

Press Release

Zurich, 16 September 2026

AI-based cyber-attacks accentuate risks for SMEs – boards of directors are lagging behind the latest developments

Cybercriminals are increasingly taking advantage of artificial intelligence (AI), which makes attacks easier to carry out and increases the potential for damage. Yet almost three-quarters of companies have no explicit strategy to counter AI-based attacks, as shown by the [20th swissVR Monitor](#). At the same time, the topic of cyber resilience is becoming increasingly important for boards of directors. Despite this, many boards lack specialist knowledge, proven crisis management skills and a reliable reporting system – particularly in smaller companies.

More and more Swiss companies are being targeted by cybercriminals. According to estimates by board members, 41 per cent of companies have already fallen victim to a cyber-attack. That is 13 percentage points more than three years ago. This increase is almost entirely attributable to small and medium-sized enterprises (SMEs). The proportion of SMEs affected rose from 20 per cent in 2023 to 37 per cent in 2026, while it remained virtually stable at 45 per cent and 48 per cent respectively for large companies. This is one of the findings of the latest survey of 281 board members for the swissVR Monitor II/2026, carried out by the swissVR association for board members in partnership with the audit and consultancy company Deloitte and the Lucerne University of Applied Sciences and Arts.

The growing significance of the issue is also reflected in the strategic priorities of boards of directors. According to the survey, IT and security management – including cyber resilience – will be among the ten most important issues facing boards of directors over the next twelve months, making it crucial to increase its priority. As indicated by the study, business interruptions are by far the most common consequence of a cyber-attack, accounting for 42 per cent of cases (see Figure 1). Data breaches come in second place, at 22 per cent. Overall, the actual number of cyber-attacks on companies is likely to be higher, since half of all boards do not receive regular reports on cyber incidents, according to the survey.

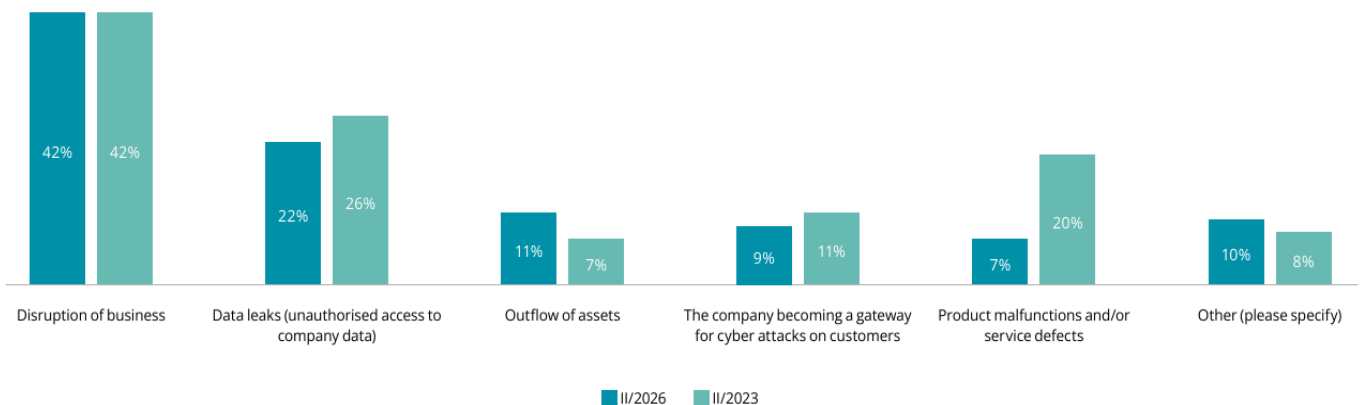


Figure 1: The consequences of cyber-attacks on companies. What impact did the attack(s) have on your company?

No explicit strategy against AI attacks

“The increased use of AI for criminal purposes is leading to a rise in cyber threats. Cyber risks are soaring, multiplying the potential for damage – with consequences that many companies, and indeed the public sector, still underestimate,” says Klaus Julisch, Cyber-Security Lead at Deloitte Switzerland.

Nevertheless, 74 per cent of companies do not have an explicit strategy to combat AI-based attacks. Furthermore, the focus on AI also varies significantly depending on company size. Only 18 per cent of small businesses have made strategic preparations, while the figure for large companies stands at 40 per cent.

There are similar shortcomings in preparations for serious incidents. 55 per cent of companies have no contingency plans, or have not tested their plans, to restore core IT processes – the ‘Minimum Viable Company’ concept – as quickly as possible following a serious cyber-attack, before permanent damage occurs. Here, too, the influence of company size is evident. Large companies (60 per cent) are twice as likely to have tested plans as small firms (32 per cent). “Financial service providers are particularly well prepared. Over two-thirds of these companies have IT recovery plans,” says Mirjam Gruber-Durrer, Professor of Normative Board Management at the Lucerne University of Applied Sciences and Arts. “The sector forms part of Switzerland’s critical infrastructure, and security standards are therefore much more firmly established, partly as a result of stricter regulation.”

Insufficient cyber expertise on boards of directors

The survey also reveals room for improvement within boards of directors themselves. Although 86 per cent of boards monitor current developments in the cyber sector and 84 per cent have adopted a risk policy for dealing with cyber-attacks, only half test crisis management processes in preparation for emergencies. This is nevertheless a significant improvement on the 34 per cent recorded three years ago. There is also scope for improvement when it comes to board expertise. 68 per cent of boards of directors have no member with proven cyber or IT expertise, and are reliant on the knowledge of senior management or an external specialist.

Reporting also remains a weak spot. Only one in two boards of directors is regularly informed about cyber incidents; a quarter receive no reports at all. One particularly worrying trend is that reporting on the need for action and investment, as well as on the general threat situation, has declined significantly by 18 and 13 percentage points respectively since 2023 – despite a rise in the number of attacks. “Defining a clear cyber strategy is a key management responsibility, and reporting is a central supervisory function, enabling boards of directors to fulfil their management role. Cyber resilience is part of risk management and is therefore an ongoing management responsibility that belongs on the risk dashboard and the board of directors’ agenda,” says Isabelle Amschwand, President of swissVR.

About the swissVR Monitor

The six-monthly swissVR Monitor survey aims to gauge the assessments of board members on business prospects, strategies and structural issues. [For the 20th swissVR Monitor, ‘How the board of directors can boost cyber resilience’](#), swissVR conducted an online survey of 281 board members between 26 May 2026 and 5 July 2026 in collaboration with Deloitte and the Lucerne University of Applied Sciences and Arts. The respondents sit on the boards of listed companies and small and medium-sized enterprises (SMEs) and represent all relevant industries and sectors. 34 per cent of the respondents are board members at large companies, 28 per cent at medium-sized companies and 38 per cent at small companies.

Contact: Michael Wiget
Head of External Communications
Tel.: +41 58 279 70 50
Email: mwiget@deloitte.ch

Contact: Kevin Capellini
External Communications
Tel.: +41 58 279 59 74
Email: kcapellini@deloitte.ch

swissVR

swissVR serves the interests of board members in Switzerland and is committed to helping them improve their expertise and share experiences with other members. As an independent association, swissVR is run by board members for board members. With its services, swissVR helps to professionalise the activities of boards of directors, promotes networking between board members from companies in all sectors, and gives its 1,400 or so members access to relevant information and tailored training. swissVR is aimed exclusively at people who actively serve on boards of directors. Further information can be found at www.swissvr.ch

The Lucerne University of Applied Sciences and Arts – representing central Switzerland

The Lucerne University of Applied Sciences and Arts is the university of the six Central Swiss cantons. It comprises the School of Engineering and Architecture, the School of Business, the School of Computer Science and Information Technology, the School of Social Work, the School of Design, Film and Art, the School of Music, and the focus area of Health. It is the largest educational institution in the heart of Switzerland, with some 8,700 students, 13,000 people in continuing education (of which 5,600 on MAS, DAS and CAS programmes), 274 new research projects and 2,144 employees. The Institute of Financial Services Zug (IFZ) at the Lucerne University of Applied Sciences and Arts puts a strong focus on the topic of governance, risk and compliance by also offering executive education courses for board members, particularly in the form of the Board Executive CAS programme. Further information can be found at www.hslu.ch/ifz-verwaltungsrat / www.hslu.ch/cas-vr / www.hslu.ch/ifz

Deloitte Switzerland

Deloitte offers integrated services that include Audit & Assurance, Tax & Legal, Strategy, Risk & Transactions and Technology & Transformation. Deloitte provides services to companies and organisations of all legal forms and sizes across all sectors in Switzerland with around 2,500 employees at six locations in Basel, Bern, Geneva, Lausanne, Lugano and Zurich, where the headquarters are located.

Deloitte's employees achieve measurable and sustainable results that help to strengthen public confidence in the capital markets and enable our clients to develop and succeed. Building on its history spanning more than 180 years, Deloitte operates in more than 150 countries and territories and employs around 470,000 professionals worldwide.

'Deloitte' refers to 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. Further information can be found at www.deloitte.com/about.

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 press release was correct at the time of publication.



© 2026 Deloitte AG