Press Release

Zurich, 20 August 2026

Swiss SMEs massively underestimate cyber risks: Basic protection and insurance cover remain inadequate

AI is making cyber-attacks faster and more scalable. Yet many Swiss SMEs are inadequately protected and underinsured. [These are among the findings of a representative Deloitte survey of employees at Swiss SMEs.] The results indicate that many companies underestimate the risks and fail to consistently implement basic protective measures. Furthermore, cyber insurance remains uncommon among small businesses in particular.

The cyber-threat landscape is becoming much more serious for Swiss companies. Cyber-attacks are on the rise and are becoming more targeted and effective thanks to artificial intelligence (AI). Small and medium-sized enterprises (SMEs) are particularly vulnerable. This is because they often have fewer resources, underestimate the risk, implement cyber-security measures to a lesser extent and are not as well covered by cyber insurance. This is shown by a study conducted by the audit and consultancy company Deloitte on cyber-security at Swiss SMEs.

The results reveal a clear gap between experienced threats and perceived risks (see Figure 1). 49 per cent of the SME employees surveyed have experienced a serious cyber incident at their workplace in the last three months, but only 22 per cent consider their company's cyber risk to be high. This perception gap is particularly pronounced among micro-enterprises with between one and nine employees. Although 38 per cent of these companies report experiencing serious cyber incidents, only 15 per cent rate the risk of a cyber-attack as high.

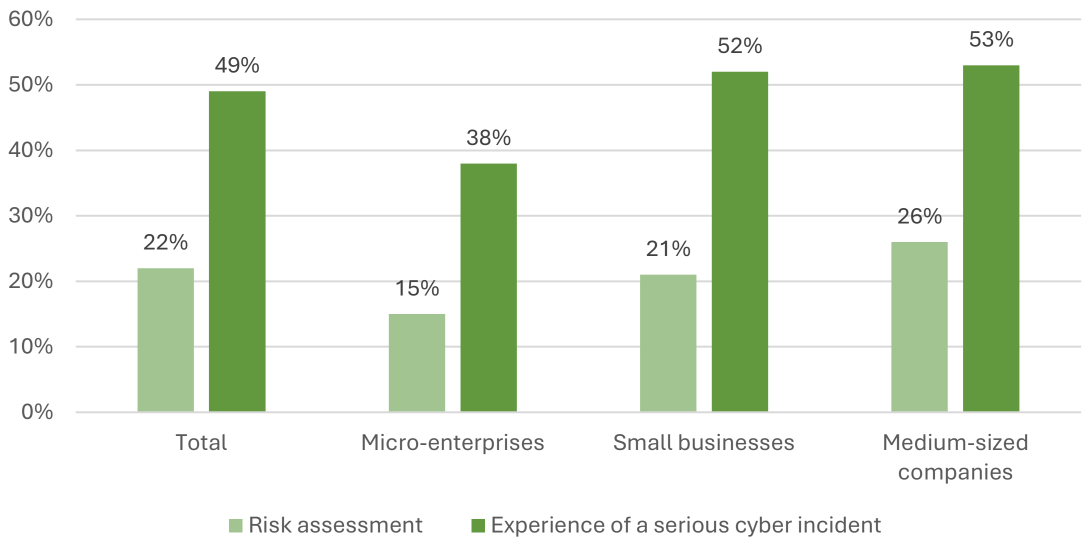

Figure 1. The proportion of respondents who rated cyber risk as very high or high, and the proportion of respondents who have experienced a serious cyber incident at their workplace in the last three months.

Phishing affects businesses of all sizes

Phishing – i.e. attempts to steal data or trigger payments via fake messages – is the most commonly perceived cyber-threat, accounting for 25 per cent of cases. One notable finding is that phishing affects micro-enterprises almost as frequently as SMEs in general. This shows that even very small businesses are exposed to cyber risks. Malware, CEO fraud, identity theft, suspected data

© 2026 Deloitte AG

breaches and operational disruptions caused by employees are also recognised as risks and affect companies of all sizes.

"Many SMEs underestimate just how much cyber-attacks have changed. Nowadays, cyber-attacks are scalable, automated and affect companies of all sizes. Phishing, compromised login details and manipulated payment processes in particular can have a severe impact even on small businesses," says Florian Widmer, Cyber Partner at Deloitte Switzerland. "An organisation's ability to withstand cyber-attacks therefore starts with the basics. Businesses must implement measures such as strong authentication, restrictive access rights, regular training, tested backups and a robust contingency plan."

Basic security measures are not yet standard practice

Deloitte's SME Cyber-security Index, which was compiled for the first time on the basis of the study, measures the prevalence of six fundamental employee-related security measures and stands at 58 out of 100 points (see Figure 2). This indicates that, on average, only 58 per cent of the security measures included in the survey have been implemented by companies, underlining a considerable shortfall in basic protective measures.

The gaps are particularly significant when it comes to modern authentication methods. Only 45 per cent of companies have introduced passwordless authentication, such as biometric methods. Multi-factor authentication is more common, at 66 per cent, but is still far from being universally adopted. At the same time, staff perceive the measures that are in place to be effective. 88 per cent of respondents whose companies use email alerts consider them to be useful. This figure illustrates employees' perceptions rather than actual effectiveness. It also shows that not all companies yet use warnings of this kind.

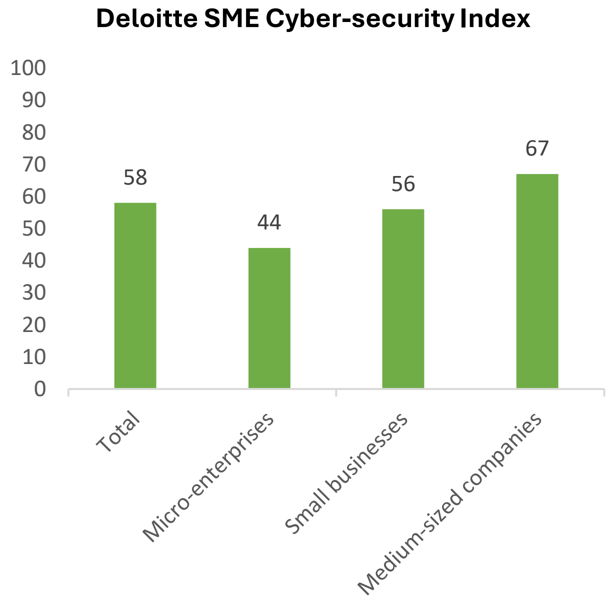

Figure 2. Unweighted average of the prevalence of six security measures. Basic cyber-security protection increases with the size of the organisation.

A significant insurance gap persists

As well as evaluating risk perception and the use of protective measures, the Deloitte study highlights a third shortcoming: insurance cover. Although the uptake of cyber insurance is growing in Switzerland, market penetration remains low. According to the latest figures from the Swiss Insurance Association (SIA), around 72,000 corporate insurance policies were taken out in 2025. This means that only 11.5 per cent of companies based in Switzerland are insured against cyber risks.

The insurance gap is particularly wide among micro-enterprises and small businesses. These companies can be affected more seriously by cyber incidents, as the damage can have a greater impact in relation to their revenue. Many SMEs nevertheless fall short of the basic security requirements for obtaining cyber insurance. Other factors also add to the difficulty of accessing cyber insurance, including complex application processes and low sales incentives, as commissions on cyber insurance policies for small businesses are often low.

"Cyber insurance does not only become beneficial to SMEs after an attack," says Marcel Thom, Partner and Insurance Lead at Deloitte Switzerland. "Its added value lies in the combination of prevention, rapid crisis response and financial protection. Small businesses in particular need clearly understandable products, transparent requirements and straightforward, digitally

© 2026 Deloitte AG

supported processes for taking out cover. This enables them to integrate cyber insurance as a key component of business resilience.”

Greater accountability, but no rigid regulation

The study also sets out clear expectations regarding the role of the state. 87 per cent of respondents are in favour of more extensive cyber-security regulations. However, only 19 per cent would prefer stricter, purely state-imposed regulations with minimum standards. For Switzerland, this results in a pragmatic agenda: the federal government should set clear minimum standards and facilitate cooperation between companies, industry associations, insurers and IT service providers.

About the study

The Deloitte study ‘Underestimated, unprotected, underinsured: Cyber risks for SMEs in Switzerland’ is based on a representative online survey of 924 employees working for Swiss companies with up to 249 employees, all of whom use computers in their work. The survey was carried out in April 2026, and cyber experts from insurance companies were then interviewed in June and July 2026. According to the classification used by the Federal Statistical Office, SMEs are defined as companies with up to 249 employees.

Contact: Michael Wiget	Contact: Kevin Capellini
External Communications Lead	External Communications
Tel.: +41 58 279 70 50	Tel.: +41 58 279 59 74
E-mail: mwiget@deloitte.ch	E-mail: kcapellini@deloitte.ch

Deloitte Switzerland

Deloitte offers integrated professional services that include Audit & Assurance, Tax & Legal, Strategy, Risk & Transactions Advisory and Technology & Transformation. With around 2,500 employees at six locations in Basel, Berne, Geneva, Lausanne, Lugano and Zurich (headquarters), Deloitte serves companies and organisations of all legal forms and sizes across all industry sectors in Switzerland.

Our people deliver measurable and lasting results that help reinforce public trust in capital markets and enable clients to transform and thrive. Building on its over 180-year history, Deloitte spans more than 150 countries and territories with approximately 470,000 professionals worldwide.

Note to editors

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (‘DTTL’), its global network of member firms and their related entities (collectively the ‘Deloitte organisation’). DTTL and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte AG is an audit firm recognised and supervised by the Federal Audit Oversight Authority (FAOA) and the Swiss Financial Market Supervisory Authority (FINMA).

The information in this media release was correct at the time of publication.

© 2026 Deloitte AG