two-thirds of Swiss SMEs were able to respond quickly to the coronavirus lockdown and in many cases could switch easily to working from home. At the start of 2020, an average of 10% of employees worked primarily from home, and during the lockdown this rose to almost four times as many. The numbers fell again after the lockdown, and with 16% of employees now working from home, this equates to a 60% increase compared to the start of the year. While Swiss SMEs demonstrated flexibility, the risks from home offices and digitalisation are underestimated by many companies. Although a quarter of Swiss SMEs have already been victims of a serious cyberattack, two-thirds of SMEs neither hold regular employee training on the subject of cyber security nor have a security concept in place.

From August to October 2020, the market and social research institute gfs-zürich conducted a representative survey of 503 CEOs of small companies (with 4 to 49 employees) in the German, French and Italian-speaking regions of Switzerland on the effects the coronavirus pandemic has had on digitalisation. The survey was commissioned by digitalswitzerland, Mobiliar, the National Cyber Security Centre (NCSC), the School of Business of the University of Applied Sciences and Arts Northwestern Switzerland (FHNW) and the Swiss Academy of Engineering Sciences (SATW).

An overview of the main findings:

- **During the lockdown, Swiss SMEs exploited the potential of the home office and the trend continues:** For a third of SMEs, working from home was not an option due to work being tied to a particular location, whereas the remaining two-thirds were able to transform workstations into home offices without any major problems thanks to modern infrastructure. This meant that the number of employees working from home during the lockdown almost quadrupled from 10% to 38%. Since then, home offices have become established in many SMEs, and with 16% of employees now working from home. This is 60% higher than before the lockdown.
- **Online conference tools gaining ground:** After e-mail and telephone, most communication within SMEs takes place using private communication channels such as WhatsApp and other messaging services. Since the lockdown began, online conference tools in particular have become more important: the number of virtual meetings has more than doubled, rising from 9% to 20%.
- **A quarter of Swiss SMEs have already fallen victim to a serious cyberattack:** Out of the 38,250 or so SMEs throughout Switzerland that have been attacked, around a third (12,930 SMEs) have suffered financial damage and every tenth attack has led to reputational damage and/or loss of customer data.
- **Not enough preventive measures are being taken:** Despite frequent cyberattacks, only half of all SMEs have an emergency plan to ensure business continuity and around two-thirds neither hold regular employee training nor have implemented a security concept within the company.
- **People as a risk factor – cyberrisks are often underestimated:** Only just under half (47%) of the CEOs stated that they are well informed about security-related issues. Even more drastic is the lack of awareness that they themselves may become a victim of a cyberattack: Just 11% consider being put out of action for a day due to a cyberattack as a major risk.

Florian Schütz, Federal Cyber Security Delegate, praised the adaptability of Swiss SMEs: “It is really promising to see how much progress even the smaller SMEs in Switzerland have made with regard to their IT infrastructure, and that increasing focus is being placed on cyber security. The lockdown showed how important the digital transformation is for companies to remain adaptable. Many SMEs have recognised this and are accelerating their digitalisation activities. However, the current situation also makes it clear how important it is that we create framework conditions in order to shape cyber security in Switzerland in a way that the opportunities associated with digitalisation can be exploited as much as possible. The federal government plans to further expand its efforts and actively support the general population and businesses in the protection against cyber risks.”

Andreas Hölzli, Head of the Cyber Risk Competence Centre at Mobiliar, explained that “Although Swiss SMEs are investing in IT security, one in four of the SMEs surveyed has already been a victim of a cyberattack. The problem is that organizational measures in particular are often considered less important. Companies need measures that go beyond the technical aspects, including raising awareness among their employees, for instance.”

Prof. Dr Marc K. Peter of FHNW believes that working from home will become an established component of the new working world strategy for “blended working” in the long term: “For many jobs, a combination of working from home and working in the office will become part of everyday life. With this, however, urgent consideration needs to be given to the fact that this will require huge investments in technology and IT at Swiss SMEs.”

For Nicole Wettstein, Cybersecurity Programme Manager at SATW, the large number of SMEs affected by a cyberattack is motivation for driving forward the current awareness-raising activities: “It is crucial that the number of SMEs implementing the minimum measures for basic cyber security protection continues to increase.”

Andreas W. Kaelin, Deputy Managing Director and Head of Cyber Security Dossier at digitalswitzerland, indicated that, “according to the survey, around two-thirds of small businesses rely on the support of external IT service providers. This means we need to urgently take action to make it easier for companies to identify trustworthy IT service providers, because the security of a company relies entirely on the service providers.”

The complete study is available for download: ictswitzerland.ch/en/publications/studies/digitisation-and-cybersecurity-sme

For more information, contact:

Andreas Kaelin, digitalswitzerland | Bern office

Tel. +41 31 311 62 45 | andreas@digitalswitzerland.com

digitalswitzerland

digitalswitzerland is a nationwide, cross-sector initiative that aims to establish and strengthen Switzerland as a leading location for digital research and innovation. The umbrella organisation deals with all aspects of digitisation, and is committed to solving the related social, economic and political challenges. To this end, citizens, research and teaching departments, business, charitable organisations and politics are all networked to promote transverse cooperation. The fields of activity include getting the public involved, promoting education and further training so as to meet the demand for qualified workers, and continuing to develop the political and economic framework conditions that strengthen the digital infrastructure as well as cyber-resilience. digitalswitzerland identifies trends, mobilises the ecosystem and activates processes of change. The umbrella organisation comprises more than 220 members from respected companies, SMEs and start-ups, municipalities and cantons, decision-makers from politics and government, universities and universities of applied sciences, associations and NGOs.

In October 2020, the new umbrella organisation "digitalswitzerland" was created by the merger of the location initiative of the same name with "ICTswitzerland", the umbrella organisation for the digital economy, which was founded in 1980. Until completion of the merger in early 2021, all topics and information can still be found on the separate websites ictswitzerland.ch and digitalswitzerland.com

Mobiliar

The Mobiliar Group ("Mobiliar") is the leading Swiss retail insurance company and number one in the field of household, SME and risk life insurance. Founded in 1826, it is the oldest private insurance company in Switzerland and is still organised on a cooperative basis. Its 80 general agencies are managed in an entrepreneurial manner with their own claims departments and ensure personal proximity to over 2.1 million customers at 160 locations. As a result, every third household and every third company in Switzerland is insured with Mobiliar. As an all-sector insurer, Mobiliar employs around 5,700 people and offers 341 apprenticeships.

mobiliar.ch

The National Cyber Security Centre

The National Cyber Security Centre (NCSC) is the federal government's centre of competence for cyber security, and thus the first point of contact for business, government offices, educational institutions and the general public regarding cyber issues. It is also responsible for the coordinated implementation of the National Strategy for the Protection of Switzerland against Cyber-Risks (NCS) 2018-2022.

ncsc.ch

School of Business at the University of Applied Sciences and Arts Northwestern Switzerland (FHNW)

The FHNW School of Business is internationally oriented with a focus on practice. It trains 3,000 Bachelor's and Master's degree students in Basel, Brugg-Windisch and Olten, and with its broad range of further education courses in business is a leader among Switzerland's universities of applied sciences. The Competence Centre for Digital Transformation offers research, consulting and educational services on all aspects of digital transformation, to help organisations and employees to develop and successfully implement their digital growth strategies.

fhnw.ch/en/about-fhnw/schools/business

Swiss Academy of Engineering Sciences (SATW)

The Swiss Academy of Engineering Sciences (SATW) is the most important network of experts in the field of engineering sciences in Switzerland. It operates on behalf of the Swiss Federal Government to identify industry-relevant technological developments, and informs politicians and the general public about their significance and consequences. As a politically independent specialist organisation, it provides impetus for the secure conduct of all actors in cyberspace.

satw.ch/en