2024 Cyber study

IT security in Swiss SMEs, IT service companies and the Swiss population

Marc K. Peter, Katja Dörlemann, Kristof Hertig, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian, Nicole Wettstein

www.cyberstudie.ch

Source:
Marc K. Peter, Katja Dörlemann, Kristof Hertig, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian, Nicole Wettstein (2024): Cyber study 2024: IT security in Swiss SMEs, IT service companies and the Swiss population.

digitalswitzerland, Die Mobiliar, Swiss Internet Security Alliance SISA, Swiss Digital Security Alliance ADSS, Swiss Academy of Technical Sciences SATW, University of Applied Sciences Northwestern Switzerland FHNW, YouGov Switzerland.

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

digitalswitzerland · die Mobiliar · SWISS INTERNET SECURITY ALLIANCE · ALLIANCE DIGITAL SECURITY SWITZERLAND · satw · n|w University of Applied Sciences and Arts Northwestern Switzerland School of Business · YouGov

2024 Cyber study

IT security in Swiss SMEs, IT service companies and the Swiss population

Cybersecurity feeling regarding cybercrime

	We feel (very) safe	Neutral	We feel (very) insecure
Pioneers	37 %	63 %	
Early followers	64 %	30 %	5 %
Late followers	53 %	34 %	11 %
All SMEs	57 %	33 %	7 %
IT service companies	77 %	19 %	3 %
Internet users (population)	47 %	39 %	8 %

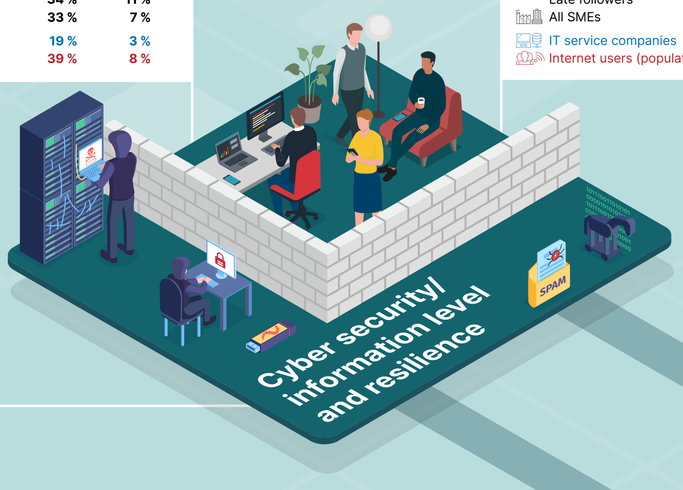
Cyberresilience: protection against cyberattacks

	We are (very) well prepared	Neutral	We are (very) poorly prepared
Pioneers	57 %	33 %	10 %
Early followers	59 %	27 %	13 %
Late followers	51 %	27 %	17 %
All SMEs	55 %	27 %	14 %
IT service companies	75 %	21 %	4 %
Internet users (population)	37 %	39 %	18 %

Degree of information on cyber issues

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

Pioneers	3.9
Early followers	3.5
Late followers	3.1
All SMEs	3.4
IT service companies	4.2
Internet users (population)	3.3



Blackmailed by cybercriminals (or cheated when shopping online)

Pioneers	1 %
Early followers	7 %
Late followers	5 %
All SMEs	6 %
IT service companies	5 %
Internet users (population)	

Internet users

Fraudulent online shopping

18–29 years	17 %
30–39 years	17 %
40–64 years	11 %
65–79 years	10 %

Risk assessment of cyberattacks

	(Very) High Risk	Neutral	(Very) Small Risk
Pioneers	11 %	22 %	53 %
Early followers	14 %	38 %	46 %
Late followers	11 %	27 %	58 %
All SMEs	12 %	30 %	51 %
IT service companies	17 %	32 %	49 %
Internet users (population)	16 %	37 %	38 %

Cyberrisk responsibility in the company

	Special function	Subtask of a function	External partners	No one/ no priority
Pioneers	20 %	21 %	23 %	34 %
Early followers	10 %	21 %	36 %	34 %
Late followers	4 %	9 %	26 %	58 %
All SMEs	7 %	14 %	29 %	44 %

Artificial Intelligence (AI) risk assessment

	Great danger	Neutral	Great opportunity
Pioneers	0 %	77 %	17 %
Early followers	7 %	78 %	10 %
Late followers	17 %	65 %	2 %
All SMEs	11 %	69 %	6 %
IT service companies	4 %	76 %	17 %
Internet users (population)	15 %	74 %	6 %

Internet users

Assessing cybersecurity in your own home

(Very) Safe	47 %	18–29 years	10 %
Neutral	39 %	30–39 years	13 %
(Very) Uncertain	8 % →	40–64 years	7 %
		65–79 years	6 %

Cybersecurity Priority

	Is (very) important	Neutral	Is (at all) not important
Pioneers	51 %	38 %	11 %
Early followers	63 %	25 %	11 %
Late followers	36 %	39 %	25 %
All SMEs	47 %	34 %	18 %
IT service companies	79 %	15 %	5 %

Planning of additional cybersecurity measures

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

Pioneers	3.1
Early followers	3.1
Late followers	2.6
All SMEs	2.9
IT service companies	3.6
Internet users (population)	3.0

Technical cybersecurity measures

		Pioneers	Early Followers	Late Followers
Backup of data	88 %	5.0	4.8	4.2
Regular update of the software	86 %	4.9	4.7	4.3
Securing the Wi-Fi network with passwords	83 %	4.7	4.7	4.3
Use of a firewall	79 %	4.7	4.6	4.2
Installing additionally purchased software	73 %	4.5	4.3	3.9
Control Recoverability of data backup	66 %	4.7	4.2	3.7
Enable existing security software	59 %	4.3	4.1	3.7
Two-way or re-authentication (2FA/MFA)	50 %	4.5	3.7	3.3
Use of a password manager	37 %	3.3	3.1	2.5
Login by biometric data or passkeys	34 %	3.7	2.9	2.6
Use of Artificial Intelligence (AI)	6 %	2.4	1.6	1.3
Average (SMEs)		4.3	3.9	3.5

Organisational cybersecurity measures

		Pioneers	Early Followers	Late Followers
Caution when sharing personal information	79 %	4.3	4.3	4.2
Use of secure passwords	76 %	4.4	4.3	4.0
Checking the origin and content of documents	72 %	3.7	4.1	3.9
Raising employees' awareness of phishing e-mails	67 %	3.7	4.2	3.7
Provision of IT security support	38 %	3.6	3.2	2.5
Evaluate partner IT security	34 %	2.9	3.1	2.6
Contingency plan/concept for business continuity	33 %	3.7	3.0	2.5
Regular training of employees	32 %	3.3	3.2	2.5
Implementation of a security concept	25 %	3.2	2.9	2.1
Conduct of security audit	19 %	2.6	2.4	1.9
Average (SMEs)		3.5	3.5	3.0

Internet users

Attitudes to cybercrime

Cybercrime is a serious problem	94 %
Measures against cyberattacks are important	90 %
I am aware of the threats posed by cybercrime	82 %
Measures against cyberattacks are effective	70 %
Measures against cyberattacks can be easily implemented	40 %
I plan additional measures against cybercrime	29 %

Internet users

Regular data backups

18–29 years	71 %
30–39 years	75 %
40–64 years	76 %
65–79 years	70 %

Internet users

Use of passwords

Always the same password	3 %
Almost always the same passwords	30 %
Almost never the same password	34 %
Never the same passwords	17 %
Use of a password manager	11 %

Internet users

Implementation of updates (at least monthly)

18–29 years	85 %
30–39 years	88 %
40–64 years	93 %
65–79 years	88 %

Internet users

Attend cybersecurity training courses

18–29 years	30 %
30–39 years	31 %
40–64 years	35 %
65–79 years	11 %

Internet users

Impact/disadvantages of a cyberattack

Data theft/loss	41 %
Financial consequences (e.g. theft of bank details)	33 %
Restricted access to device, data, software, Internet	11 %
Misuse of personal data / identity theft	8 %
Administrative / time expenditure	8 %
Theft of bank data	7 %
Mental stress, loss of confidence	6 %
Publication of data / damage to reputation	5 %

Collaboration with IT service companies

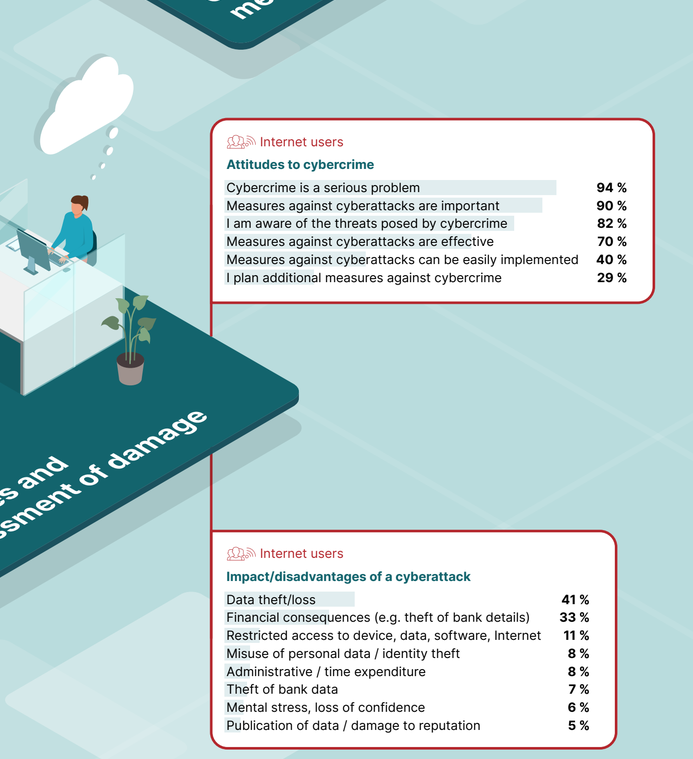
Clarity regarding security certifications (e.g. ISO 27001) of IT service companies

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

IT service companies

Cybersecurity in consulting/sales discussions

The topic is being actively worked on	57 %
Neutral	15 %
The topic is not being edited	23 %



Number of external IT service partners

	One	Several	None
Pioneers	48 %	16 %	36 %
Early followers	41 %	32 %	26 %
Late followers	50 %	17 %	32 %
All SMEs	43 %	24 %	32 %

Proportion of external IT work

Pioneers	18 %
Early followers	28 %
Late followers	16 %
All SMEs	20 %

IT service companies

Recommendations for increased cybersecurity

Taking safety seriously	43 %
Training of employees	29 %
Investing in IT / Updating infrastructure	13 %
Creating financial resources	11 %
Increase IT security in general	9 %
Control internal processes	6 %
Provide IT security specialists	6 %
Assessing risks	6 %
Draw up emergency plan	5 %

Collaboration with IT service companies

	from an SME perspective	from the perspective of IT service companies
Good (customer) service	41 %	38 %
Trust in the IT service company	39 %	54 %
Good price/performance ratio	39 %	28 %
Experience and expertise	30 %	60 %
Proximity, regionality	28 %	13 %
Flexibility/adaptability to customer needs	23 %	25 %
Knowledge of cybersecurity	21 %	22 %
Recommendations from colleagues etc.	14 %	18 %
Good reputation of the service company	14 %	21 %
Certifications, e.g. ISO 27001	7 %	10 %
Wide/diversified offer	5 %	2 %

Source:
Marc K. Peter, Katja Dörlemann, Kristof Hertig, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian, Nicole Wettstein (2024): Cyber study 2024: IT security in Swiss SMEs, IT service companies and the Swiss population.

digitalswitzerland, Die Mobiliar, Swiss Internet Security Alliance SISA, Swiss Digital Security Alliance ADSS, Swiss Academy of Technical Sciences SATW, University of Applied Sciences Northwestern Switzerland FHNW, YouGov Switzerland.

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

Research methodology:

The field research was conducted between 4 July and 5 August 2024.

The **SME sample** comprises 526 interviews with owners and CEOs from companies with 1–3 (n = 165), 4–9 (n = 174), 10–19 (n = 96) and 20–49 (n = 91) employees from the German (n = 363), French (n = 116) and Italian (n = 47) language region of Switzerland as well as from all sectors. The sample was disproportionately collected and then weighted according to its effective distribution. Of these, 34 (6 %) describe themselves as digital pioneers who adopt digital technologies early, 263 (50 %) as early followers who adopt digital technologies shortly after market launch, and 196 as late followers (37 %) who do not adopt digital technologies until they are successfully used by others.

The sample of **IT service companies comprises** 401 interviews with owners, managing directors and technical staff from companies with 1–9 (n = 288) and 10+ (n = 113) employees from the German (n = 320), French (n = 58) and Italian (n = 23) language regions of Switzerland. Of these, 121 (30 %) describe themselves as digital pioneers, 205 (51 %) as early followers and 43 as late followers (11 %).

The sample of the **Swiss population (Internet users)** comprises 1.247 interviews from all age groups, gender groups and language regions in proportion to the total population. The sample from Ticino was disproportionately collected and then weighted proportionally. Of these, 100 (8 %) describe themselves as digital pioneers, 557 (45 %) as early followers and 549 as late followers (44 %).

Where an evaluation does not give 100 %, the answer “don’t know” or no indication was given. The mean values were calculated on the scale from 1 (e.g. “not at all”) to 5 (very much), using the values 1+2 as (very) low, 3 as neutral and 4+5 as (very) high. On the scale of 10 (from 0–100 %) the values 1–3 as (very) low, 4–7 as neutral and 8–10 as (very) high were used for the evaluation.

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, Katja Dörlemann, Kristof Hertig, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian, Nicole Wettstein (2024): Cyber study 2024: IT security in Swiss SMEs, IT service companies and the Swiss population.

digitalswitzerland, Die Mobiliar, Swiss Internet Security Alliance SISA, Swiss Digital Security Alliance ADSS, Swiss Academy of Technical Sciences SATW, University of Applied Sciences Northwestern Switzerland FHNW, YouGov Switzerland.

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

digitalswitzerland · die Mobiliar · SWISS INTERNET SECURITY ALLIANCE · ALLIANCE DIGITAL SECURITY SWITZERLAND · satw · n|w University of Applied Sciences and Arts Northwestern Switzerland School of Business · YouGov