SME Cybersecurity 2025

IT security in Swiss SMEs and IT service providers

Marc K. Peter, Martina Dalla Vecchia, Katja Dörlemann, Kristof A. Hertig, Andreas W. Kaelin, Manuel Kugler, Karin Mändli Lerch & Simon B. Seebeck

www.cyberstudie.ch

Source:
Marc K. Peter, Martina Dalla Vecchia, Katja Dörlemann, Kristof A. Hertig, Andreas W. Kaelin, Manuel Kugler, Karin Mändli Lerch & Simon B. Seebeck (2025): SME Cybersecurity 2025: IT security in Swiss SMEs and IT service providers (www.cyberstudie.ch).

digitalswitzerland, Die Mobiliar, Swiss Academy of Technical Sciences SATW, Information Security Society Switzerland ISSS, Swiss Internet Security Alliance SISA, Swiss Digital Security Alliance ADSS, University of Applied Sciences Northwestern Switzerland FHNW, HES-SO Valais-Wallis School of Management, YouGov Switzerland.

Research report and infographic in German, English, French and Italian are available at **www.cyberstudie.ch**

digitalswitzerland · die Mobiliar · satw · /SSS information security society switzerland · SWISS INTERNET SECURITY ALLIANCE · ALLIANCE DIGITAL SECURITY SWITZERLAND · n|w University of Applied Sciences and Arts Northwestern Switzerland School of Business · Hes·so VALAIS WALLIS School of Management · YouGov

SME Cybersecurity 2025

IT security in Swiss SMEs and IT service providers

Cybersecurity feeling regarding cybercrime

	We feel (very) safe	Neutral	We feel (very) insecure
Pioneers	58 %	39 %	–
Early followers	51 %	37 %	10 %
Late followers	52 %	37 %	6 %
All SMEs	52 %	33 %	9 %
IT service companies	65 %	22 %	10 %

Cyberresilience: protection against cyberattacks

	We are (very) well prepared	Neutral	We are (very) poorly prepared
Pioneers	48 %	50 %	–
Early followers	55 %	33 %	11 %
Late followers	32 %	36 %	24 %
All SMEs	42 %	33 %	17 %
IT service companies	68 %	24 %	7 %

Degree of information on cyber issues

Mean on the scale from
1 (very poorly informed) to 5 (very well informed)

Pioneers	3.6
Early followers	3.5
Late followers	3.2
All SMEs	3.3
IT service companies	4.1

Blackmailed by cybercriminals

Pioneers	–
Early followers	3 %
Late followers	6 %
All SMEs	5 %
IT service companies	4 %

Money payments due to fraudulent emails

Pioneers	–
Early followers	3 %
Late followers	6 %
All SMEs	4 %
IT service companies	2 %

Risk assessment of cyberattacks

	(Very) High Risk	Neutral	(Very) Small Risk
Pioneers	25 %	13 %	58 %
Early followers	15 %	31 %	48 %
Late followers	6 %	30 %	59 %
All SMEs	10 %	28 %	54 %
IT service companies	18 %	28 %	51 %

Cyberrisk responsibility in the company

	Special function	Subtask of a function	External partners	No one/ no priority
Pioneers	39 %	19 %	29 %	14 %
Early followers	9 %	19 %	31 %	36 %
Late followers	4 %	11 %	25 %	50 %
All SMEs	8 %	15 %	26 %	42 %

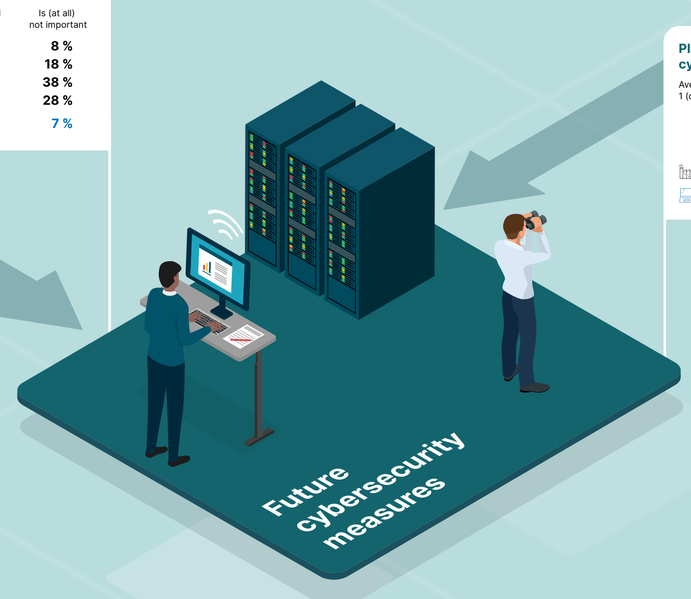
Cybersecurity Priority

	Is (very) important	Neutral	Is (at all) not important
Pioneers	55 %	37 %	8 %
Early followers	42 %	39 %	18 %
Late followers	23 %	36 %	38 %
All SMEs	33 %	35 %	28 %
IT service companies	76 %	16 %	7 %

Planning of additional cybersecurity measures

Average on the scale from
1 (disagree at all) to 5 (strongly agree)

Pioneers	3.6
Early followers	3.4
Late followers	3.1
All SMEs	3.2
IT service companies	4.0



Technical cybersecurity measures

Average value on a scale of 1 (not at all) to 5 (completely)

		Pioneers	Early Followers	Late Followers
Backup of data	87 %	–	–	–
Securing the Wi-Fi network with passwords	81 %	4.9	4.6	4.5
Regular update of the software	81 %	4.9	4.6	4.2
Use of a firewall	68 %	4.7	4.2	4.0
Installing additionally purchased software	62 %	4.4	4.1	3.7
Control Recoverability of data backup	61 %	4.6	4.1	3.7
Enable existing security software	55 %	4.0	3.9	3.6
Two-way or re-authentication (2FA/MFA)	53 %	4.2	3.7	3.4
Use of a password manager	42 %	4.5	3.4	2.8
Login by biometric data or passkeys	38 %	3.9	3.2	2.5
Use of Artificial Intelligence (AI)	8 %	2.1	1.9	1.6

Organisational cybersecurity measures

Average value on a scale of 1 (not at all) to 5 (completely)

		Pioneers	Early Followers	Late Followers
Use of secure passwords	74 %	4.5	4.2	4.0
Caution when sharing personal information	70 %	4.4	4.2	3.9
Raising employees' awareness of phishing e-mails	67 %	4.6	4.3	3.7
Checking the origin and content of documents	66 %	4.5	4.0	3.9
Provision of IT security support	36 %	4.2	3.4	2.7
Regular training of employees	31 %	3.9	3.3	2.3
Contingency plan/concept for business continuity	30 %	3.9	3.2	2.4
Implementation of a security concept	30 %	4.0	3.2	2.5
Evaluate partner IT security	30 %	3.5	2.9	2.5
Conduct of security audit	20 %	3.3	2.5	2.0

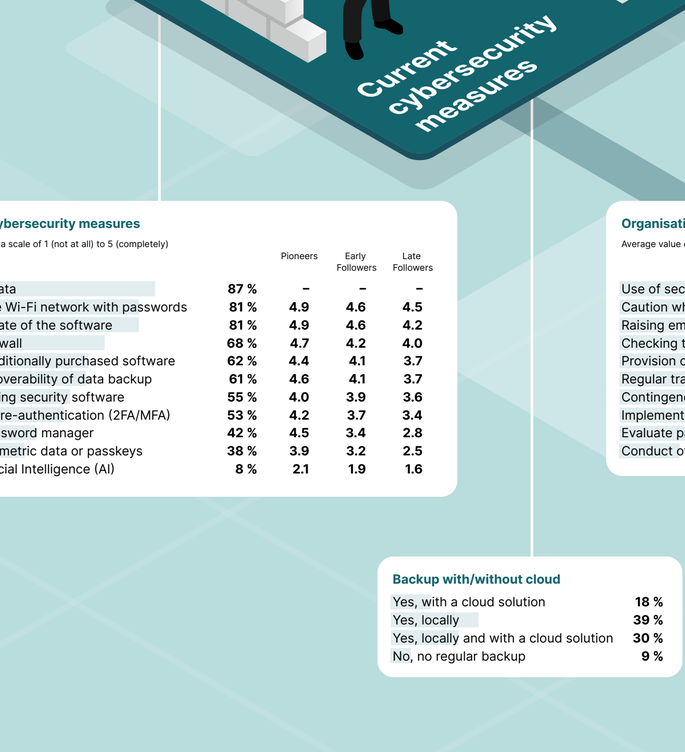
Backup with/without cloud

Yes, with a cloud solution	18 %
Yes, locally	39 %
Yes, locally and with a cloud solution	30 %
No, no regular backup	9 %

Attitude towards cybercrime

Cybercrime is a serious problem	88 %
Measures against cyber attacks are important	83 %
I am aware of the threats posed by cybercrime	80 %
Measures against cyber attacks are effective and reduce the risk	66 %
Measures against cyber attacks can be easily implemented	37 %
I am planning additional measures against cybercrime	29 %
My colleagues think that my company should protect itself against cyber attacks	24 %

Collaboration with IT service companies



Clarity regarding security certifications

	Yes	No	Don't know
Pioneers	72 %	21 %	7 %
Early followers	50 %	14 %	37 %
Late followers	36 %	14 %	50 %
All SMEs	44 %	13 %	43 %

Future demand for cyber security: Challenges for the industry

(open question, coded retrospectively)

Employee training	22 %
Financial resources / high investments	22 %
Lack of skilled personnel	17 %
Improving/updating IT infrastructure	12 %
Raising awareness of IT security among customers	12 %
Information gathering in general	7 %
Recognising the complexity of attack methods	6 %
Providing user-friendly applications	5 %

Number of external IT service partners

	One	Several	None
Pioneers	37 %	27 %	35 %
Early followers	34 %	24 %	38 %
Late followers	45 %	23 %	30 %
All SMEs	39 %	24 %	34 %

Collaboration with IT service companies

	from an SME perspective	from the perspective of IT service companies
Good price/performance ratio	46 %	28 %
Good (customer) service	43 %	37 %
Trust in the IT service company	40 %	51 %
Experience and expertise	30 %	57 %
Flexibility/adaptability to customer needs	23 %	24 %
Proximity, regionality	21 %	12 %
Knowledge of cybersecurity	19 %	18 %
Recommendations from colleagues etc.	19 %	21 %
Good reputation of the service company	18 %	24 %
Wide/diversified offer	7 %	3 %
Certifications, e.g. ISO 27001	5 %	10 %

Recommendations for increased cybersecurity

Take cybersecurity seriously	36 %
Train employees	26 %
Invest in IT / update infrastructure	15 %
Create financial resources	13 %
Control internal processes	10 %
Increase IT security in general	7 %
Provide specialist IT security personnel	6 %
Optimise passwords / 2FA	5 %
Regular data backup	5 %

Source:
Marc K. Peter, Martina Dalla Vecchia, Katja Dörlemann, Kristof A. Hertig, Andreas W. Kaelin, Manuel Kugler, Karin Mändli Lerch & Simon B. Seebeck (2025): SME Cybersecurity 2025: IT security in Swiss SMEs and IT service providers (www.cyberstudie.ch).

digitalswitzerland, Die Mobiliar, Swiss Academy of Technical Sciences SATW, Information Security Society Switzerland ISSS, Swiss Internet Security Alliance SISA, Swiss Digital Security Alliance ADSS, University of Applied Sciences Northwestern Switzerland FHNW, HES-SO Valais-Wallis School of Management, YouGov Switzerland.

Research report and infographic in German, English, French and Italian are available at **www.cyberstudie.ch**

SME Cybersecurity 2025

IT security in Swiss SMEs and IT service providers

Cyber attacks and the attitude of SME managers
As in 2024, 4 % of the companies surveyed in 2025 reported that they had been the victim of a cyber attack in the last three years. 5 % of companies had already been blackmailed by cyber criminals and 4 % had accidentally transferred money due to fraudulent emails. Accordingly, 88 % of respondents (9/10 of the SMEs surveyed) consider cybercrime to be a serious problem. Nevertheless, only 24 % feel social pressure from colleagues to take additional IT security measures.

IT security confidence and cyber resilience are declining
While 57 % of companies still felt secure in 2024, only 52 % feel secure in 2025. At the same time, the proportion of those who feel insecure is rising from 7 % to 9 %. The assessment of their own cyber resilience is also declining: only 42 % (2024: 55 %) consider their protection to be sufficient in the event of an attack, while 17 % (2024: 14 %) rate themselves as poorly protected.

The priority of cyber security is declining
Cyber security is becoming less important for small Swiss companies: for 28 % of them, the issue will no longer be a priority (2024: 18 %). However, cyber security remains a key concern for many larger companies with 10–49 employees and for technology pioneers.

Responsibility for cyber risks is increasingly being taken seriously
Responsibility is increasingly being taken seriously in small businesses. As of 2025, 23 % of small businesses have a person or function that is at least partially responsible for this issue (2024: 21 %).

Organisational protective measures are being neglected
Technical measures such as software updates, firewalls and data recovery tests are implemented by around two-thirds of companies. However, there is still room for improvement when it comes to organisational measures: only 20 % carry out IT security audits and only 30 % have an IT security concept, regularly train their employees or have an emergency plan.

Willingness to invest in cyber security is declining
Only 40 % of companies plan to increase their cyber security measures in the next 1–3 years – in 2024, the figure was 48 %.

IT service providers see a need for SMEs to catch up
IT service providers also see a need to invest: Only 39 % rate their SME customers as secure, while 14 % rate their customers' security as inadequate (2024: 12 %). In addition, the importance of cyber security is declining slightly among IT companies' customers (2024: 46 %, 2025: 43 %). On a positive note, 84 % of IT service providers expect an increase in demand for security measures from their SME customers.

Study methodology
The aim of the cyber study is to survey the attitudes of Swiss SMEs and IT service providers towards cybercrime. Between 25 June and 5 August 2025, 515 SME interviews and 336 interviews with IT service providers were conducted (via online questionnaires). In SMEs with 1 to 49 employees, people who make decisions regarding corporate strategy in their company, either alone or together with others, were interviewed. Of these, 26 describe themselves as digital pioneers who adopt digital technologies early on, 221 as early followers who adopt digital technologies shortly after their market launch, and 208 as late followers who only introduce digital technologies once they have been successfully used by others (not all participants answered this question). The IT service providers were invited to participate in writing. They were identified by NOGA codes 620200, 620300, 620900 and 631100.

Download the study presentation and infographic at www.cyberstudie.ch

Tips for safer Internet use

1. Check links in emails whose sender you don't know before clicking.
2. Do not share personal or sensitive information with unknown persons.
3. Shop at shopping sites you know or where you can verify the company.
4. Create a regular/automated backup of your data.
5. Automatically/regularly update the software on your mobile phone, tablet and laptop/computer.
6. Use strong passwords – use a password manager.
7. Where offered, enable two- or multi-factor authentication (2FA/MFA).
8. Use public Wi-Fi only when necessary and with a VPN.
9. Be sure to obtain information from trustworthy sources.
10. Report fraud to the police.

Further information:
iBarry – Tips and Checklists from the Internet Security Platform, www.ibarry.ch

iBarry
Internet security platform

Source:
Marc K. Peter, Martina Dalla Vecchia, Katja Dörlemann, Kristof A. Hertig, Andreas W. Kaelin, Manuel Kugler, Karin Mändli Lerch & Simon B. Seebeck (2025): SME Cybersecurity 2025: IT security in Swiss SMEs and IT service providers (www.cyberstudie.ch).

digitalswitzerland, Die Mobiliar, Swiss Academy of Technical Sciences SATW, Information Security Society Switzerland ISSS, Swiss Internet Security Alliance SISA, Swiss Digital Security Alliance ADSS, University of Applied Sciences Northwestern Switzerland FHNW, HES-SO Valais-Wallis School of Management, YouGov Switzerland.

Research report and infographic in German, English, French and Italian are available at **www.cyberstudie.ch**