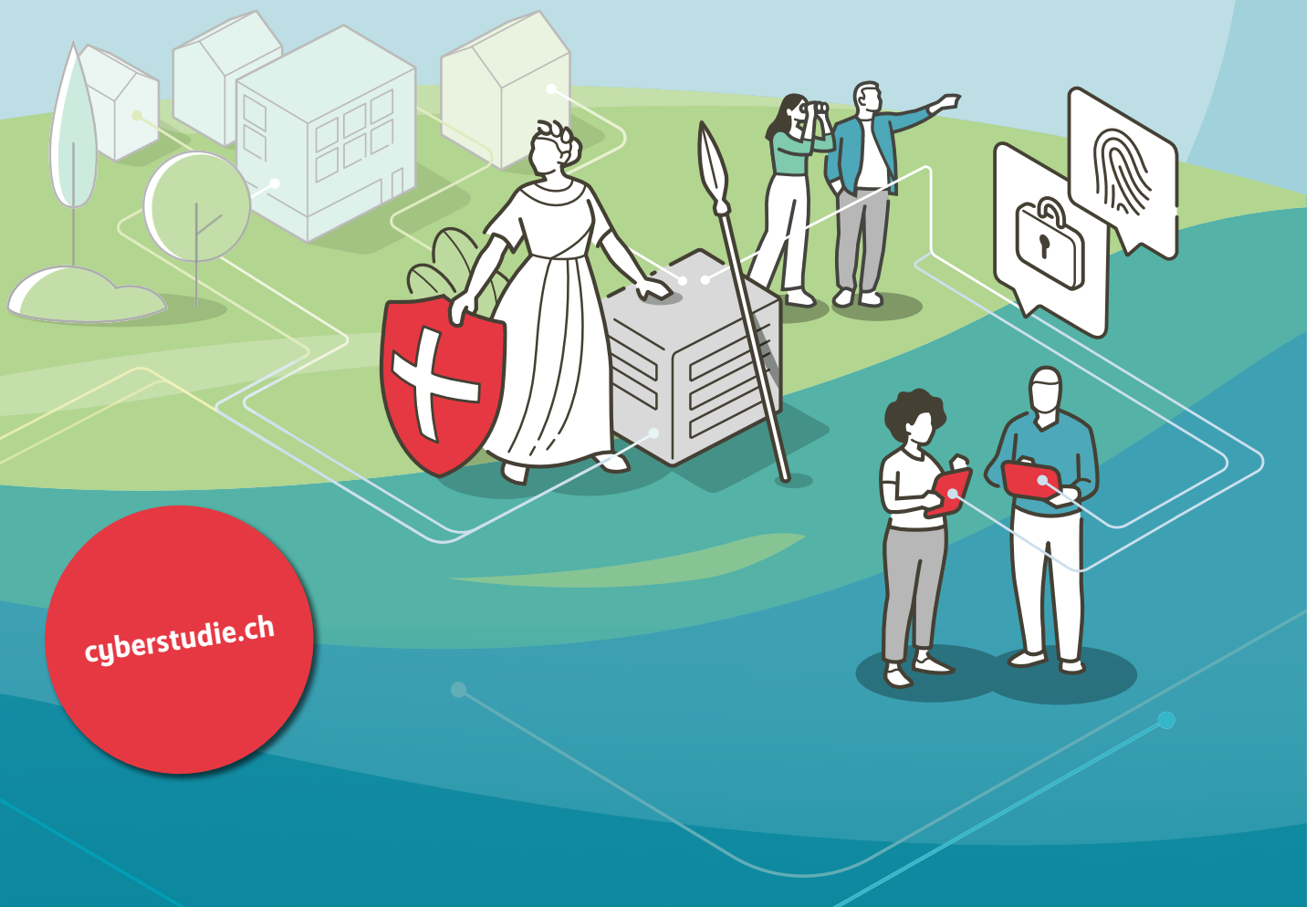


# SME cyber security in 2026

A study by la Mobilière in cooperation with the NCSC, digitalswitzerland, HES-SO, HWZ and SATW

Marc K. Peter, Romain Geiser, Anu Anthamatten, Léonard Marbe, Anna V. Rozumowski, Tobias Schlegel and Karin Mändli Lerch



# Contents

|                                                                                           |    |
|-------------------------------------------------------------------------------------------|----|
| Introduction                                                                              | 3  |
| 01 Swiss SMEs – what is their current status in the digital age?                          | 4  |
| 02 Digital sovereignty – a new subject area in current world politics                     | 6  |
| 03 Cyber crime – a problem to be taken seriously and that presents new threats through AI | 8  |
| 04 Cyber crime at SMEs: over 35 000 victims, often with serious consequences              | 10 |
| 05 Knowledge of cyber threat situation and support                                        | 12 |
| 06 Cyber security is growing in importance and regaining significance                     | 14 |
| 07 Cyber risk responsibility: more SMEs are allocating responsibilities                   | 16 |
| 08 Implementation of technical cyber security measures                                    | 18 |
| 09 Implementation of organisational cyber security measures                               | 20 |
| 10 The future: cyber resilience is becoming more important, but many SMEs remain cautious | 22 |
| Checklist for Swiss SMEs                                                                  | 24 |
| Practical tools and research methodology                                                  | 26 |
| Contact authors                                                                           | 27 |

# Introduction

The digital transformation has enabled Swiss small and medium-sized enterprises (SMEs) to achieve major progress in recent years. Many companies are investing in digital processes, using cloud services, increasingly relying on digital strategies and working with new technologies such as artificial intelligence (AI). This has simultaneously led to a growing dependency on digital systems, data and external service providers, while also increasing exposure to the concomitant risks. Cyber crime is currently one of the key strategic challenges facing Swiss SMEs and the great majority of companies expect the threat to increase further in future due to AI.

This study of the SME sector has been conducted annually since 2020. The findings of the SME cyber security study in 2026 paint a varied picture across the SME landscape in Switzerland: many SMEs master the technical fundamentals, such as software updates, firewalls, data backups and multi-factor authentication. At the same time, there remains significant room for improvement in terms of organisational measures (as in previous years). Emergency planning, security audits, supplier evaluations and systematic employee training tend to be overlooked, even though they may be crucial to a company's ability to withstand an emergency.

One positive factor identified is the renewed emphasis on cyber security. More companies are defining responsibilities and investing consistently in additional protective measures. The self-perception of cyber resilience is higher than in 2025, although it remains below the 2024 level. The study also shows that many SMEs still consider the risk of a serious cyber incident as rather low.

The main conclusion is therefore that cyber security is no longer merely an IT matter but a managerial issue. Successful SMEs do not just protect their systems and data but also engage in contingency planning at the organisational level. Combining protective technical measures with clear responsibilities, trained staff, tested backups and effective emergency planning brings a sustainable improvement in cyber resilience while at the same time strengthening competitiveness.

In the following ten chapters, we set out the main findings of the latest edition of the “SME cyber security in 2026” study and present recommendations for increasing cyber security and cyber resilience among SMEs. The detailed study results are available at [cyberstudie.ch](https://cyberstudie.ch).

Bern and Zurich, October 2026

La Mobilière, NCSC, digitalswitzerland, HES-SO, HWZ and SATW

# 01 Swiss SMEs – what is their current status in the digital age?

The latest SME survey presents a varied picture of digital transformation in Switzerland. Many companies have started their digital journey, although progress varies across sectors, company sizes and propensity to innovate.



***On a positive note, most SMEs rate their digital development as at least moderately advanced.***

Roughly one company in ten sees the progress of its digital strategy as advanced or highly advanced. At the same time, there is considerable room for improvement: ***almost one SME in five concedes to having no digital strategy or projects.***

The link between innovative behaviour and digitalisation is especially interesting. ***Companies that move early to experiment with and imple-***

***ment new technologies (pioneers) rate their digital maturity level much higher than late followers,*** which are also the most likely to lack a digital

strategy. The study shows how ***companies that try out and implement new technologies early demonstrate much greater digital maturity than late followers.***

The practical benefits stand out most among the ongoing digitalisation projects. ***SMEs mainly invest in projects to increase customer satisfaction, improve data use and develop process digitalisation and automation.*** These initiatives contribute directly to greater efficiency and competitiveness. By contrast, projects to develop new digital business models, introduce new technologies or increase employer attractiveness are less common.

The situation with regard to artificial intelligence (AI) is especially interesting: ***almost half of SMEs surveyed have yet to implement any AI-related projects.*** Although AI is a frequent subject of conversation, its deployment in the Swiss SME sector remains in its infancy.

SMEs consider the ***main strategic opportunities*** to lie in the corporate and innovation culture, in partnerships and in digitalisation and automation. Working from home is also more common than

## Almost half of SMEs surveyed have yet to implement any AI-related projects.

***ment new technologies (pioneers) rate their digital maturity level much higher than late followers,*** which are also the most likely to lack a digital

last year in the SME sector: ***61% of companies offer their staff the option of working from home at least on a part-time basis.***

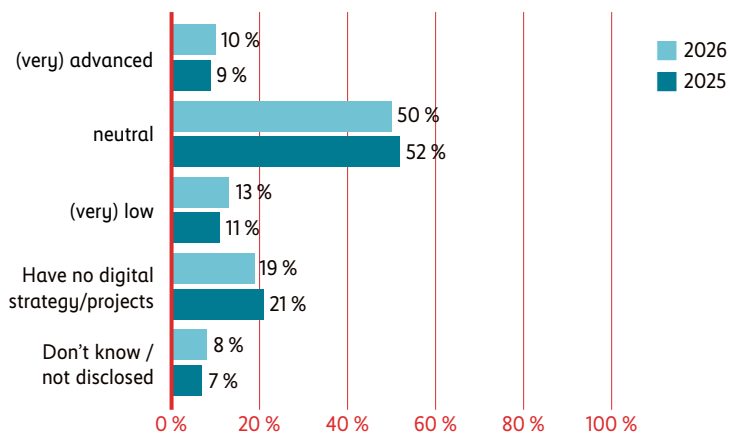
**SMEs see the global political and economic situation as the biggest strategic risk.** About a fifth to a quarter see inflation, cyber crime and skills deficits as strategic risks. The bigger companies in particular consider skills deficits and cyber crime as more acute risks.

Overall, the results show the following: digitalisation is ongoing among Swiss SMEs, however the focus is mainly on optimising existing business. To date, only a minority make active use of the really big opportunities of digital transformation, for example through new digital offerings, innovative business models or the targeted use of AI, which is where the main potential may lie for many companies over the next few years.

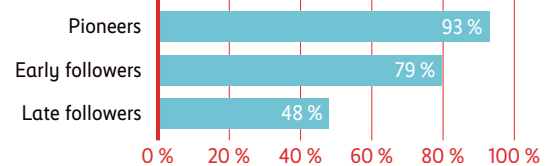
### Progress of digital strategy

Question: How do you rate the progress of your digital strategy or digital transformation?

Scale: 1–2: (very) low / 3–5: neutral / 6–7: (very) advanced.

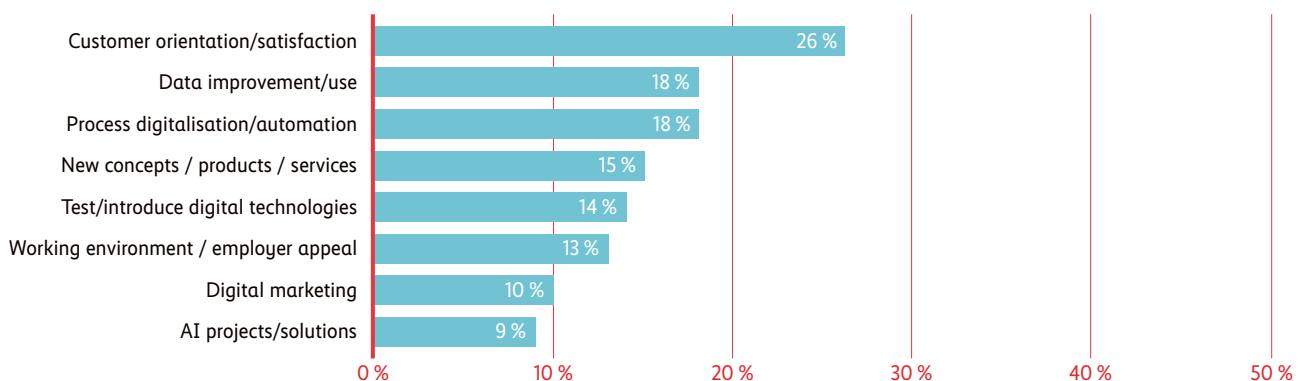


Of which (neutral/advanced)



### Strategic digital measures implemented

Question: Please state the extent to which your company has implemented the following measures in the past three years on a scale of 1–7. Scale: 1–2: no, not implemented (at all) / 3–5: neutral / 6–7: (fully and completely) implemented. Results shown: Scale 6–7 ((fully and completely) implemented)



## 02 Digital sovereignty – a new subject area in current world politics

Geopolitical developments over recent years have shed light on a new issue: digital sovereignty. Digital sovereignty is **the ability of a company to make its own decisions as far as possible regarding data, technologies and digital dependencies**. However, this study shows that the topic is still in its infancy in the Swiss SME sector.

SMEs are strongest in the traditional areas of **data protection, data sovereignty and data storage**. More than a third of companies surveyed have already implemented specific measures in these fields. Many companies are actively working on **protection from cyber risks**. Companies evidently consider these areas as being of direct relevance and business critical.

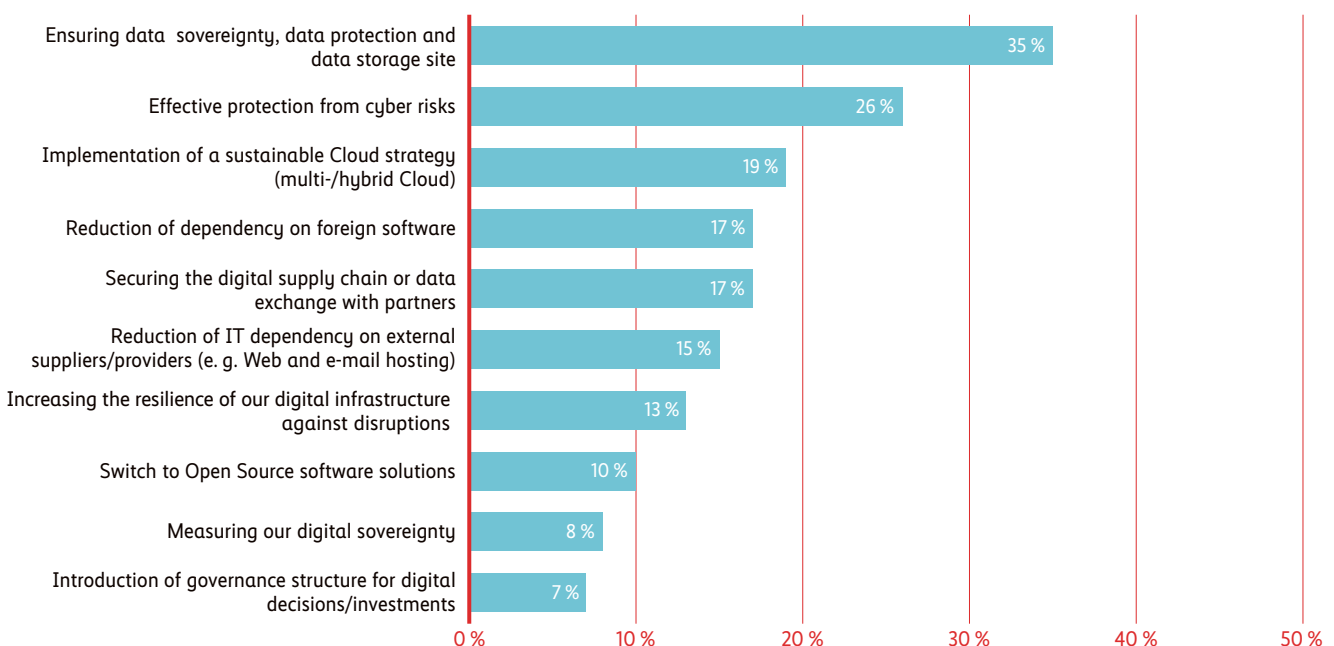
By contrast, measures to lessen **dependency on sole technologies or providers** are sparse by comparison. For example, only a minority of SMEs have already taken steps to reduce their dependency on foreign software, external IT service providers or cloud hosts. By the same token, such topics as securing the digital supply chain or switching to open source solutions have only been implemented in a piecemeal fashion to date.

Of particular interest is the finding **that many companies have still hardly heard about some aspects of digital sovereignty**. For example, about one quarter of respondents have no governance structures for digital decisions (only 7% have governance) and almost a third have never even addressed

### Digital sovereignty

Question: Have you already planned or implemented “digital sovereignty” measures?

Scale: 1 (never heard of it) to 4 (already implemented). Results shown: Scale 4 (already implemented)



the issue of their own digital sovereignty. These are the subjects most likely to become more important in future if companies wish to apply more systematic digital risk management.

Overall, the study shows that Swiss SMEs are actively addressing data protection and cyber security, but tend for the most part to see digital sovereignty solely through these factors. ***Many companies have yet to broach the broader subject of how to reduce their strategic dependency on***



## Many companies have still hardly heard about some aspects of digital sovereignty.

***technologies, platforms or individual providers.***

Moving early on these issues can strengthen resilience and enable greater independence of action in a growingly uncertain digital world.

## 03 Cyber crime – a problem to be taken seriously and that presents new threats through AI

Cyber crime is a longstanding agenda item on the management boards of Swiss SMEs. This study shows a strikingly clear picture: almost nine out of ten companies (88 %) see cyber crime as a problem to be taken seriously. The situation is largely identical across different company sizes, sectors and business types: ***cyber attacks are now a real threat to every SME.***

Of particular interest is that small and larger SMEs basically see the threat in the same light. It is immaterial whether a company only employs a few staff or several dozen persons: their threat perception is broadly identical. Cyber crime is now seen as a challenge by the entire Swiss SME landscape.

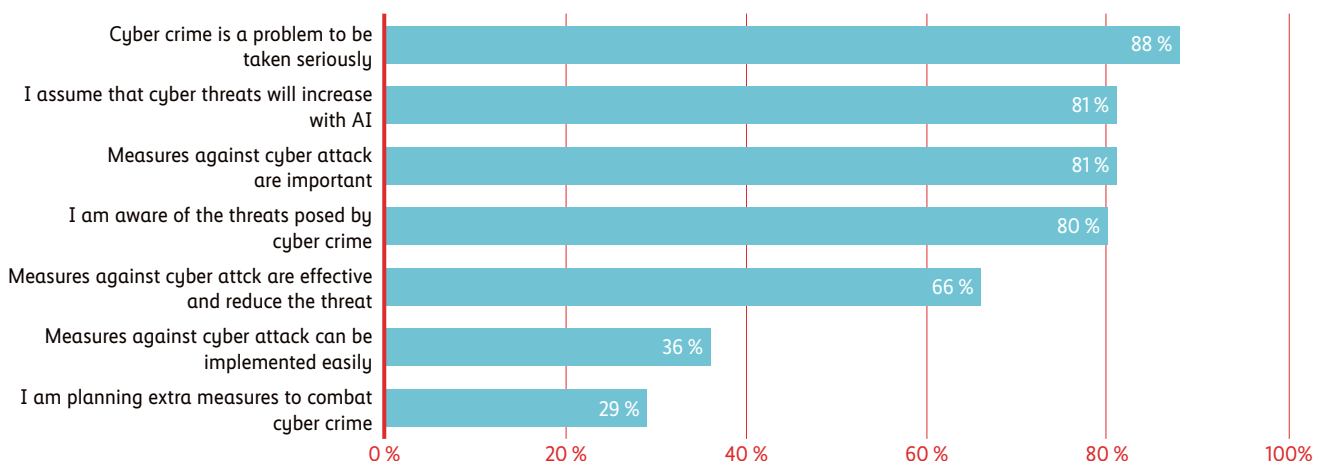
### Well prepared SMEs thus do not see increased threats but increased scope for action.

The study also reveals for the first time that companies are not just concerned about existing cyber risks. ***Four out of five SMEs (81%) believe that cyber threats will increase further through AI.*** Only a very small minority does not subscribe to this view. AI is thus not only seen as an opportunity by many companies but also as a new risk factor.

However, the study also reveals a key finding: it's not enough to just be aware of the problem. Companies that consider themselves better informed about cyber security and have already implemented technical or organisational protective measures rate the scale of the risk as high as other companies. At the same time, the better

#### Perception of cyber crime

Question: To what extent do you agree with the following statements on cyber crime, for example malware, online fraud or hacking?  
Scale: 1 (not at all) to 5 (fully and completely). Results shown: Scale 4–5 (fully and completely)



prepared companies are much more confident that cyber risks can be effectively reduced. ***Well prepared SMEs thus do not only see increased threats but also increased scope for action.***

The broad conclusion is that Swiss SMEs see the threat of cyber crime more clearly than ever before. At the same time, the rapid advance of AI means many companies expect risks to grow still more acute. Raising awareness of the problem will thus not be a challenge over the years to come. The challenge will instead be to convert this awareness into specific protective measures and ongoing further training.



## 04 Cyber crime at SMEs: over 35 000 victims, often with serious consequences



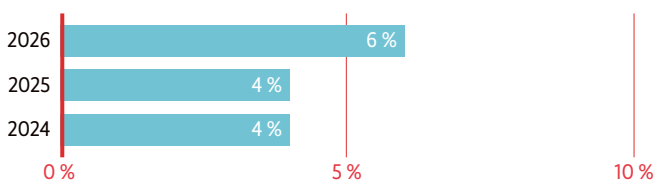
The nature of the losses incurred is particularly interesting. Contrary to public perception, these losses are not primarily financial in nature. **The main problem reported is the volume of work required to repair the damage, followed by the emotional burden.** Other factors such as financial loss, reputational damage and loss of client data are only reported thereafter. In many cases, cyber attacks thus primarily cost time and energy, while also affecting the nerves of the managers involved.

First, the good news: the vast majority of Swiss SMEs have been spared from serious (known) cyber attacks over the past three years. Nonetheless, the study shows that cyber crime can have serious consequences for those companies affected. Six percent of SMEs surveyed (extrapolating to over 35 000 SMEs in Switzerland) admitted to having suffered a cyber attack in the past three years (statistical range: 35 200–36 700 SMEs). Many of those affected reported that the attack caused financial loss, reputational problems, great inconvenience or took a major personal toll. The proportion of affected companies with at least ten employees is considerably higher, going up to 16%.

Another important finding was that there is no typical attack. **Successful attacks occur in a number of ways. The most common forms are phishing, password hacking, malware or network and server attacks, each of which are involved in about a third of incidents.** In other words, SMEs do not just face one specific threat. Instead they have to ward off a full range of different types of attack.

### Cyber attacks resulting in losses

Question: Has your company suffered a cyber attack in the past three years leading to a financial loss or reputational damage, entailing considerable effort to rectify the damage or exerting a major emotional impact on you? (Answer: yes)



## The most frequent problem reported is the volume of work required to repair the damage.

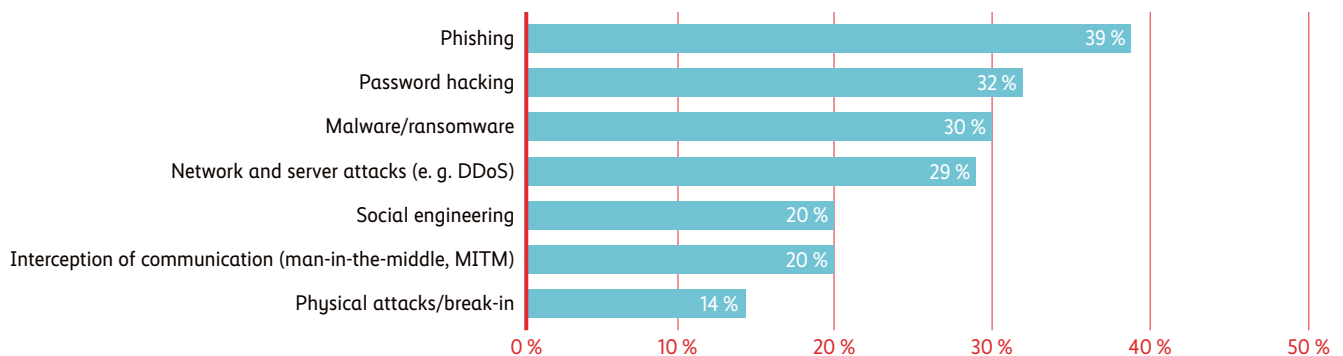
### **Blackmail is also an issue.**

About seven percent of companies surveyed (extrapolating to about 45 000 SMEs in Switzerland) have already been blackmailed by cyber criminals (statistical range: 43 300–45 380 SMEs). Larger SMEs and companies in industry or construction are particularly affected. In some cases, the companies even paid out ransoms. This shows that cyber crime has long been more than a purely technical issue and is increasingly evolving into a business and strategic challenge.

The results leave no room for doubt: even if only a minority of SMEs have been directly impacted, a successful attack can involve major consequences. The size of a company is irrelevant in the face of a cyber attack; being well prepared for different attack scenarios and having cover against financial losses are what matter.

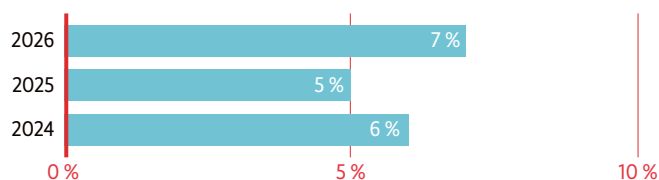
### **Type of attack**

Question: What type of attack have you suffered? (Filter: for cyber attack)



### **Blackmail**

Question: Has your company been blackmailed by cyber criminals? (Answer: yes)



## 05 Knowledge of cyber threat situation and support

The latest survey shows that many Swiss SMEs feel well equipped to deal with cyber risks. **Almost half the companies say they are well enough informed about the key cyber threats relevant to their business.** In addition, many respondents believe that they know where they can receive information, support or specific recommendations on what to do in an emergency.

It is also encouraging that **40 % of companies would be prepared to voluntarily report relevant cyber incidents to the National Cyber Security Centre (NCSC).** A basic awareness of the importance of exchanging information and cooperation thus seems to exist.

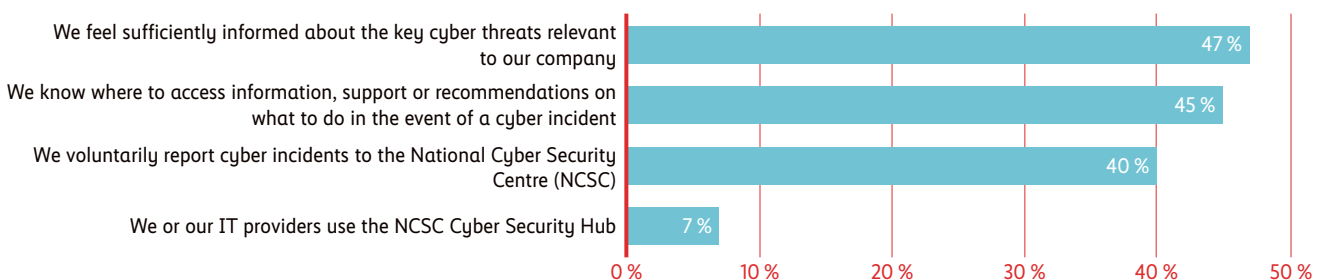
The study shows that SMEs could still make more use of the Cyber Security Hub, especially the very small ones. The NCSC Cyber Security Hub is only used by about seven percent of companies or their IT service providers. The Cyber Security Hub is primarily intended for critical infrastructure operators and their service providers. However, SMEs can also join and access its offering.



### Knowledge of cyber threat situation and support

Question: To what extent do the following statements apply?

Scale: 1 (does not apply at all) to 5 (applies fully and completely). Results shown: Scale 4–5 (fully and completely)



It is also noticeable that ***larger SMEs are more aware of the support available to them than their smaller counterparts.*** Companies with 10 to 49 employees are a lot more likely to have specific knowledge of whom they can contact in a cyber emergency and much more frequently use the support available to them, such as that offered by the Cyber Security Hub. Smaller companies appear to rely more on their general knowledge or on external partners.

## Larger SMEs know more than their smaller counterparts about where to access support.

The results indicate that many SMEs tend to assess their cyber resilience on the basis of personal knowledge. Their organisational preparation for a cyber incident is, however, not so advanced in some ways. ***Contingency arrangements, defined processes and the use of specialised support can make all the difference if there is an incident.***

Many SMEs feel well informed and believe they know whom to contact for support. At the same time, security concepts, contingency planning and audits are often lacking. The results thus indicate a gap between perceived and organisationally embedded cyber resilience.

## 06 Cyber security is growing in importance and regaining significance

Following a decline last year, the subject of cyber security has significantly regained priority this year for Swiss SMEs. In 2026, 46 % of companies surveyed rated cyber security as important or very important. This is up from 33 % in 2025. **In other words, cyber security is again taken as seriously as in prior years,**

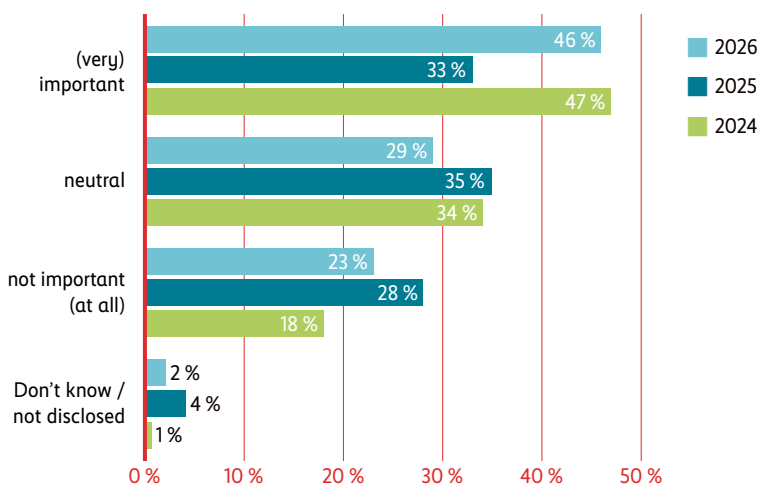
especially among companies with ten or more staff. **About six in ten companies in this category treat cyber security as a high priority.** Technologically advanced companies, i.e. pioneers or early followers, also take cyber security much more seriously than less innovative entities (late followers).

**Sensitivity to cyber risks increases with company size.**

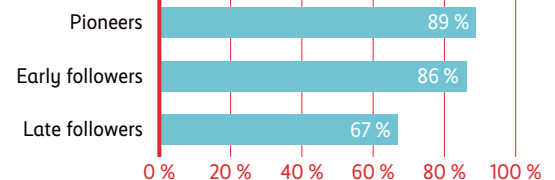
### Prioritising cyber security

Question: How much of a priority is cyber security in your company?

Scale: 1-2: not important (at all) / 3: neutral / 4-5: (very) important



Of which (neutral / very important)



***This increased vigilance has not arisen through chance.*** The study shows that cyber crime is currently one of the key strategic risks for Swiss SMEs. At 23% of nominations, it is practically on a par with inflation and cost increases as well as skills deficits. Only global political and economic uncertainties rank slightly higher as a long-term risk.

***It is particularly noteworthy that sensitivity to cyber risks increases in line with company size.***

Over a third of companies with 20 to 49 staff already see cyber crime as one of their main strategic risks, placing it a lot higher on the list of risks for this category of company.

The results on the whole give a clear picture: Swiss SMEs are increasingly recognising that cyber security is not just a technical IT issue but a strategic business matter. Protection of data, processes and business relationships is again becoming more of a priority at management level in view of growing digital dependencies, new threats and professional cyber criminals.



## 07 Cyber risk responsibility: more SMEs are allocating responsibilities

This study shows a positive trend: **Swiss SMEs are increasingly allocating clear responsibilities with regard to cyber security.** There was a time when cyber risks tended to be treated as an incidental inconvenience. However, now there are more companies assigning responsibility to a designated person for managing these issues.

The increase in the proportion of companies assigning responsibility for cyber security to one person **as a subtask** has been especially pronounced, rising from 15 % to 21 % within a year. **Moreover, almost one SME in ten even has a special function with clearly defined responsibilities for cyber security.**

**Many companies also rely on external support**, with over a quarter of SMEs surveyed working with an external partner to manage cyber risks. This can be an efficient way of compensating for a lack of in-house resources or expertise, especially for smaller companies.

The biggest change, however, has been among those companies that have largely ignored cyber security to date. The proportion of SMEs for which cyber risks have no priority is down from 42 % in 2025 to 36 % this year. The change is even evident among the smallest companies employing one to three staff. **This signals heightened cyber risk awareness, even among the smallest businesses.**

**Many companies rely on external support.**

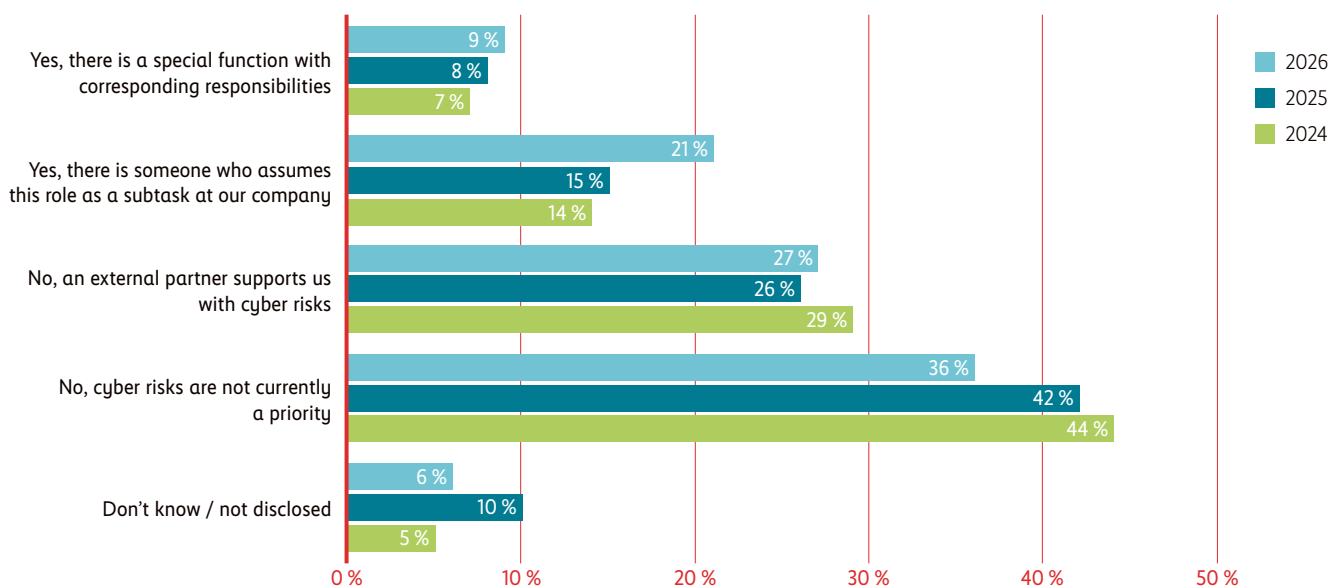


The difference among companies of different sizes is striking: responsibility for risk management is a lot more likely to be clearly designated at companies with 10 or more employees, whether in-house or with external support. Moreover, these companies are much less likely to consider cyber risk a “non-priority issue”.

Overall, the results show that the Swiss SME sector is increasingly reclassifying cyber security from a technical issue to a managerial one. The main conclusion drawn in this context is that not every SME needs its own cyber security manager. What is required instead is clear role allocation, so people know who is responsible for what within the company and who is to take over in an emergency.

### Responsibility for cyber risks

Question: Does your company have one or more persons who are responsible for cyber security?



## 08 Implementation of technical cyber security measures

Swiss SMEs are still investing primarily in proven technical protective measures. Regular software updates are the most common: over 80 % of companies consistently conduct these updates. Firewalls, data backups and two-way or multi-factor authentication (MFA) are also widespread. These measures currently form the basis underpinning cyber security at most SMEs.

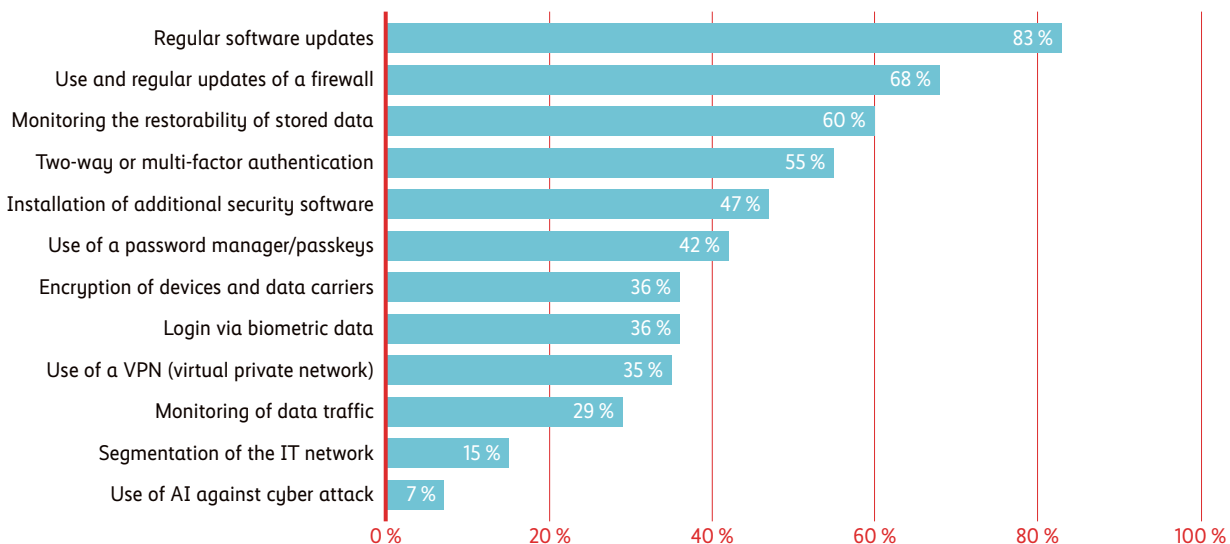
Advanced protective mechanisms, by contrast, are not nearly as popular. They include, for example, monitoring data traffic, segmenting networks and using AI to protect against cyber attacks. There is a great divide between technological pioneers and late followers in these areas. Innovative com-

panies are increasingly making use of these measures, while many other SMEs continue to rely on the basic traditional methods.

The finding on the use of backups is particularly pleasing: **nine out of ten Swiss SMEs currently conduct regular data backups**. The proportion of companies that do not regularly back up their data is down to just four percent. In addition, more and more companies are using a combination of local data storage and cloud backup. This approach improves reliability and reduces the risk of complete data loss.

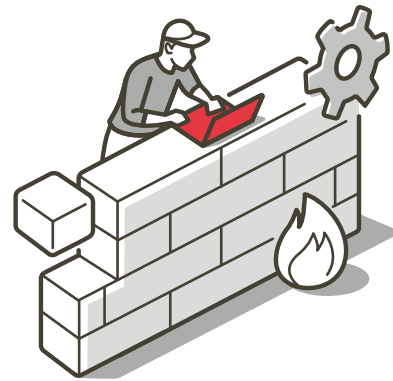
### Technical cyber security measures

Question: To what extent have the following technical measures to enhance cyber security been implemented at your company?  
Scale: 1-2: not (at all) / 3-5: neutral / 6-7: (fully and) completely. Results shown: Scale 6-7 (fully and completely implemented)



The storage location of the backups is also interesting. ***Approximately three quarters of companies that back up their data store it in Switzerland.*** Only a few store their backups outside Europe. This demonstrates that data sovereignty and control of sensitive company information are important to many SMEs.

The main vulnerability, however, lies elsewhere: a backup only helps if it actually works in an emergency. Although regular data backups are currently standard practice, ***only a quarter of SMEs regularly restore their backups for test purposes.*** As a result, many companies cannot be sure whether their data could actually be restored following a cyber attack, technical fault or operating error.



## Nine out of ten Swiss SMEs conduct regular data backups.

Overall, the results show the following: many SMEs employ basic technical measures. However, deficiencies persist with regard to access protection, monitoring, segmentation and tested restoring. There has been major progress in recent years, particularly in backing up data. However, the next challenge involves not only backing up data but also regularly testing data restoration. It is not enough merely to have a backup if a major event occurs. The data must also be accessible.

## 09 Implementation of organisational cyber security measures



The study shows that Swiss SMEs mainly use technical preventive measures to ensure cyber security. **Organisational measures, on the other hand, are much less common.** Basic procedural rules such as the careful handling of personal information, use of secure passwords and the scrutiny of suspicious documents or e-mails are the most common practices. These measures are now firmly established at the great majority of companies.

However, once overarching processes and structures come into play, the degree of implementation falls markedly. **Only about a third of SMEs systematically complete inventories of their IT systems and cloud services or conduct regular employee training.** There is even less evidence of contingency

planning for business continuation, evaluation of suppliers' IT security, formal security concepts and data classification by degree of sensitivity. **Security audits are the least common protective measure.**

The impact of company size is particularly striking. While the basic procedural rules are broadly followed to the same extent at both small and large SMEs, professionalisation increases markedly in line with the number of staff. Companies with 10 to 49 employees are considerably more likely to have contingency planning, IT security support, security guidelines and regular audits than the smallest companies.

Knowledge of cyber security reveals another interesting correlation. Companies that feel they are well informed about cyber risks apply organisational protective measures much more often than businesses that are less informed. This applies to

**Only about a third of SMEs systematically complete inventories of their IT systems and cloud services or provide regular employee training.**

almost all reviewed areas, from employee training through contingency planning to security concepts. The only exception is security audits and the classification of sensitive data. The higher the information level, the higher the degree of implementation of organisational protective measures.

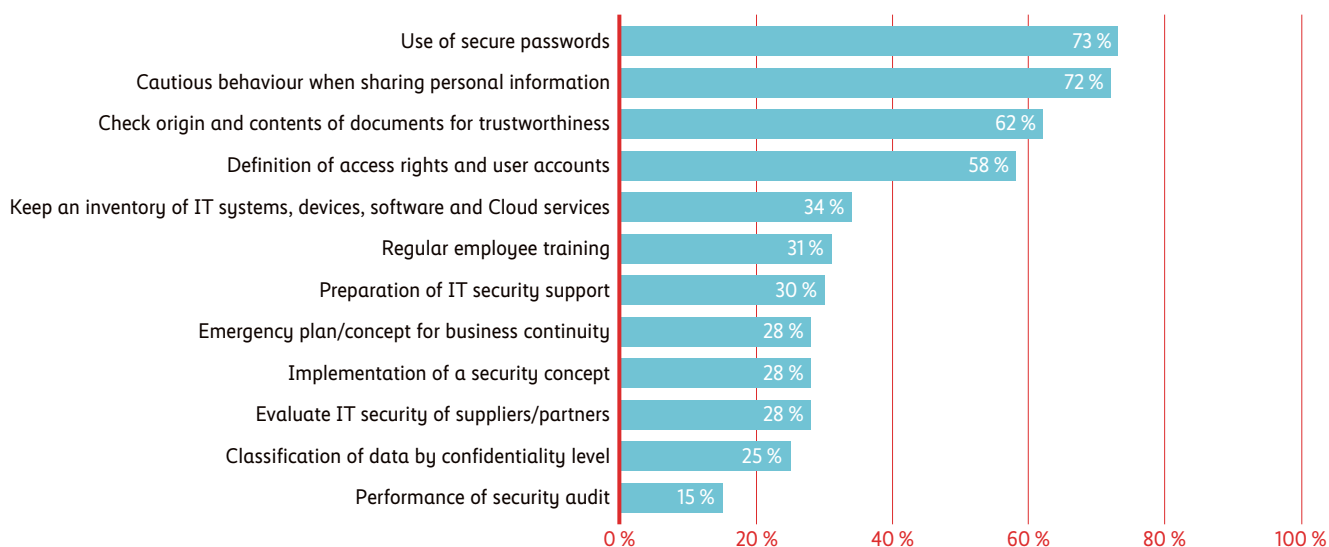
The innovation culture also plays a big part. Companies that embrace technology and early followers employ many more protective measures than late followers, which are much less likely to have structured security processes and record low values more often than average when reporting on their organisational protective measures.

The results show a clear picture overall: most SMEs know how to be prudent when going about their daily business. ***The real challenge, however, lies in placing cyber security on a firm footing at the organisational level.*** Contingency plans, training, supplier evaluations and regular security audits are often less visible than, for example, firewalls. Nonetheless, they can make all the difference in an emergency when determining how quickly a company can react to a cyber incident and remain operational.

### Organisational cyber security measures

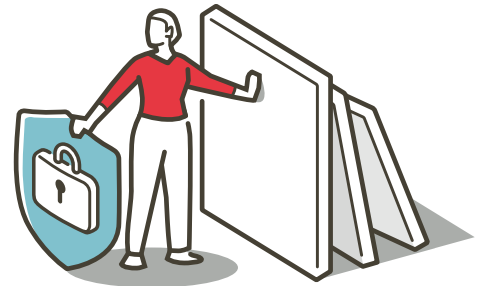
Question: To what extent have the following technical measures to enhance cyber security been implemented at your company?

Scale: 1-2: not (at all) / 3-5: neutral / 6-7: (fully and) completely. Results shown: Scale 6-7 (fully and completely implemented)



## 10 The future: cyber resilience is becoming more important, but many SMEs remain cautious

The study shows a fundamentally positive picture of cyber resilience among Swiss SMEs. Every second company believes they are well or very well protected from cyber attack and prepared for an incident. This is slightly higher than in the previous year. The larger companies and technologically advanced entities are particularly confident. **Digitalisation pioneers rate their resilience much higher than late followers, which are much more critical of their cyber resilience.**



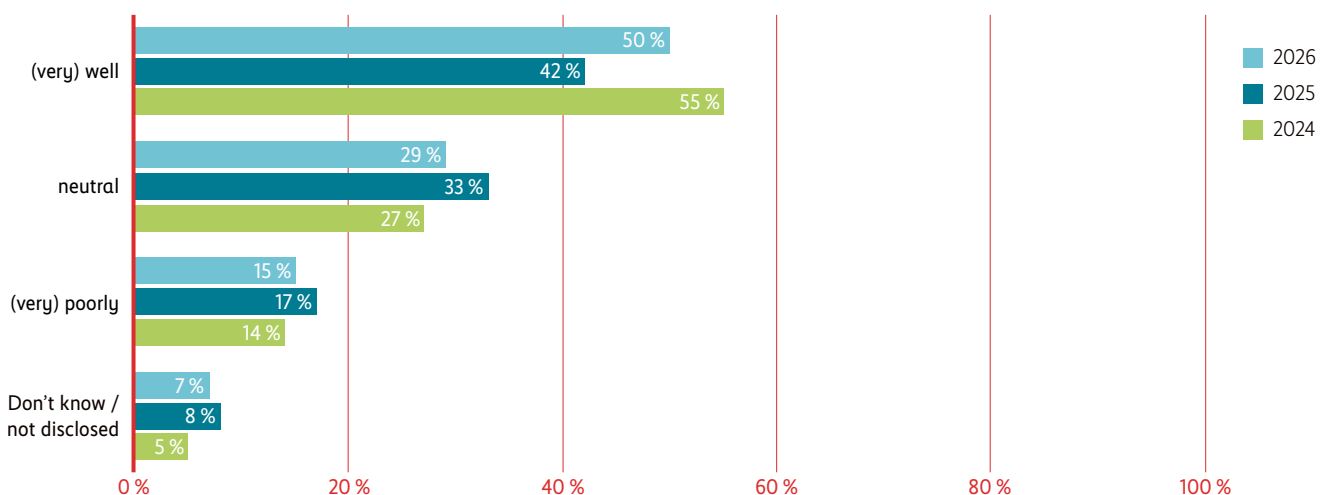
At the same time, the subject of cyber security is gaining in strategic significance. Having receded as a priority in the previous year, almost one in two SMEs now rates cyber security as important or very important. The issue has thus once again moved up the agenda, particularly among companies with more than ten employees. Innovative companies also attribute higher than average importance to cyber security.

The future looks exciting: **about two in five SMEs say extra security measures in the next one to three years are (very) likely.** Preparedness increases in line with company size and the information level. Those companies that consider themselves well informed about cyber security plan additional investment much more often than less well informed businesses.

### Cyber resilience

Question: In your estimation: How well protected are you from cyber attacks and prepared for an attack?

Scale: 1-2: (very) poorly / 3: neutral / 4-5: (very) well



## Cyber resilience does not just mean preventing attacks, but also being able to return quickly to business as normal following an incident.

However, there appears to be a paradox despite the high level of awareness of the cyber issue. Although cyber crime is clearly perceived as a threat to be taken seriously in other parts of the questionnaire, a majority of SMEs at the same time see the risk of a cyber attack entailing at least one day of business interruption in the next two to three years as rather small. Only about one in ten companies rates this risk as high. The risk is only really taken seriously by the larger SMEs.

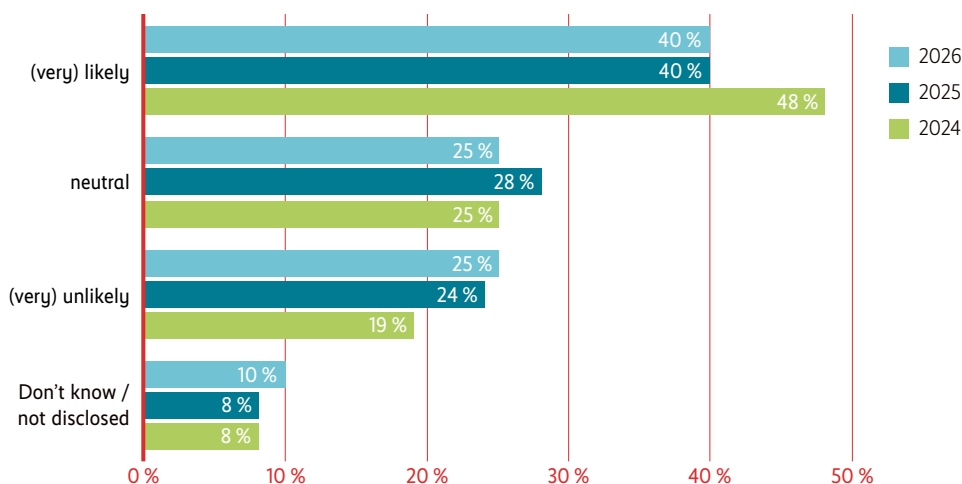
The results indicate that many companies have more confidence in their own resilience than they may have done in the past, but at the same time are susceptible to underestimating the effects of a

potential incident. ***Cyber resilience does not just mean preventing attacks, but also being able to return quickly to business as normal following an incident.*** That is why the ongoing improvement of protective measures, contingency planning and regular in-house security checks will become more important over the next few years.

### Increased cyber security measures

Question: How likely are you to take additional security measures against cyber crime in the next 1-3 years?

Scale: 1-2: (very) unlikely / 3: neutral / 4-5: (very) likely



# Implementation

## Cyber security and cyber resilience checklist for Swiss SMEs

The study results show that: many SMEs have a good command of the basics. The greatest potential for improvement currently stems from organisational measures, contingency planning and the regular review of the effectiveness of existing protective measures. This checklist will help you strengthen your cyber resilience.

### Technical cyber security measures

#### 1. Securing the basics

- ☐ Regularly update all the operating systems, applications and devices.
- ☐ Install a firewall and update it regularly.
- ☐ Activate multi-factor authentication (MFA) for e-mail, cloud services and critical systems.
- ☐ Use extra security software (ERD / endpoint protection, antivirus).
- ☐ Use password manager or passkeys.

#### 2. Protect data

- ☐ Back up data on a regular basis.
- ☐ Store backups locally and in the cloud.
- ☐ Ensure backed up data is stored in Switzerland wherever possible.
- ☐ Test the restoration of backed up data regularly. A backup only helps if it can be restored in an emergency.
- ☐ Encrypt devices, data carriers and sensitive data.

#### 3. Secure infrastructure

- ☐ Use VPN solutions for external access.
- ☐ Employ a biometric login procedure where it adds value.
- ☐ Monitor data traffic and suspicious activities.
- ☐ Keep discrete critical systems through network segmentation.
- ☐ Review potential of AI-based protection solutions.

## Organisational cyber security measures

### 1. Raise employee awareness

- ☐ Establish clear rules for dealing with personal and confidential information.
- ☐ Introduce mandatory secure password rules.
- ☐ Review e-mails, links and documents to ensure they can be trusted.
- ☐ Provide employees with regular training in cyber risks.

### 2. Establish structures and responsibilities

- ☐ Allocate clear cyber security-related responsibilities.
- ☐ Systematically manage access rights and user accounts.
- ☐ Make an inventory of all IT systems, devices, software packages and cloud services.
- ☐ Organise in-house or external IT security support.
- ☐ Document the security concept for the company.

### 3. Increase resilience

- ☐ Create a contingency plan and concept for business continuity.
- ☐ Define responsibilities in the event of a crisis.
- ☐ Know where support is available in an emergency (IT service provider, insurer, National Cyber Security Centre (NCSC)).
- ☐ Report relevant cyber incidents to the National Cyber Security Centre (NCSC).

### 4. Monitor risks regularly

- ☐ Evaluate IT security of suppliers and business partners.
- ☐ Classify data according to need for protection.
- ☐ Conduct regular security audits.
- ☐ Review digital dependencies of individual providers, platforms or cloud services.

Cyber resilience is not just about preventing attacks. Successful companies know how to recognise an attack, contain the damage, quickly restore operations and learn from what happened.

## Practical tools to strengthen your cyber security

### Cyber test for SMEs

- Find out with this self assessment (in French, German and Italian) what hackers are looking for from you and obtain cyber tips tailored to your business.  
<https://www.mobiliar.ch/kampagne/cybertest>
- Find out your cyber score with IT Sec 4 KMU (in French and German) and define concrete measures to improve your cyber security.  
<https://itsec4kmu.ch/>

### National Cyber Security Centre NCSC

- Information for companies and authorities on protection and how to respond to cyber incidents, as well as on the obligation to report.  
<https://www.bacs.admin.ch/en/infos-companies-and-authorities>
- Information on the Cyber Security Hub (CSH)  
<https://www.bacs.admin.ch/en/information-about-the-csh>

### Cybersecurity Map

- The Cybersecurity Map provides decision-makers with a concise overview of major technological developments.  
<https://www.satw.ch/en/focus-topics/cybersecurity/satw-cybersecurity-map>

## Research methodology

The aim of this study was to establish the position of Swiss SMEs with regard to cyber crime, cyber security and digitalisation.

Five hundred and seven interviews via online questionnaire were conducted from 24 June to 10 July 2026 with managers of SMEs with 1–49 employees. The invitation procedure was based on the YouGov internet panel with about 115 000 members.

The sample was compiled disproportionately on the basis of quotas by company size and linguistic region and then weighted proportionally.

The sample covers about 614 400 companies with 1 to 49 employees (FOS STATENT, 2025) in all parts of the country. The confidence interval for the total sample is  $\pm 4.4$  percentage points with a security level of 95 % (50/50 distribution).

The weighted sample shows a structurally homogeneous universe in terms of company size and language region. The results can thus be extrapolated taking account of the confidence interval.

Contact YouGov:  
Karin Mändli Lerch,  
[karin.maendlilerch@yougov.ch](mailto:karin.maendlilerch@yougov.ch)

## Contact authors



Marc K. Peter  
Professor of Digital Business  
HES-SO Valais-Wallis School of Management  
marckurt.peter@hes-so.ch



Romain Geiser  
NCS Program Manager  
National Cyber Security Centre  
ncs@ncsc.admin.ch



Anu Anthamatten  
Senior Project Manager  
digitalswitzerland, Zurich  
anu@digitalswitzerland.com



Léonard Marbe  
Senior Marketing Manager  
La Mobilière  
leonard.marbe@mobiliar.ch



Anna V. Rozumowski  
Lecturer and Course Director  
HWZ University of Applied Sciences in Business  
Administration Zurich  
anna.rozumowski@fh-hwz.ch



Tobias Schlegel  
Head of Tech Intelligence  
SATW Swiss Academy of Engineering Sciences  
tobias.schlegel@satw.ch



Karin Mändli Lerch  
Senior Research Consultant  
YouGov  
karin.maendlilerch@yougov.ch

Marc K. Peter, Romain Geiser, Anu Anthamatten,  
Léonard Marbe, Anna V. Rozumowski,  
Tobias Schlegel and Karin Mändli Lerch:

### **SME cyber security in 2026**

A study by la Mobilière in cooperation  
with the NCSC, digitalswitzerland, HES-SO,  
HWZ and SATW

- National Cyber Security Centre NCSC
- La Mobilière
- digitalswitzerland
- HES-SO Valais-Wallis School of Management
- HWZ University of Applied Sciences in Business  
Administration Zurich
- SATW Swiss Academy  
of Engineering Sciences
- YouGov

cyberstudie.ch  
Bern and Zurich, October 2026

## Imprint

Marc K. Peter, Romain Geiser, Anu Anthamatten, Léonard Marbe, Anna V. Rozumowski,  
Tobias Schlegel and Karin Mändli Lerch

SME cyber security in 2026:

A study by la Mobilière in cooperation with the NCSC, digitalswitzerland, HES-SO, HWZ and SATW

National Cyber Security Centre NCSC, la Mobilière, digitalswitzerland, HES-SO Valais-Wallis School of  
Management, HWZ University of Applied Sciences in Business Administration Zurich, SATW Swiss  
Academy of Engineering Sciences, YouGov  
Bern and Zurich, October 2026

Great care was taken in the preparation of this work. Nonetheless, the authors and research partners  
involved accept no liability of any kind, including for this work, with regard to the accuracy of the  
information, indications and advice or for any print errors.

All rights, including translation into other languages, remain reserved.  
The rights over the brand names lie with their respective owners.

No part of this work may be reproduced in any form without the written approval of the authors or  
transmitted and/or translated into a language usable by machines, especially data processing software.

Coordination of this publication: Prof. Marc K. Peter,  
HES-SO Valais-Wallis School of Management

With the cooperation of Thomas Burkhardt (YouGov), Michèle C. Kaufmann (YouGov), Kenza Leclere  
(NCSC), Bettina Mavrommatis (NCSC) and David Torcasso (digitalswitzerland).

Design: Media design team, la Mobilière  
Illustration: Livia Lüthi

The set of slides with all the survey results is available on the websites of the study partners or at  
cyberstudie.ch.