How the Board of Directors can boost cyber resilience

swissVR Monitor II/2026
September 2026

swissVR®

Deloitte.

Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern

Contents

3 Foreword

4 Summary and key findings

5 Economic, sector and business outlook

7 Focus topic: How the Board of Directors can boost cyber resilience
8 Incidence and impact of cyber attacks
9 Artificial intelligence, the minimal viable company, and measures employees need to take
12 The Board of Directors and cyber resilience

16 Strategic and structural issues facing the Board of Directors
16 Roles and responsibilities, number of meetings, time commitment and liability insurance
19 Key issues for the Board of Directors

20 Interviews
20 Marc Ruef on current trends in cyber resilience
22 Sandra Emme on the Board's role in cyber resilience
26 Frank Desiere on the importance of artificial intelligence in cyber attacks

30 Authors

About the Survey
This is the 20th edition of swissVR Monitor and is based on a survey of 281 members of Swiss company Boards of Directors. The aim of the survey is to gauge Board members' attitudes to the outlook for the economy and business, and to corporate governance issues. This edition also focuses specifically on the topic of cyber resilience.

The swissVR Monitor survey was conducted by swissVR in collaboration with Deloitte AG and the Lucerne University of Applied Sciences and Arts between 26 May and 5 July 2026. A total of 281 Board members took part, representing listed companies as well as small and medium-sized companies (SMEs) from every major sector of the Swiss economy. 38% of the participants are from small companies, 28% from medium-sized companies, and 34% from large companies.

The aim of swissVR Monitor is to offer Swiss Board members a benchmark for comparing the issues facing their own Board with those facing their counterparts on other company Boards. swissVR Monitor also aims to share with the wider public the ways in which Board members perceive their role and the current economic situation.

A note on the methodology
When comparing survey results over time, please note that the sample may have changed. Percentage figures are rounded to add up to 100. Company size is determined by workforce: small companies have between 1 and 49 employees, medium-sized companies have between 50 and 249 employees, and large companies have 250 or more employees.

Foreword

Dear reader

We are delighted to bring you swissVR Monitor II/2026. For this edition, we surveyed 281 members of Boards of Directors across Switzerland. The findings reflect their attitudes to the economy, the outlook for business and relevant areas of their own role.

Cyber attacks have risen sharply in both frequency and level of sophistication over recent years, so this swissVR Monitor returns to the issue of cyber resilience, which it last investigated in swissVR Monitor II/2023. The considerable losses companies can suffer as a result of a cyber attack make it essential that Boards tackle cyber resilience as part of their mandate, achieving a clear understanding of their role and resulting responsibilities in this area. This edition of swissVR Monitor explores the possible impact of cyber attacks, the counter-measures companies are taking and management reporting to the Board on cyber-related issues.

The findings of swissVR Monitor II/2026 show a marked rise since 2023 in the proportion of companies reporting that they have been the victim of a cyber attack. However, artificial intelligence (AI) technology is involved in fewer than half of all such attacks. Therefore, the most important areas for Boards to focus on are testing their crisis management plan, ensuring their Board has the expertise it needs, and safeguarding comprehensive cyber reporting by management. Smaller companies have more to do than large companies in these three areas.

Alongside the Survey findings, swissVR Monitor II/2026 has conducted interviews on the focus topic with:

- Marc Ruef, Head of Research at scip and Lead Architect at VulDB
- Sandra Emme, Industry Leader Cloud Enterprise at Google and member of the Board of Directors of Belimo and Zehnder Group International
- Frank Desiere, CEO and member of the Board of Directors of CorTec

We would like to thank our interviewees and all the Board members who participated in this swissVR Monitor. We hope you will find this report an informative and enjoyable read.

Isabelle Amschwand
President swissVR

Reto Savoia
CEO Deloitte Switzerland

Prof. Dr. Mirjam Gruber-Durrer
Lecturer IFZ/Lucerne University of Applied Sciences and Arts

Summary and key findings

16%
of Board members rate the outlook for the Swiss economy over the next 12 months as positive.

Modest improvement in the outlook for the Swiss economy

- Swiss Board members are slightly more optimistic than in H2 2025 and H1 2026 in their rating of the economic, sector and business outlook over the next 12 months.
- Board members are still concerned, however, about risks and uncertainties facing the Swiss economy, including tensions in the Persian Gulf and the possibility of further tariffs on Swiss exports to the US.

41%
report that their company has been the victim of a cyber attack.

Cyber resilience seen as increasingly important

- The proportion of companies falling victim to at least one cyber attack has risen by almost half since 2023.
- The most frequent impacts of a successful cyber attack include disruption to the company's operations and unauthorised access to company data (data leaks).

74%
of Swiss Boards do not currently have a strategy for tackling AI-based cyber attacks.

Majority of companies unprepared for AI-based cyber attacks

- Fewer than one in five Swiss companies has a strategy for tackling AI-based cyber attacks and briefs the Board regularly on the implementation and effectiveness of this strategy.
- More than half of all companies either have no plan for restoring their IT systems in the event of a serious cyber attack or have a plan but have not yet tested it.

68%
of Boards do not have a member with expertise in cyber-related issues or IT.

Boards have more to do in the area of cyber resilience

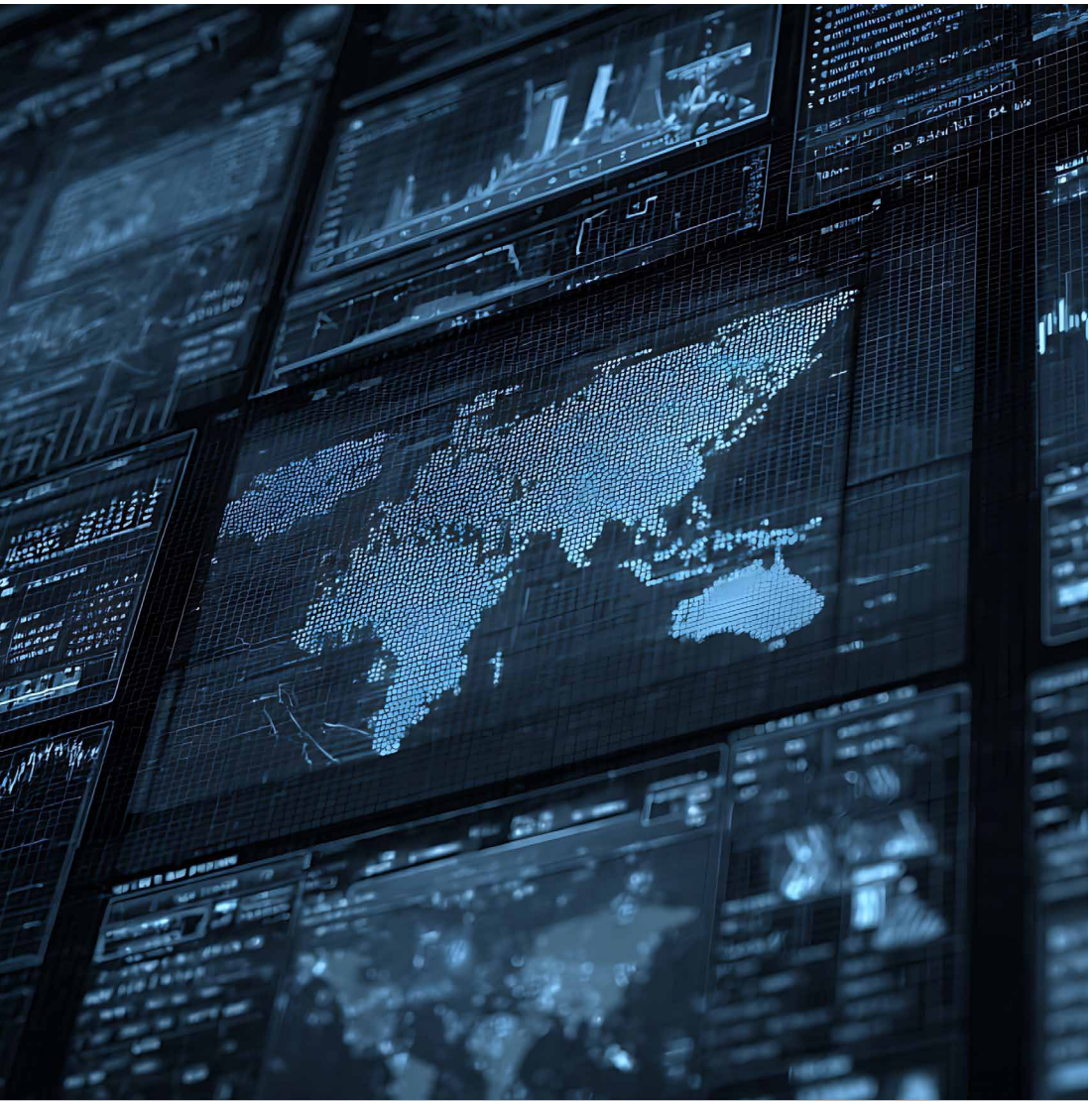
- Only half of Swiss Boards have rehearsed their crisis management plans in the event of a cyber attack.
- Half of all Boards report that they are not regularly briefed by management on cyber attacks on the company.
- Only one Board in three has a member with expertise in cyber-related issues or IT.

33%
of Swiss Board members see improving efficiency and optimising internal processes as a major issue over the next 12 months.

Changes in the areas Boards expect to tackle over the next 12 months

- Improving efficiency and optimising internal processes is the most frequently cited issue for Boards over the next 12 months, up from second place in swissVR Monitor I/2026.
- Risk management has slipped from top of the list of issues to second place. Digitalisation, robotics and automation is now the third most frequently cited issue, up from sixth place in the previous survey.

Economic, sector and business outlook



Board members are slightly more optimistic in their expectations for the economic, sector and business outlook for the next 12 months than in swissVR Monitor I/2026 and swissVR Monitor II/2025 (see Chart 1). The findings suggest an upward trend, albeit still modest. This is surprising given the many risks and uncertainties the Swiss economy continues to face, including tensions in the Persian Gulf, the possibility of new tariffs on Swiss exports to the US, a further rise in the value of the Swiss Franc compared to other currencies, and the ongoing economic weakening of key foreign markets.

Around two-thirds of Swiss Board members (68%) rate the prospects for the country's economy over the next 12 months as neutral, with 16% rating them as positive and the same proportion as negative. These findings mirror those of other current forecasts, which assume modest growth in the Swiss economy in both 2026 and 2027, albeit markedly below the long-term average.

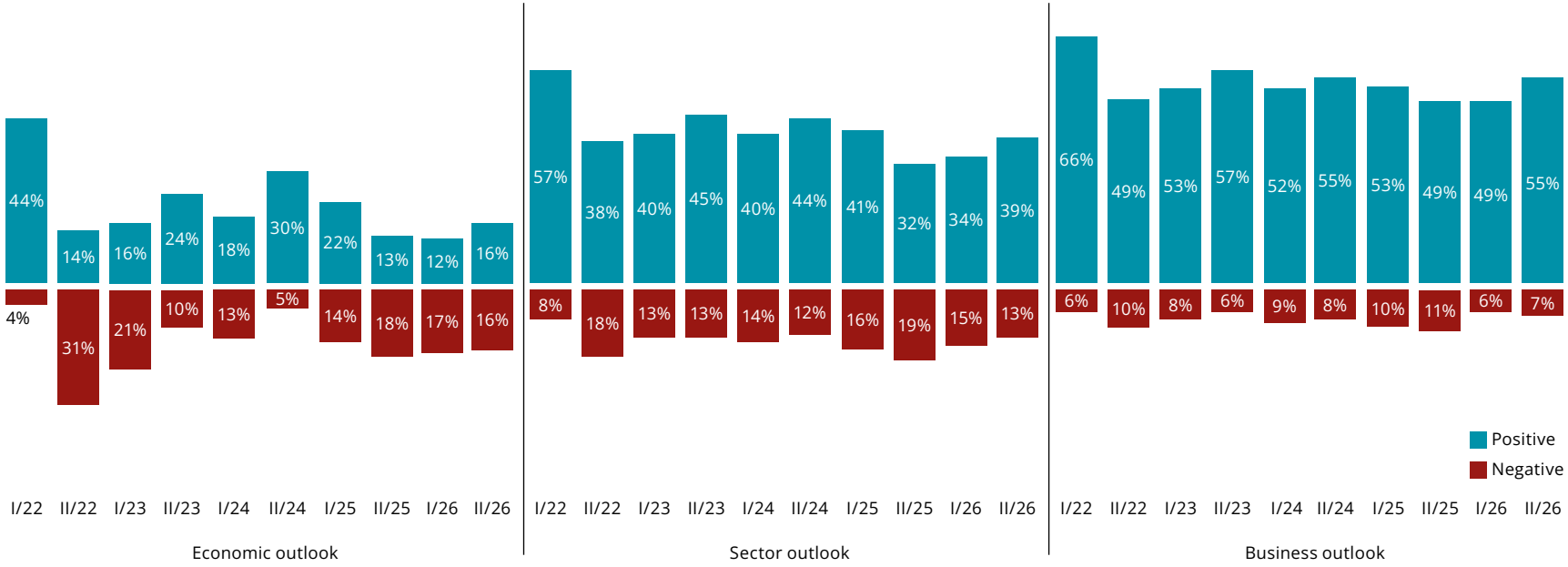
Almost half of Board members (48%) also rate the prospects for their sector over the next 12 months as neutral; three times as many rate them as positive as rate them as negative (39% as against 13%). Board members in the ICT sector are more likely than the average to rate the prospects for their sector as positive (53% of Board members, as against just 3% who rate them as negative). This has increasingly been the case with this sector over recent years, given the growing importance of artificial intelligence, but the trend is particularly marked in the current survey. In contrast, the findings for manufacturing and chemicals are below average, with 20% of Board members rating the prospects for their sector as positive and 28% rating them as negative. This probably reflects the fact that this is an export-oriented sector and is affected by tariffs as well as by the strength of the Swiss Franc and continued sluggish demand from abroad.

More than half of all Swiss Board members (55%) rate the prospects for their own company over the next 12 months as positive, 38% rate them as neutral and just 7% rate them as negative. Board members

in the ICT and pharma and life sciences sectors are most optimistic about their company's prospects, with 73% and 68% respectively rating them as positive as against just 3% and 0% respectively who rate them as negative. As with the sector outlook findings, Board members in the manufacturing and chemicals sector are less likely than average to rate the prospects for their company as positive (24% against 16% who rate them as negative). The shrinking net balance between positive and negative ratings also indicates that companies are less optimistic than in swissVR Monitor I/2026.

Chart 1. Economic, sector and business outlook over the next 12 months [swissVR Monitor I/2022 to II/2026]

Question: How do you rate the prospects for the Swiss economy / sector / your company over the next 12 months?
Note: Neutral answers are reflected in the difference between the sum of positive and negative answers.

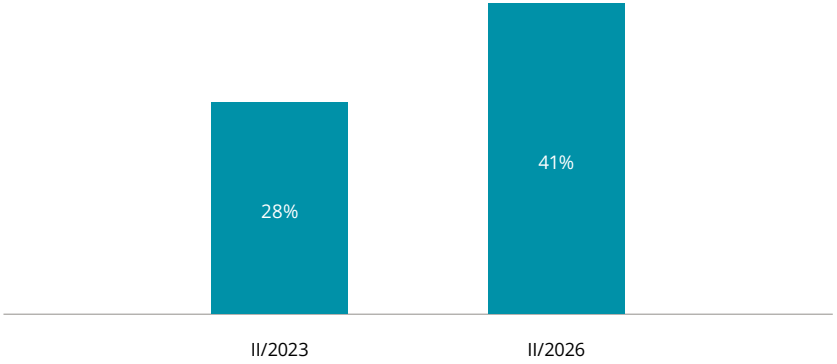


Focus topic: How the Board of Directors can boost cyber resilience

Cyber attacks on companies and other organisations have become much more frequent as well as more sophisticated over recent years. One key driver of this trend is the greater dependency of businesses and organisations on highly networked and complex digital systems, such as cloud services and supply chains. The rapid ongoing development of artificial intelligence, with new models and more powerful agents reaching the market all the time, is another factor enabling criminals to launch cyber attacks more easily, more rapidly and more frequently. Against this backdrop, cyber attacks can be expected to become more frequent and more serious in future. It is therefore even more important that Boards of Directors address the cyber resilience of their company and boost it as part of their role and responsibilities.

Chart 2. Companies impacted by cyber attacks

Question: To the best of your knowledge, has your company ever been the victim of a cyber attack (phishing, unauthorised access to data, website hacking, etc.)?



Incidence and impact of cyber attacks

Four out of every ten Swiss Board members (41%) report that their company has been the victim of a cyber attack (see Chart 2). This question was last asked in 2023, when the proportion was 28% (swissVR Monitor II/2023), indicating an increase of almost half (46%) in the number of companies reporting such an attack.

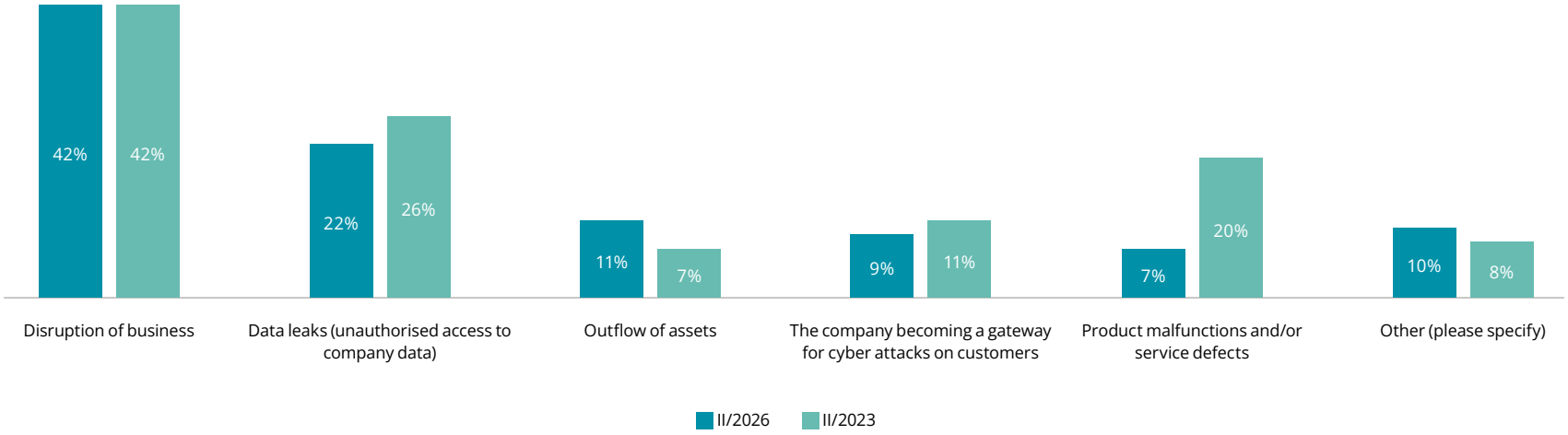
This increase is surprising in that more and more companies are reporting cyber attacks despite having invested in cyber resilience over recent years. It is also likely that a substantial number of such attacks go unrecorded: the current Survey also shows that only half of all Boards regularly receive cyber briefings or reporting from management (see Chart 9).

The increase in reported cyber attacks over the past three years focuses particularly on small and medium-sized companies: the number of such companies reporting a cyber attack has almost doubled, from 20% to 37%, since the last time this question was asked, whereas the proportion of large companies reporting such incidents has remained almost unchanged (48% in swissVR Monitor II/2026 as against 45% in swissVR Monitor II/2023). While large companies remain more vulnerable to cyber attack because of their size, small and medium-sized businesses are increasingly falling victim to such attacks. Therefore, the issue of cyber resilience is not a matter of company size, but an existential threat to all companies.

The importance of robust cyber resilience is also reflected in the impact on companies of a successful cyber attack (see Chart 3). As in swissVR Monitor II/2023, the most frequently cited impact by some margin is disruption of business (42% of responses), followed in second place by data leaks (22% of responses). Relatively few respondents cite other impacts, and these are reported in similar proportions to the 2023 findings. The exception is product malfunctions and/or service defects.

Chart 3. Impacts of cyber attacks on companies

Question: What impact did the attack(s) have on your company? Please tick all that apply. (n = 113)



Artificial intelligence, the minimal viable company, and measures employees need to take

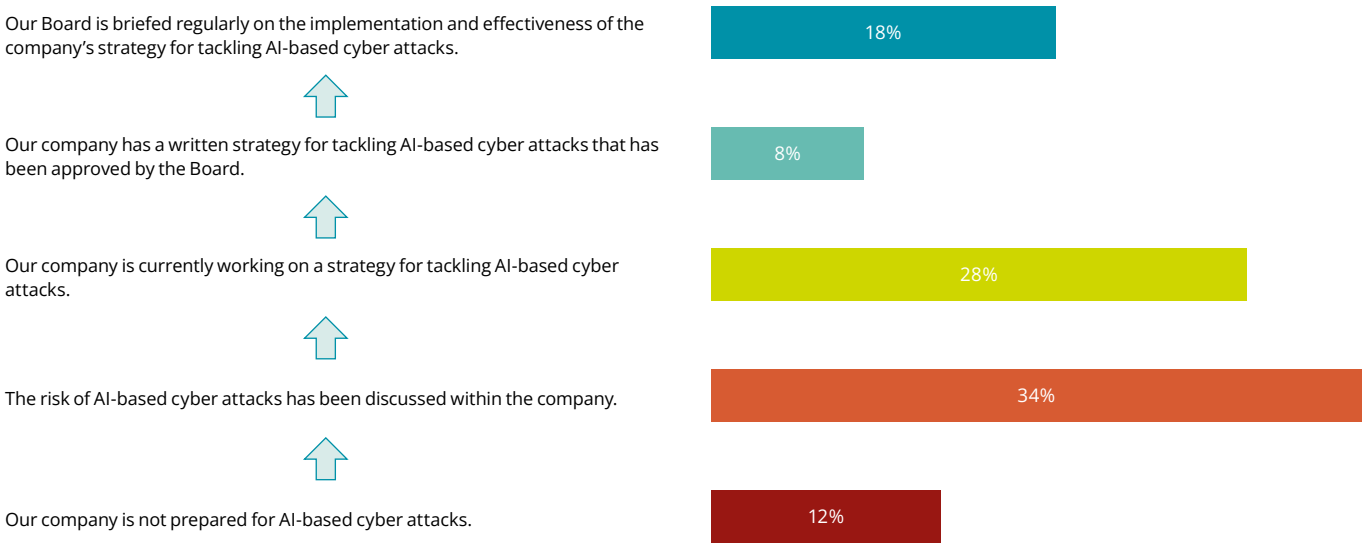
As noted above, developments in artificial intelligence (AI) mean that criminals are now able to cause significant damage to companies more easily and more rapidly. So what preparations have companies made specifically for the increased threat of cyber attack (see Chart 4)?

Around three-quarters of all companies (74% across the bottom three bars in the chart below) do not currently have a written strategy for tackling AI-based cyber attacks. Of the remaining companies, 8% report having a strategy for at least part of the company and 18% that they regularly brief the Board on the implementation and effectiveness of this strategy. It is important to note here that simply having a strategy for tackling AI-based cyber attacks and reporting to the Board on its effectiveness does not provide any direct indication of how well a company would able to defend itself against a cyber attack.

Company size also plays a key role in Swiss companies' level of preparedness. Just 18% of small companies have a strategy for tackling AI-based cyber attacks, compared with 40% of large companies. Reasons for this finding may be the link between company size and frequency of cyber attacks or the fact that large companies are more likely that smaller ones to discuss and act on cyber-related issues, such as through their IT function or by having a Chief Information Security Officer (CISO).

Chart 4. Preparation for AI-based cyber attacks

Question: Artificial intelligence (AI) can cause considerable damage to cyber systems. How prepared is your company for AI-based cyber attacks?



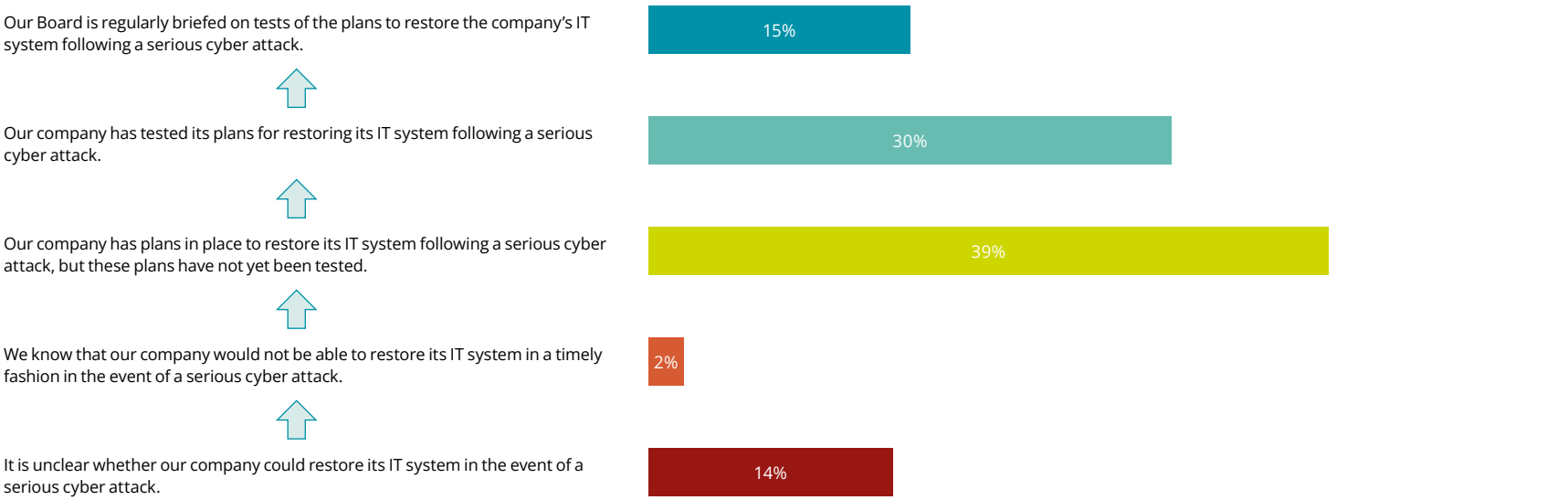
Where companies are unable to prevent a cyber attack, the focus shifts to how quickly essential core IT processes – the minimal viable company – can be restored and long-term damage averted (see Chart 5). More than half of all companies (55% across the bottom three bars in the chart below) either do not have plans for restoring their IT system following a serious cyber attack or have such plans in place but have not tested them.

45% of companies have tested their plans for a minimal viable company, with one in three reporting the results of these tests to their Board of Directors (15% of respondents). It should be noted here that simply having plans that have been tested and reporting the test results to the Board does not mean that IT systems can be restored in all cases.

Once again, the findings differ according to company size. Large companies are almost twice as likely as small companies to have tested their plans for a minimal viable company (60% and 32% respectively). Companies in the financial services sector are particularly well prepared in terms of plans to restore their IT system after a cyber attack, with 70% having such plans. This reflects the particular importance of IT systems in financial companies compared with other sectors such as construction or tourism, and the fact that the finance sector is part of a country's critical infrastructure, so sectoral standards are more rigorous in this area.

Chart 5. Minimal viable company in case of cyber attack

Question: If the company suffered a cyber attack, could its essential core IT processes be restored and a 'minimal viable company' re-established without unacceptable cost or damage to the business?



The impact of cyber attacks on companies can be extremely serious, so companies have a number of measures at their disposal to ensure that employees take appropriate precautions in cyberspace (see Chart 6). Almost nine out of ten Swiss Board members (89%), for example, report that roles and responsibilities for cyber security are clearly defined within the company, while the same proportion report proactive promotion of a positive security culture. Regular training on cyber risks features in 83% of companies, with 74% running structured awareness programmes and 61% measuring the effectiveness of training.

Small companies are markedly less likely than large companies to implement the measures listed. For example, awareness-raising of risks such as phishing are reported in just over half of small companies (54%). However, only one-third of small companies measure how effective training measures really are. In companies with more than 1,000 employees, in contrast, nearly every company is implementing all the measures listed below.

Against the backdrop of threats from AI-based cyber attacks, the role of the Board of Directors is to ensure that management devises an informed strategy and to monitor its implementation and effectiveness. The Board's aim should be to assess whether the company is able to fend off a serious attack and to initiate any necessary improvements in the company's cyber resilience.

The same applies to ensuring a minimal viable company. Here, too, the Board must be able to monitor the company's plans for restoring its IT system after a major cyber attack and the results of tests of those plans. On this basis, the Board can then assess whether the minimal viable company can be re-established and whether additional measures are required.

For more information and recommendations, see the following interviews:
- Marc Ruef on current trends in cyber resilience
- Frank Desiere on the importance of artificial intelligence in cyber attacks

Chart 6. Measures governing employees' handling of cyberspace

Question: Please indicate your agreement with the following statements on your company's measures governing employees' handling of cyberspace.

The Board of Directors and cyber resilience

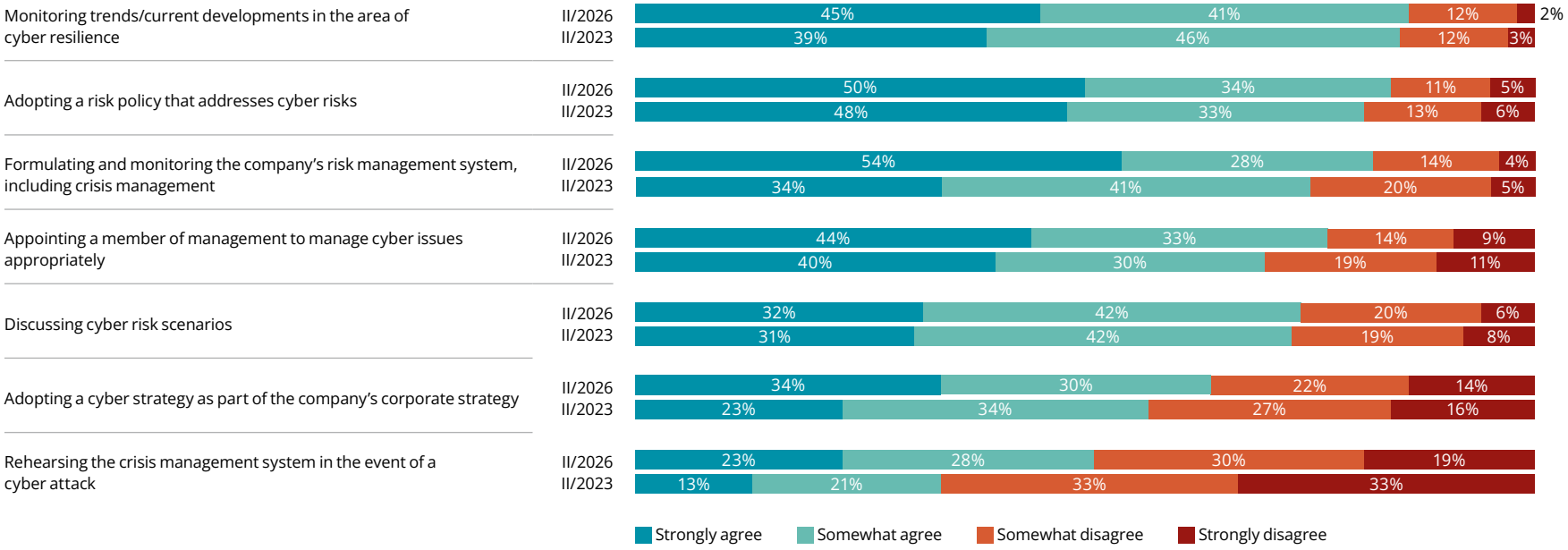
The Board has a number of roles and responsibilities in relation to cyber resilience (see Chart 7). A very large majority of Board members surveyed strongly agree or somewhat agree that their Board monitors trends and current developments in the area of cyber resilience (86% of respondents) and has adopted a risk policy that addresses cyber risks (84% of respondents).

Other responsibilities that most Swiss Board members assume at least partially include formulating and monitoring the company's risk management system, including crisis management (82%), appointing a member of management to manage cyber issues appropriately (77%) and discussing cyber risk scenarios (74%). Two-thirds of respondents (64%) agree that their Board has adopted a cyber strategy as part of the company's corporate strategy. However, there is room for improvement in the area of crisis management in the event of a cyber attack: only one Board member in two (51%) strongly agrees or somewhat agrees that this strategy is rehearsed, although this is considerably up on the findings of swissVR Monitor II/2023 (34%).

As with previous questions, Board members representing large companies are more likely than those representing small companies to strongly agree or somewhat agree with all the statements below

Chart 7. Roles and responsibilities of the Board

Question: Does your Board take responsibility for the following roles and responsibilities in the area of cyber resilience? Please indicate your agreement with each aspect.



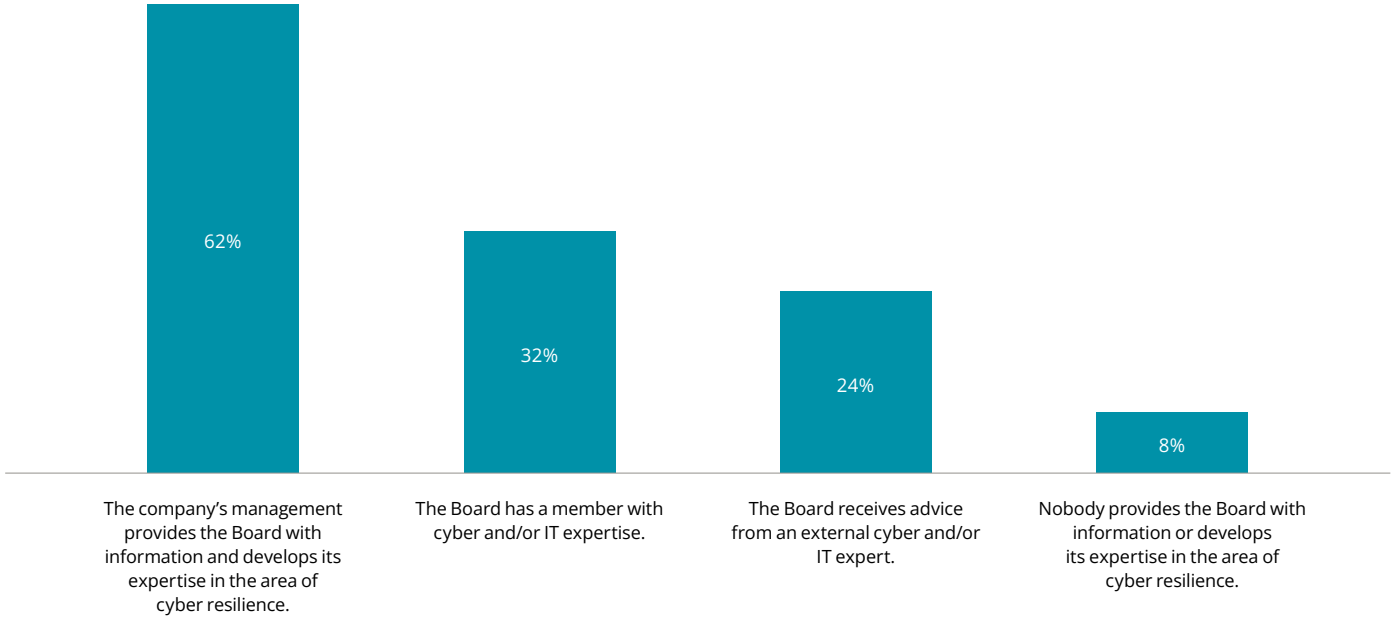
relating to roles and responsibilities. Comparisons with the findings of swissVR Monitor II/2023 also show that Board members are now more likely to be discussing cyber resilience.

The Board of Directors has various sources of expertise to draw on when it comes to cyber resilience (see Chart 8). Most Swiss Board members (62%) rely on the company's management to provide the Board with this expertise, with only one-third (32%) reporting that their Board includes a member with cyber and/or IT expertise. In almost one-quarter of cases (24%), Boards receive advice from an external expert, while 8% of Boards have no cyber expertise.

Large companies are more likely than small companies to have large Boards, so it is unsurprising that their Boards are more likely to include members with cyber and/or IT expertise (41% of Boards of large companies compared with 28% of Boards of small companies). Boards in the ICT and corporate services sectors are more likely to include members with cyber and/or IT expertise (53% and 41% of Boards respectively), whereas Boards in construction, pharma and life sciences, and manufacturing and chemicals are less likely than the average to include members with such expertise (20%, 19% and 16% respectively).

Chart 8. Cyber expertise of the Board

Question: Who provides your Board with the information and develops the expertise it requires in the area of cyber resilience? Please tick all that apply.



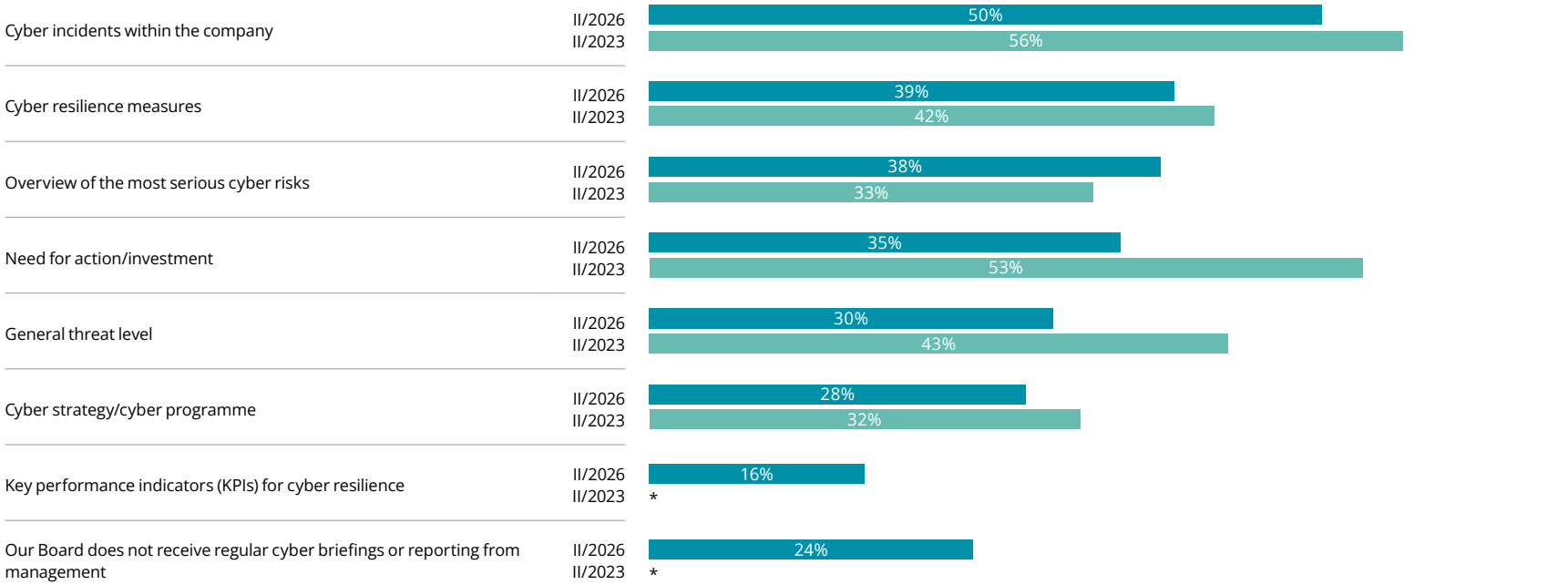
Swiss Boards regularly receive briefings and reporting from management on various aspects of cyber risk, but there is room for improvement here (see Chart 9). Only 50% of Boards are routinely informed of cyber incidents within the company, with fewer than half being informed of all the other aspects listed below. One Board in four (24%) receives no regular cyber briefings from management.

As with other questions, Board members representing large companies are more likely than those representing small companies to agree with statements relating to cyber reporting. There were, however, few significant differences between Boards representing different sectors in relation to this issue.

Although a growing number of companies have been the victim of cyber attacks, and AI-based attacks now pose an increasing risk, Boards are actually less likely than in swissVR Monitor II/2023 to receive regular briefings or reporting on the need for action/investment (down 18 percentage points) and on the general threat level to the company (down 13 percentage points). This suggests that in many companies, cyber resilience is more likely to be seen by management as a one-off project rather than as an ongoing process.

Chart 9. Cyber reporting from management

Question: On which of the following aspects does your Board receive regular cyber briefings or reporting from the company's management? Please tick all that apply.



* no data collected

The risk of a serious cyber attack on a company is significant, so Board members should rehearse the crisis management system in place within their Board. This includes, for example, assessing what measures need to be put in place in conjunction with management to ensure that a minimal viable company can be re-established in the event of such an attack.

In relation to the make-up of the Board, it is advisable for Boards either to include a member with cyber and/or IT expertise or to receive advice in this area from an external expert. This will enable Boards to fulfil their role as a sparring partner for management and enable them to help boost cyber resilience within the company.

The Board of Directors' role as the ultimate oversight body within the company also requires regular cyber briefings and reporting from management. Such reporting should include core elements such as information on cyber incidents within the company. If such information is not being communicated, Boards need to demand it.

For more information and recommendations on these issues, see the following interviews:

- Sandra Emme on the Board's role in cyber resilience
- Frank Desiere on the importance of artificial intelligence in cyber attacks

Strategic and structural issues facing the Board of Directors

Roles and responsibilities, number of meetings, time commitment and liability insurance

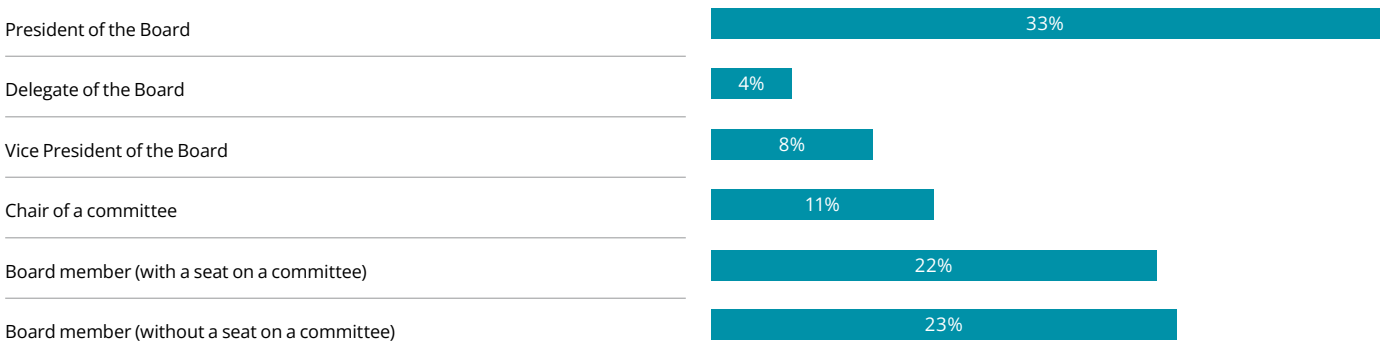
Respondents taking part in swissVR Monitor II/2026 hold a number of different Board roles (see Chart 10). The largest group (45%) is made up of Board members with or without a seat on a committee. One-third of respondents (33%) are President of their Board. The survey also includes other roles, such as Chair of a committee (11% of respondents), Vice-President of the Board (8%) and Delegate of the Board (4%).

There are marked differences between Swiss Boards in terms of the number of meetings they hold each year (excluding committee meetings) (see Chart 11). Almost three-quarters of Boards (72%) hold between three and six meetings a year, with one in four (26%) meeting more often. The number of meetings tends to increase with company size: in small companies, the median number of meetings is five a year, whereas in large companies, it is six a year. When this question was last asked in swissVR Monitor II/2024, the median for all companies was five meetings a year, which has risen to six in the current survey.

The amount of time members commit to their Board mandate each year also varies widely (see Chart 12). Including Board meetings, committees, preparation, representing the company, and initial and continuing training, the average time commitment is 22 days a year, with a median of 15 days a year. This illustrates that a few 'outliers' spend considerably more time on their mandate, pushing up the average. These individuals report spending more than 30 days a year on their Board mandate and make up around 15% of all Swiss Board members surveyed. Just under two-thirds of this sub-group (61%) are President

Chart 10. Own role(s) on the Board of Directors

Question: Which role(s) do you hold in relation to your Board of Directors? (Please select all that apply.)



of their Board. Compared with swissVR Monitor II/2022 and swissVR Monitor II/2024, there has been very little change in both the average and the median annual time commitment involved in a Board mandate.

Serving on a Board of Directors involves substantial responsibilities on the part of Board members, both to their company and to themselves. For example, they run the risk of personal liability claims against them in the event of loss or damage. To protect themselves

Chart 11. Number of Board meetings per year

Question: Excluding committee meetings, how many Board meetings does your company hold each year?

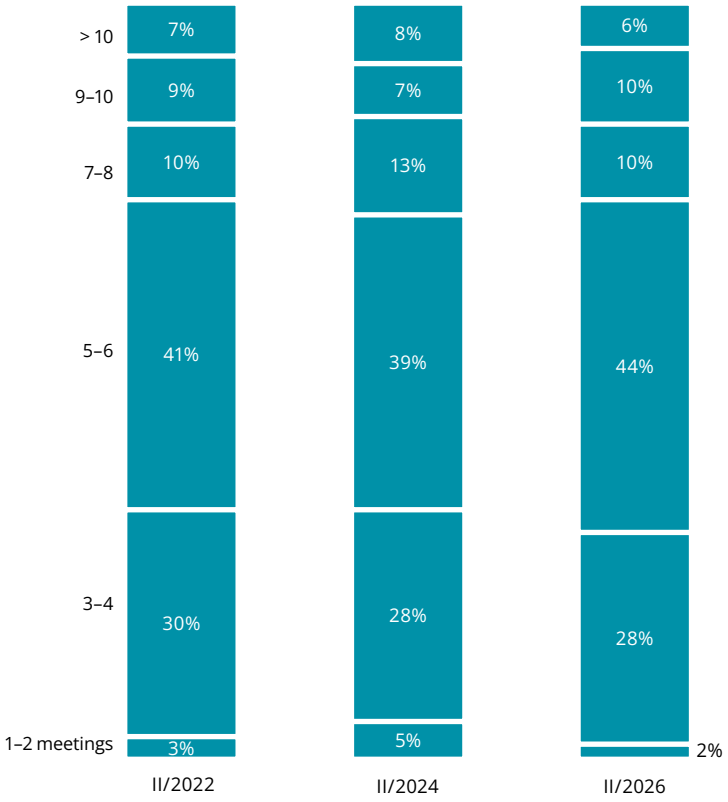
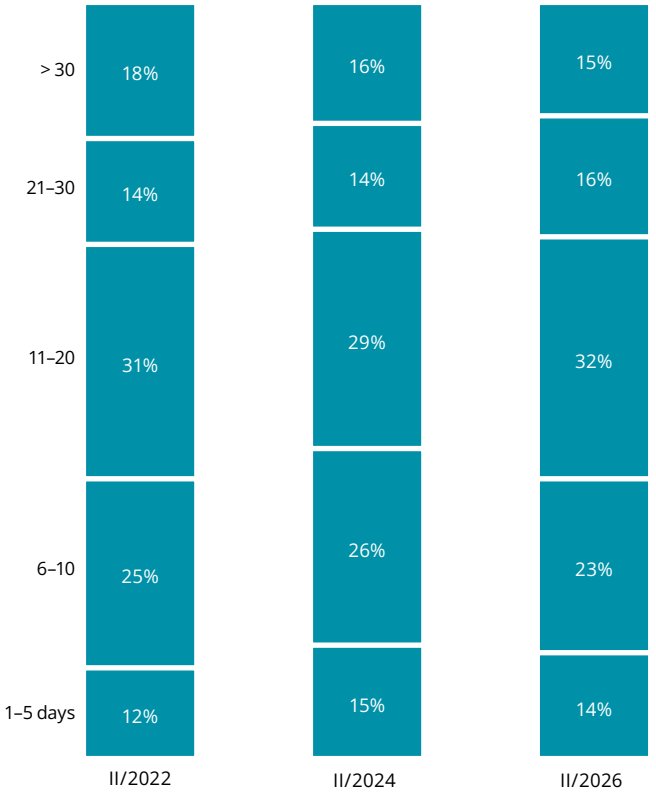


Chart 12. Time spent on Board mandate per year

Question: Approximately how much time do you commit each year to your Board mandate? Please include meetings, committees, preparation, representing the company, and initial and continuing training.



against the cost of defending such claims, unconditional claims and possible compensation payments, individual Board members and companies can take out professional liability insurance, also known as directors' and officers' (D&O) insurance.

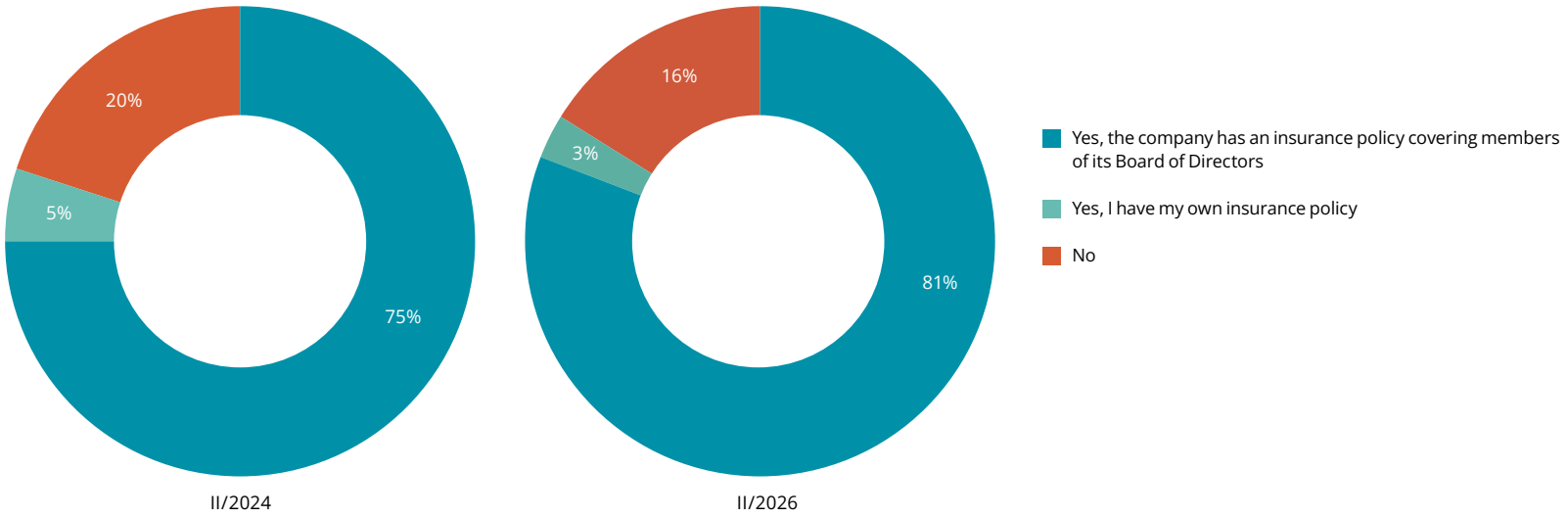
Four-fifths of companies (81%) have a company D&O insurance policy in place for their Board members, and 3% of Board members surveyed have their own insurance policy (see Chart 13). This means, though, that one Board member in six (16%) has no liability insurance.

Nearly all Board members in large companies have insurance – 89% provided by their company and 1% their own insurance policy – but this falls to around three-quarters of Board members in small companies (70% provided by their company and 5% their own policy).

There has been a modest improvement in these figures since this question was last asked in swissVR Monitor II/2024. This may reflect the fact that Swiss Board members are increasingly demanding insurance cover under a policy provided by their company.

Chart 13. Directors and officers (D&O) insurance

Question: Do you have professional liability insurance (directors' and officers' insurance)?



Key issues for the Board of Directors

The most frequently cited issue facing Swiss Boards over the next 12 months is improving efficiency and optimising internal processes (cited by 33% of Board members; see Chart 14). This issue ranked fourth in swissVR Monitor I/2026, probably because – as explored in that report – companies are now rolling out and refining artificial intelligence (AI) applications.

The second and third most important issues Boards will be facing over the next 12 months are risk management (cited by 29% of respondents) and digitalisation, robotics and automation (cited by 28%). Risk management has fallen one place in the rankings compared with I/2026, while digitalisation has risen three places.

The growing importance of IT (cited by 19% of respondents), security management (including cyber resilience) (18% of respondents) and go-to-market strategy (also 18%) is striking, given that these issues did not previously feature among the top ten issues cited by Board members. In contrast, formulating a new corporate strategy – also cited by 18% of respondents – has fallen dramatically in the ratings, from second place to eighth.

Chart 14. Key issues for the Board of Directors

Questions: What have been the most important issues that your Board of Directors has had to tackle over the last 12 months? In your view, what will be the most important issues that your Board of Directors will have to tackle over the next 12 months?

Next 12 months		Rank II/2026	Issues
1 (33%)	▲	**4** (27%)	**Improving efficiency / optimising internal processes**
2 (29%)	▼	**1** (38%)	**Risk management**
3 (28%)	▲	**6** (23%)	**Digitalisation / robotics / automation**
4 (27%)	▲	**5** (25%)	**Responding to market developments / behaviour of competitors**
5 (24%)	▲	**7** (22%)	**Talent (recruitment, retention, etc.)**
6 (22%)	▼	**3** (28%)	**HR challenges at management level**
7 (19%)	▲	– (15%)	**IT**
8 (18%)	▲	– (16%)	**Security management, including cyber resilience**
8 (18%)	▲	– (13%)	**Go-to-market issues (marketing and sales strategy)**
8 (18%)	▼	**2** (36%)	**Formulating a new corporate strategy**

"–" means "not one of the top-10 issues".

Interviews

Current trends in cyber resilience

Marc Ruef, Head of Research at scip and Lead Architect at VulDB

"Businesses need to take the time to prepare thoroughly for a crisis. [...] It is devastating when companies do not tackle this issue early enough: once the crisis has happened, they are in survival mode and simply do not have time to think carefully about the decisions they are making, let alone make plans."

swissVR Monitor: You have proven skills and expertise in the cyber field. How do you see companies' cyber resilience having improved over the last few years?

Marc Ruef: Cyber resilience has improved markedly. Many companies now understand cyber security as a crucial aspect of corporate risk, and members of management teams are now much more likely to be discussing digital risks and regulatory requirements. However, cyber crime has also become more professional over that time: ransomware groups now operate like industrial service providers with specific roles, workloads and business models, so the race against the criminals continues.

swissVR Monitor: Our survey findings show that more than one company in three has been the victim of a damaging cyber attack. Where do you see the major vulnerabilities? And where do companies need to put most effort into making their systems more secure?

Marc Ruef has worked in cyber security since the late 1990s and is the founder of computec.ch, the best-known German-language computer security portal. He published his first book at the age of 18 and went on to write "Hacking Intern" (published by Data Becker Verlag) and "Die Kunst des Penetration Testing" ("The Art of Penetration Testing"), which was published by C&L Verlag, among other titles. Over the last 25 years, Marc Ruef has collaborated on 16 books, published more than 275 specialist articles in seven languages and given over 200 interviews. He is one of the most widely-read German-language writers in his area. He also lectures at a number of Swiss higher education institutions, including ETH Zurich, the University of Applied Sciences in Business Administration Zurich, Lucerne University of Applied Sciences and Arts, and the Institute of Communication and Leadership in Lucerne. Marc Ruef is co-founder of scip AG, a Zurich-based company that has been providing consultancy in cyber security since 2002. He heads scip AG's research department, which focuses on unconventional projects, such as car hacking and the testing of medical equipment.

Marc Ruef: Theft of log-in credentials is still the greatest risk: successful attacks resulting from phishing, data theft and compromised user accounts can have a devastating impact on a company. And most recently, we have seen a ramping-up of the risk from third-party providers and supply chains. The increasing complexity and multifaceted nature of modern systems involve risks that are not always evident, so companies are therefore more likely to downplay their significance.

swissVR Monitor: Three years ago, around one company in four reported being the victim of a cyber attack. How do you explain the increase, given that businesses are now much more aware of cyber-related issues?

Marc Ruef: There's no contradiction between a greater frequency of attacks and a better understanding of cyber risk. The complexity of systems and, hence, the extent of companies' vulnerability to cyber attack has increased, so it hasn't become any easier to protect systems. Meanwhile, cyber crime has become a business model and is constantly being refined. We are now seeing the first, but very serious, impacts of AI on cyber security, with both companies and criminals benefitting from the new opportunities AI brings.

swissVR Monitor: What measures do you think are most effective in preparing employees for cyber attacks?

Marc Ruef: Successful implementation of cyber security does not start with procuring expensive technology but rather with the company's culture of security, which dictates its specific needs and its scope for action in this area. Staff training is crucial to reducing vulnerability to attack, and over recent decades, companies have had access to a range of technological means to deploy and optimise on an ongoing basis. These include traditional defences, such as firewalls, network segmentation, anti-virus programs and regular systems updates.

swissVR Monitor: Our latest survey shows that more than half of all companies do not have plans in place for restoring essential core IT process following a cyber attack without incurring unacceptable costs or damage. What should plans for such a scenario actually look like? And how should they be tested?

Marc Ruef: Caution and discipline are the key requirements for a secure company. Businesses need to take the time to prepare thoroughly for a crisis, identifying core processes that are at risk and measures to contain the impact of an attack and to restore systems. It is devastating when companies do not tackle this issue early enough: once the crisis has happened, they are in survival mode and simply do not have time to think carefully about the decisions they are making, let alone make plans.

The Board's role in cyber resilience

Sandra Emme, Industry Leader Cloud Enterprise at Google and member of the Board of Belimo and Zehnder Group International

"Many Board members do not realise they have an important role to play. […] Ensuring cyber resilience is not a responsibility that can be delegated to the IT Department; it is an integral part of the Board's non-transferable role of providing overall management of the company."

swissVR Monitor: What is the general role of a Board of Directors in ensuring that their company is cyber resilient?

Sandra Emme: In my discussions with Board members, I am often struck by the fact that many of them do not realise they have an important role to play. In fact, I'd like to add that ensuring cyber resilience is not a responsibility that can be delegated to the IT Department; it is an integral part of the Board's non-transferable role of providing overall management of the company under Article 716a of the Swiss Code of Obligations.

Cyber risk is a strategic risk in the same way financial and operational risk is, and Boards need to tackle it as such and ensure that it is integrated within the company's broader risk management system. The Board's core responsibility is to provide strategic management, defining tolerance of risk, providing adequate financial resources and overseeing clear governance.

The Board must also ensure it receives regular reports on threat levels and security indicators and oversee the effectiveness of emergency planning. It is advisable to document this process to provide a record of fiduciary responsibility, care and continuity. If there is an incident, the Board must ensure that statutory reporting provisions are complied with.

Sandra Emme began her entrepreneurial career in France as the co-founder of a number of IT start-ups, which went on to expand globally and were later bought out. For the past 15 years, she has worked for Google, where she is currently Industry Leader Cloud Enterprise and advises manufacturing companies on transformation, cyber and data strategy. In 2018, Sandra Emme joined the Board of Directors of Panalpina Welttransport Holding AG, followed in 2019 by the Board of Metall Zug AG. She has been a member of the Board of Belimo Holding AG since 2018 and of Zehnder Group AG since 2022. She is also a member of the Executive Board of digitalswitzerland and Lecturer in Digital Business Transformation at IMD Business School in Lausanne. Sandra Emme also has qualifications in Corporate Governance (HSG) and ESG (Competent Boards).

swissVR Monitor: Our survey of Board members shows that only around half of all Boards rehearse their crisis management plans for the eventuality of a cyber attack. What specific risks are the remaining half running?

Sandra Emme: If a Board seriously neglects the issue of cyber resilience, it is breaching its statutory duty of due diligence. A serious cyber attack involving massive financial loss threatens individual Board members with personal civil liability as well as criminal prosecution if statutory reporting responsibilities have not been complied with.

I'd also add that rehearsing crisis management does not mean that the Board actually gets involved operationally in the case of a crisis; that would be counterproductive and would actually hamper the management's crisis team in doing its job. The Board's role is, rather, to check whether the organisation is prepared for a crisis and whether the Board is receiving the information it needs. If Boards do not

rehearse this, they risk wasting a lot of time and making the wrong strategic decisions once a crisis hits the company.

The first specific risk is legal liability: the Board is not liable for the attack itself but it is held responsible for inadequate preparation or strategic errors during a crisis, such as breaching the duty to provide ad hoc disclosure or data protection updates. In such cases, D&O insurers may refuse to cover the cost of such breaches.

Second, there is a risk of paralysis in a crisis. If the Board does not test its plans, it will not know which strategic decisions it will face under enormous time pressure, such as decisions on releasing special funds or informing major shareholders or regulators. Third, there is the dilemma posed by ransom demands: if it has not discussed in advance how to react to a ransom demand, the Board cannot know once an attack is under way whether, and how, it should react to such demands. Nor will it have the resources readily available if it decides it should pay.

The fourth and final risk is that of reputational damage and financial loss: a cyber attack almost always causes reputational damage, even when the crisis is managed well. If the Board is unprepared and communications are not coordinated, though, the risk of damage and loss rises massively to the point of becoming an existential threat, especially to SMEs.

My advice is to conduct tabletop exercises and ensure that management has an 'incident response retainer' in place – an on-call contract with external experts who can provide immediate help and advice. Insurance providers often recommend such a contract or may even make it a condition of insuring companies against cyber risk.

swissVR Monitor: We also found that only about half of all Swiss Boards regularly receive briefings and reports from management about cyber incidents within the company. What is your view of what management should regularly be telling the Board about such incidents?

Sandra Emme: Simply listing incidents, for example, does not address the level of strategic responsibility the Board has. The focus must be on managing risk, and the Board must be able to take specific and well-founded investment decisions. Quantifying cyber risk in monetary terms is the best way of doing that: how many Swiss Francs are we willing to risk?

Future-oriented reporting needs to cover a number of dimensions. The first is reporting on the greatest cyber risks and how they can be mitigated – in other words, what are the major risks to the company's business model, and how is management mitigating them?

Second, how can we protect our 'crown jewels'? How well protected are our most business-critical systems and our most valuable data? Backups should always be stored separately from the main network, for example, placing them out of the reach of external encryption.

The third dimension is reactivity or resilience, with metrics for average detection time. How long does it take for the company to become aware that its network is under attack? How long does it then take to react to that attack? And if an external software manufacturer warns of a security vulnerability, how long does it take for the internal team to patch that vulnerability?

The fourth dimension addresses supply chains and third parties – the need to assess cyber risk across the supply chain, which is often a major gateway for criminals. The fifth dimension involves identifying human risk and AI risk, drawing not only on training but also on a strategic assessment of the security of any AI tools employees are using.

The sixth and final dimension involves an independent view from outside the company or the findings of independent cyber audits, penetration testing or maturity assessments along with security scores, enabling objective benchmarking of the company.

swissVR Monitor: The great majority of Boards do not include members with expertise in cyber issues. When should a Board appoint someone with specific cyber or IT expertise?

Sandra Emme: Not every Board member needs to be an IT expert, but for the whole Board to be tech-blind is strategically very risky indeed. A targeted appointment is a particularly good idea if the 'enablement gap' is widening: the Board needs a member who can act as an interpreter and critically engage with what management has to say about the company's IT systems.

Another reason for making a specific appointment is the fundamental transformation in the IT landscape, including global migration to new ERP systems, 'cloud-first' strategies and instances of AI disrupting core business models. Having a Board member with relevant expertise is also essential to ensuring that the company's cyber maturity meets requirements. If cyber audits reveal gaps, Boards should not wait for the company to fall victim to a major attack – and for shareholders facing personal losses to demand greater know-how within the Board – before they take action in this area.

It's also a good idea to make a targeted appointment in listed companies: investors and advisers on shareholder voting rights are increasingly calling for Boards to have active digital skills, with at least one member with proven experience in technology and cyber-related issues.

It's less common to find medium-sized companies with a full-time IT expert, and having one can make one of the few available Board seats too specific in terms of skills. Convening an external advisory board or inviting an external CISO to act as an adviser is a good way of providing independent input to sit alongside cyber reporting from management.

swissVR Monitor: When is it a good idea for the Board to set up a Cyber Committee or an IT Committee?

Sandra Emme: Having that kind of committee is increasingly seen as best practice across many different sectors. However, it is only essential where the IT landscape within the company is so complex that neither the Board as a whole nor a traditional Audit Committee has the time to develop a deep understanding of the issues at stake. This is particularly the case where there is convergence between OT (operational technology) and IT. If manufacturing companies blend production plants using OT with traditional IT in automated factories, the result is highly complex new vectors for a cyber attack.

Other reasons for having a Cyber Committee or an IT Committee would be that the company needs to reduce massive IT debts, has invested heavily in AI, or needs to carry out complex IT integration following acquisitions.

And a dedicated Cyber Committee or IT Committee can also carry out 'deep dives', enhancing the Board's knowledge and understanding in areas with particular strategic relevance for the company, such as SOC (security operations centre) strategy, protection of supply chains, cyber security, and AI/Internet of Things trends as part of the company's innovation strategy.

Finally, setting up such a committee may also be a response to regulatory pressure. For listed or highly regulated companies, a Technology and Cyber Committee is crucial to provide the 'deep dives' to test IT architectural issues, large IT budgets and security audits, and to provide the Board of Directors with evidenced recommendations.

The importance of artificial intelligence in cyber attacks

Frank Desiere, CEO and member of the Board of Directors of CorTec

"Surveys, including swissVR Monitor, show that a considerable proportion of Boards of Directors are not being briefed regularly on the use and risks of AI. But without such reporting, the Board simply cannot fulfil its duty of oversight."

swissVR Monitor: The uses of artificial intelligence (AI) are expanding, now including the launch of cyber attacks. How has AI changed the nature and frequency of cyber attacks over recent years?

Frank Desiere: I'd describe the role of AI as shifting the economy of a cyber attack. AI reduces the marginal cost of such an attack to almost zero, as it means the brief, research into targets and creation of convincing content can all be automated and scaled up as much as needed. In the past, a cyber attack required a specialised team; now, the skills threshold is much lower.

In terms of the nature of attacks, the shift is probably even more serious. IBM's "Cost of a Data Breach Report 2025" finds that around 16% of data breaches investigated that year involved attackers using AI, in most cases AI-generated phishing and deepfakes for impersonation purposes. Linguistic errors are no longer a reliable way of detecting attacks, which are now individualised and highly contextualised, and use deepfakes to reproduce CEOs' voices and appearance convincingly for the purposes of fraud.

The key concern for Boards of Directors is the ever-shorter window between detection of a vulnerability and its exploitation by cyber attackers. This shifts the company's position from 'defending its perimeter' to 'rapid detection and containment'. Cyber defence is therefore no longer a question simply of having good IT but of resilience – something that is firmly part of the Board's agenda.

Dr. Frank Desiere is CEO of CorTec, where he is also a non-executive director. This dual role shapes his view of governance: he is familiar with operational managerial responsibility but also with the supervisory and monitoring role of a Board of Directors – the interface where effective management is forged. His newsletter and podcast, WE TALK BOARD, are aimed at serving and incoming Board members, Presidents of Boards and senior managers. His focus takes both a Swiss and a European perspective to the effectiveness of Boards, responsible company management, and ongoing training and development of non-executive directors. Alongside his managerial and governance roles, Dr. Desiere gives keynote addresses and delivers executive sessions on governance issues, including as part of Deloitte's Board Programme. His priority is practical and evidence-based guidance for all those who take on a Board of Directors mandate.

swissVR Monitor: We're currently at a point of transition from agentic AI to multi-agent AI. What does this technological advance signify for the risk of cyber attack in the future?

Frank Desiere: The distinction is qualitative, not a matter of degree. Generative AI has provided attackers with better tools but left human managers without a defence. And this is exactly where agentic AI is pushing at the boundaries: the AI agent plans, acts, observes and adapts – in most cases without any human intervention at all.

In November 2025, Anthropic demonstrated the new reality when it published details of the first documented – and largely AI-orchestrat-

ed – espionage campaign on around 30 targets worldwide. The company estimates this was the work of an actor close to government but that the AI carried out between 80% and 90% of the operation autonomously, with human intervention at only a small number of key points. And this attack took place at machine speed.

Multi-agent systems are now taking this to the next level, using specialist agents to carry out a chain of attacks collaboratively and react to defence in real time. We are moving towards a machine versus machine dynamic in which purely human defences are structurally too slow.

The implications for Boards are that the company's defences must also be automated and that the agents we currently use, with their rationales, storage capacity and access to tools, are themselves becoming independent targets of attack. This is the downside of any AI-based efficiency measures a Board approves.

swissVR Monitor: Our survey of Swiss Board members demonstrates that only a small minority of companies have a detailed strategy to tackle AI-based cyber attacks. How do you asses the risk to companies that fail to take account of cyber attacks using AI?

Frank Desiere: That risk is considerable – but I want to be clear exactly where it lies. There are two areas of vulnerability. First, if companies do not take account of AI-supported attacks, they are using yesterday's tools to defend themselves against today's threats. Signature-based detection is powerless against adaptive malware, and attackers have already industrialised their methods.

The second vulnerability arises within the company itself and is underestimated: companies' own uncontrolled use of artificial intelligence. The 2025 IBM report found that around one data security breach in five was related to 'shadow AI' and that incidents of this kind cost an average of USD 670,000 more to tackle than other kinds of breaches. And 63% of the companies falling victim to this kind of attack had no guidelines on AI governance in place. Here, the risk is not from the criminals behind an attack but from company employees feeding customer data or intellectual property into external AI models.

But I would also like to warn against purely performative action. Not every company needs a free-standing AI cyber strategy document. What is important is that cyber issues are integrated into the company's existing risk framework and that managing these risks is seen as an issue for the whole company, not just as an IT issue, and is oriented to recognised standards, such as NIST CSF 2.0 or ISO 27001. SMEs are particularly vulnerable: they have fewer resources but are also increasingly at risk through their supply chains, such as in the wake of the European Union's NIS2 Directive. Companies that delay taking action here risk becoming a case study for the next incident.

swissVR Monitor: So what specific measures should companies take to protect themselves against AI-based cyber attacks?

Frank Desiere: I'd identify five priorities – and I'll list them in order. First, fight AI with AI. Companies need behaviour- and anomaly-based detection and automatic responses if they are to be able to react at machine speed. IBM reports that organisations already using AI and automation as part of their defence save around USD 1.9 million a year on each incident – and can limit attacks much more quickly.

Second, zero trust and rigorous identity and permissions management, specifically for machine identities and AI agents that increasingly have their own access credentials, is vital. Third, introduce phishing-resistant authentication, such as passkeys, combined with mandatory four-eyes scrutiny and the ability to recall payments and authorisations. Simply having a 'bad feeling' is no use when you are up against deepfake CEO fraud: what's needed is a proper process.

Fourth – and this is often underestimated – human sensitivity needs to be recalibrated. The rule of thumb that typos and linguistic errors are a giveaway of a cyber attack simply won't work now that notifications are linguistically impeccable. And fifth, basic hygiene remains crucial: patch management, backups that cannot be changed or amended, network segmentation, and an incident response plan that is regularly tested rather than remaining a paper document.

I'd also add two further things at company level: hedging the supply chain and governance of the company's own AI applications against data leaks and injection of prompts. The order is important here: build resilience first and then add in other measures. Finally, the Board needs to be briefed on the maturity of each one of these aspects, not just on activity.

swissVR Monitor: And what is the role of the Board in ensuring that a company is always up to date with technological trends and that it is prepared for the risks they pose, such as AI-based cyber attacks?

Frank Desiere: Cyber risks and AI risks are matters for the Board, both in law and in practical terms. These risks relate to the non-transferable responsibility of the Board for overall management of the company and to its duty to act with due diligence under Articles 716a and 717 of the Swiss Code of Obligations. Operational implementation can be delegated to management or a CISO; oversight cannot and if the Board fails to fulfil its duties, it is personally liable for any losses under Article 754 of the Code of Obligations. Having D&O insurance does not replace this duty; it makes it a prerequisite.

The Board of Directors does not require extensive technological expertise, but it does need to know enough to ask the right questions and to make well-founded requests of management. It must also ensure that the necessary expertise is available either within the Board or from expert advisers. Specifically, this means: a clear line of responsibility via a Risk Committee or Audit Committee, structured reporting rather than simply listing details of incidents, a tried and tested crisis plan that sets out the specific role of the Board, resources that reflect the company's appetite for risk, and a keen eye on the regulatory horizon, including revisions to the Swiss Federal Data Protection Act, the impact of NIS2, and the EU's AI Act.

This is where the vulnerability actually lies. Surveys, including swissVR Monitor, show that a considerable proportion of Boards of Directors are not being briefed regularly on the use and risks of AI. But without such reporting, the Board simply cannot fulfil its duty of oversight.

My principle, both as a CEO and as a Board member, is that our job is not to provide security ourselves but to ensure that the right questions are being asked consistently and that the company tackles cyber resilience as part of its overall resilience plan and not simply as an IT issue. These are exactly the kinds of governance issues I discuss regularly and in detail in my LinkedIn newsletter WE TALK BOARD.

Authors

swissVR

Isabelle Amschwand
President swissVR
+41 41 757 67 11
isabelle.amschwand@swissvr.ch

Dr. Brigitte Maranghino-Singer
CEO swissVR and Lecturer, Institute of Financial Services Zug (IFZ), Lucerne University of Applied Sciences and Arts
+41 41 228 41 19
brigitte.maranghino@swissvr.ch

Deloitte AG

Reto Savoia
CEO Deloitte Switzerland
+41 58 279 60 00
rsavoia@deloitte.ch

Dr. Michael Grampp
Chief Economist and Head of Research
+41 58 279 68 17
mgrampp@deloitte.ch

Dr. Daniel Laude
Project and Research Manager
+41 58 279 64 35
dlaude@deloitte.ch

Hochschule Luzern

Prof. Dr. Mirjam Gruber-Durrer
Lecturer in Normative Board Management, Institute of Financial Services Zug (IFZ), Lucerne University of Applied Sciences and Arts
+41 41 228 41 73
mirjam.gruber-durrer@hslu.ch

swissVR is an association of Board members in Switzerland – from Board members for Board members – attractive – independent – focused – across Switzerland. With its offering, swissVR contributes to professionalising Board member activities in Switzerland. It enables its members to share their experience with Board members from all sectors of the Swiss economy. It also offers its almost 1,400 members information and training tailored to their needs. swissVR is targeted exclusively at individuals with an active Board mandate. Detailed information can be found at www.swissvr.ch.

Deloitte AG is a shareholder in Deloitte EMEA BV (EMEA), which is a member firm of Deloitte Touche Tohmatsu Limited (DTTL). DTTL and its member companies are legally independent and stand-alone companies. DTTL and Deloitte EMEA BV themselves do not provide services to clients. A detailed description of their legal structures can be found at www.deloitte.com/ch/about. Deloitte AG is an audit firm recognised and supervised by the Swiss Federal Audit Oversight Authority (FOAO) and the Swiss Federal Financial Market Supervisory Authority (FINMA).

The **Hochschule Luzern** is the University of Applied Sciences and Arts of the six Central Swiss cantons and brings together Schools of Engineering and Architecture, Business, Computer Science and Information Technology, Social Work, Design, Film and Art, and Music, as well as a focus on health. It is the largest educational institution in Central Switzerland with around 8,700 students attending courses and a further 13,000 on continuing education programmes, including 5,600 studying for its Certificate of Advanced Studies (CAS), Diploma of Advanced Studies (DAS) or Master of Advanced Studies (MAS) courses for members of Boards of Directors. It is currently engaged in 274 new research projects and has a staff of 2,144. The Institute of Financial Services Zug (IFZ) of the Hochschule Luzern focuses on governance, risk and compliance and offers continuing education for Board Members, in particular the Certificate of Advanced Studies for Boards of Directors (CAS Verwaltungsrat). Detailed information can be found at www.hslu.ch/ifz-verwaltungsrat / www.hslu.ch/cas-vr / http://www.hslu.ch/ifz.