Cyber resilience – increasingly important for Boards

swissVR Monitor II/2023
September 2023

swissVR®

Deloitte.

Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern

Contents

About the survey
This is the 14th edition of swissVR Monitor and is based on a survey of 400 members of Swiss company Boards of Directors. The aim of the survey is to gauge Board members' attitudes to the economy and the outlook for business, and corporate governance issues. This edition also focuses specifically on the topic of companies' 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 22 May and 8 July 2023. A total of 400 Board members took part, representing listed companies as well as small and medium-sized companies (SMEs) from every major sector of the Swiss economy. 32% of the participants are from large companies, 35% from medium-sized companies and 33% from small companies.

The aim of swissVR Monitor is to offer 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/2023. For this edition, we surveyed 400 members of company Boards of Directors across Switzerland. The findings reflect their attitudes to the economy and the outlook for business and to relevant areas of their own role.

The special focus topic in this edition is cyber resilience. This has become an increasingly important issue over the last few years, and this edition of swissVR Monitor explores it for the first time since H2 2017. The number of cyber attacks on companies has risen in recent years, so it is important for Board members to focus on cyber resilience as part of their mandate and to reach a clear understanding of their role and responsibilities. This edition therefore focuses on, among other things, the potential consequences of cyber attacks on companies, how Board members assess their company's cyber resilience, and cyber reporting by management to the Board.

Alongside the survey findings, swissVR Monitor II/2023 conducted interviews on the focus topic with:

- Maya Bundt, Chair of the Nomination and Remuneration Committee of Valiant Bank and member of the Board of Bâloise and APG|SGA
- Florian Schütz, Federal Cyber Security Delegate, head of the Swiss National Cyber Security Centre (NCSC) and, from 1 January 2024, Director of Switzerland's new Federal Office for Cybersecurity
- Sonja Stirnimann, Chair of the Audit Committee of Glarner Kantonalbank and member of the Board of Directors of Apiax

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.

Cornelia Ritz Bossicard
President swissVR

Reto Savoia
CEO Deloitte Switzerland

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

Summary and key findings

24%
of Board members rate the prospects for the Swiss economy over the next 12 months as positive.

Economic outlook slightly brighter than in the beginning of 2023
Board members in Swiss companies are a little more upbeat than in the beginning of 2023 in their rating of the country's economic, sector and business outlook over the next 12 months. Across all three indicators, more Board members rate the prospects as positive than rate them as negative. Factors still causing economic uncertainty include geopolitical risks, the energy situation in winter 2023–24, and persistent – and above average – inflation.

42%
of cyber victims say an attack has disrupted their company's operations.

Cyber attacks can have very serious consequences for companies
Board members whose company has already been the victim of at least one cyber attack report a (serious) impact on the company's processes. Most frequently, cyber attacks disrupt operations. They can also result in data leaks, product malfunctions or service disruption. Less frequently, they result in the company becoming a gateway for cyber attacks on customers or in loss of assets.

55%
of Board members think the importance of cyber resilience has increased significantly over the last three years.

Cyber resilience now markedly more important to companies
Almost all Swiss Board members surveyed agree that the importance to their company of cyber resilience has increased in the last three years. A majority think this increase has been marked, especially those on the Boards of small companies. Only a small minority of Board members report that there has been no change in the importance of cyber resilience, and none think the topic has become less important.

46%
report that their company is insured against cyber risks.

Mixed picture in relation to cyber risk insurance
Although cyber resilience has grown in importance and cyber attacks can have serious consequences, only just under half of all companies are insured against cyber risks. Companies in the financial, the manufacturing/chemicals and the construction sectors are more likely than average to be insured against such risks. Company size is much less likely to play a part in whether companies have cyber risk insurance.

56%
of Boards receive reports from management on cyber-related incidents within the company.

Regular cyber reporting to the Board could be improved
More than half of all Swiss Boards receive regular reports from management on cyber-related incidents in the company or on the need for action and/or investment in cyber resilience. Just under half receive reports focusing on the general threat level or on cyber resilience measures. Only around one Board in three is regularly briefed by management on the main cyber risks facing the company or on its cyber strategy.

43%
of Boards set up committees.

Large companies and financial services firms most likely to have committees
Just under half of all Boards set up committees to tackle specific issues. The figure is higher in large companies (where three-quarters of Boards have committees) than in small companies (one in five Boards). Boards in the financial services sector are most likely to have committees: three-quarters of Boards have at least one committee. In most other sectors, fewer than half of Boards have one or more committees. However, many Boards assign special responsibilities or areas to individual members.

Outlook

Economic, sector and business outlook

Board members in Swiss companies believe the **economic, sector and business outlook** over the next 12 months will follow the pattern of the last few years (see Chart 1). From its 2019 average, the outlook worsened in 2020 as a result of the COVID-19 pandemic before recovering markedly in 2021. Expectations then dipped again as a result of the outbreak of the war in Ukraine in early 2022, but Board members' optimism about the prospects for the Swiss economy over the next 12 months is now returning. Factors still causing economic uncertainty include ongoing geopolitical risks, the energy situation in winter 2023-24, and persistent – and above average – inflation.

Board members are slightly more optimistic in their rating of the country's **economic outlook** than in H1 2023. 24% of Board members rate the prospects for the Swiss economy over the next 12 months as positive compared with 10% who rate them as negative. A large majority of Board members (66%) therefore rate the outlook as neutral. These findings are in line with other current forecasts for modest growth in the Swiss economy.

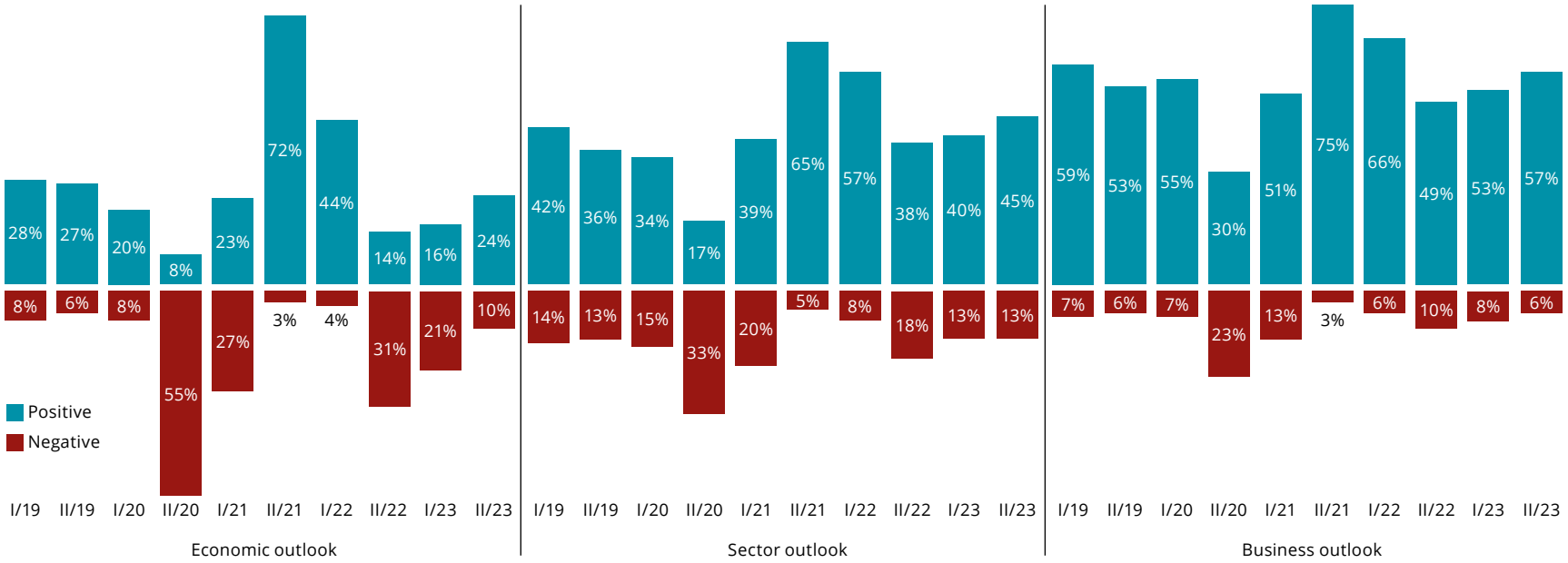
The **sector** outlook is also more positive than in H1 2023. 45% of Board members rate it as positive, while 13% rate it as negative. Board members from the ICT sector are particularly likely to take an optimistic view: 81% rate the outlook as positive, with none rating it as negative. This may be linked to the ongoing digitalisation of the Swiss economy. By contrast, respondents from the manufacturing/chemicals sector are most likely to be pessimistic, with slightly more Board members rating it as negative than as positive (24% and 22% respectively). The main drivers of these findings are the ongoing inflationary pressures on raw materials and intermediate products and uncertainties in global demand.

The **business outlook** is also slightly brighter than in H1 2023, with more than half of Board members (57%) rating the outlook for their company's business over the next 12 months as positive; just 6% rate it as negative. As with the economic and sector outlook, Board members from the ICT sec-

tor are particularly likely to rate the business outlook as positive (83%) of respondents, with none rating it as negative. Respondents from the manufacturing/chemicals sector are most likely to take a pessimistic view, with 32% rating the outlook as negative as against 22% who rate it as positive.

Chart 1. Economic, sector and business outlook over the next 12 months [swissVR Monitor I/2019 to II/2023]

Question: How do you rate the prospects for the Swiss economy / sector / your company over the next 12 months?
Note: Responses that are neither negative nor positive are deemed to be neutral.



Focus topic: Cyber resilience – increasingly important for Boards

Cyber attacks on businesses and other organisations have become much more frequent and serious over recent years. The COVID-19 pandemic has been a key driver of this trend: having more employees than ever before working from home has laid bare the vulnerability of some companies' IT infrastructure. The media have also been reporting more cases of cyber attacks on large and prominent businesses that have impacted on their operations and profitability. Finally, ongoing digitalisation and the advance of artificial intelligence mean that cyber attacks are likely to become even more frequent and more serious in future. For these reasons, Board members need to tackle the issue of cyber resilience within their own company and come to a clear understanding of their role and responsibilities in this area.

Cyber-related incidents and the impact of cyber attacks

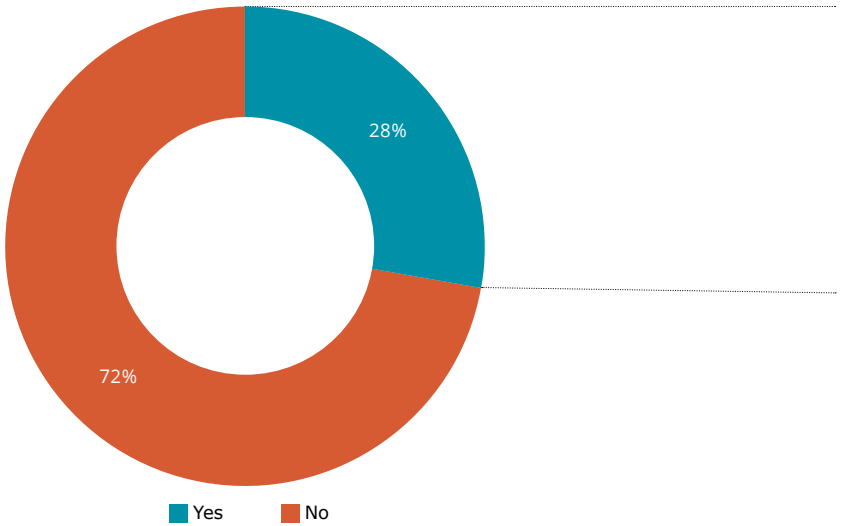
A minority of Swiss companies (28%) report that their company has been **the victim of a cyber attack** (see Chart 2). The remaining 72% say their company has not been the victim of a cyber attack or that they are not aware of such an attack. The number of companies affected may actually be slightly higher: the survey also shows that Board members do not always receive regular reports from management on cyber-related incidents, with only around 56% reporting that they are regularly briefed (see Chart 7).

Company size is a major factor here. Just 18% of Board members from small companies report one or more cyber attacks on their company, but this rises to almost half (45%) of Board members from large companies. This disparity may be the result either of a correlation between company size and the frequency of cyber attacks (the larger the company, the more attacks it is victim to) or of the fact that Board members from large companies are better informed about cyber attacks (see section "The Board of Directors and cyber resilience").

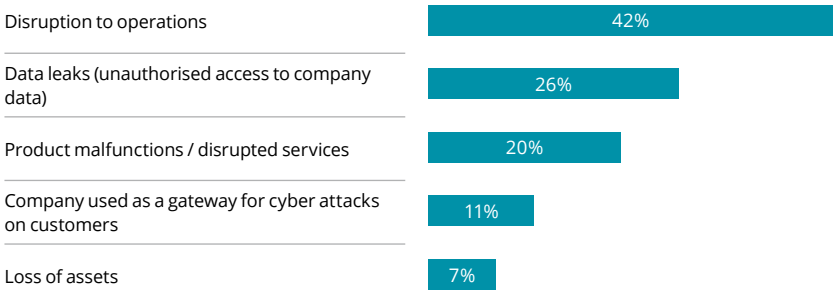
Chart 2 also illustrates the impact a cyber attack has on companies and shows that **disruption to operations** is by far the most frequent consequence (42% of responses). Board members from the ICT sector are particularly likely to cite disruption to operations following a cyber attack, with nearly seven out of ten listing this impact (69%). **Data leaks** and **product malfunctions/disrupted services** follow, cited by 26% and 20% of Board members respectively. The frequency with which respondents cite disruption to operations and product malfunctions/disrupted services demonstrates that cyber attacks frequently have a very specific impact on the company's processes. 11% of Board members also cite such attacks as resulting in the company being used as a gateway for **cyber attacks on customers**. Finally, 7% report **loss of assets.**

Chart 2. Cyber-related incidents and the impact of cyber attacks on the company

Question: As far as you are aware, has your company ever been the victim of a cyber attack (unauthorised access to data, hacking of customer communications, disruption to your website, etc.)?



Question: What impact did the attack(s) have on the company? (Multiple answers possible, n=113)



The importance of cyber resilience

Board members report that the importance to companies of cyber resilience and related topics has increased markedly over recent years (see Chart 3). A majority of Board members from Swiss companies (55%) report that its importance has **increased a lot**, 40% say it has **increased somewhat** and just 5% report **no change**. No respondents report that this topic has decreased in importance.

As with the frequency of cyber attacks, company size is a determining factor here: 88% of Board members from small companies say that the importance of cyber resilience has increased (43% that it has increased a lot and 45% that it has increased somewhat). This compares with 99% of Board members from large companies who report that the importance of cyber resilience has increased a lot or somewhat (70% and 29% respectively). This finding may point to a correlation between company size and the incidence of cyber attacks or else to the fact that large companies tackle cyber issues more systematically, for example by having a dedicated IT department or a Chief Information Security Office (CISO).

Among the sectors reporting the largest increase in the importance of cyber resilience is the manufacturing/chemicals sector, where an above-average 65% of Board members report that the importance of cyber resilience has increased a lot. Across all sectors, new business models and the greater networking of humans, machines, products, systems and companies – the 'Internet of Things' (IoT) – is another reason for cyber resilience being a growing concern for many companies.

Cyber risk insurance

As Chart 4 shows, Board members are divided on the issue of insurance against cyber risks. Just under half (46%) report that their company is **insured against cyber risks**, only slightly more than the 41% whose compa-

Chart 3. Importance of cyber resilience for companies

Question: How has the importance of cyber resilience to your company changed over the last three years?

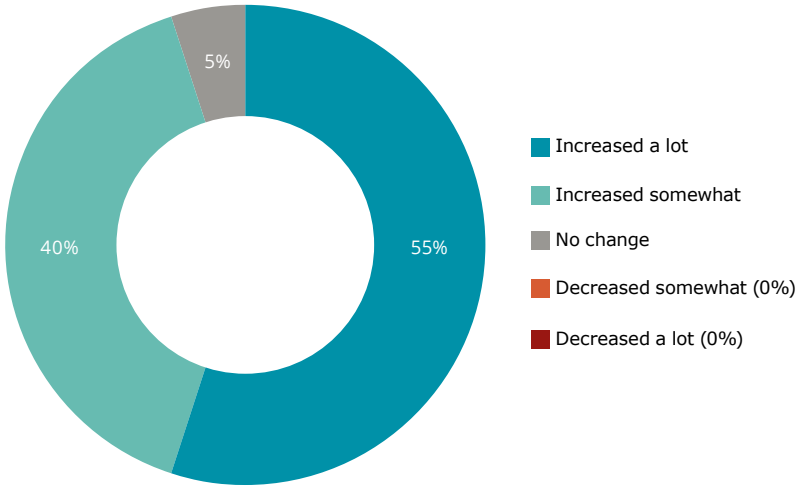
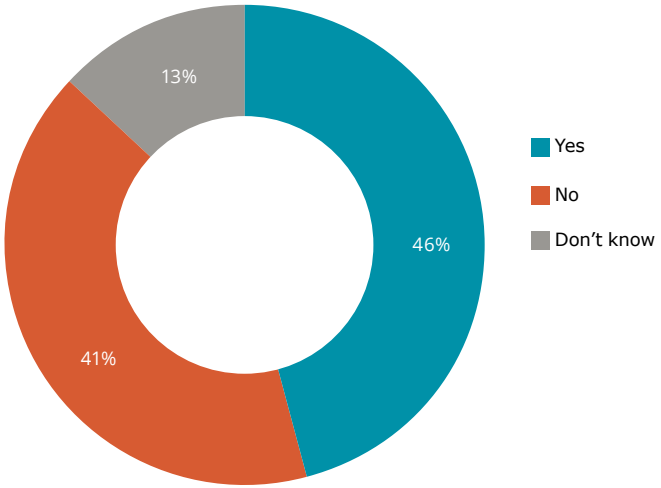


Chart 4. Insurance against cyber risks

Question: Is your company insured against cyber risks?



ny is **not insured.** Around one Board member in eight (13%) **do not know** whether or not their company is insured.

Companies from the financial services, manufacturing/chemicals and construction sectors are most likely to be insured against cyber risks (58%, 54% and 51% of companies respectively). In all other sectors, a minority of companies have cyber risk insurance. There are few differences between companies of differing size.

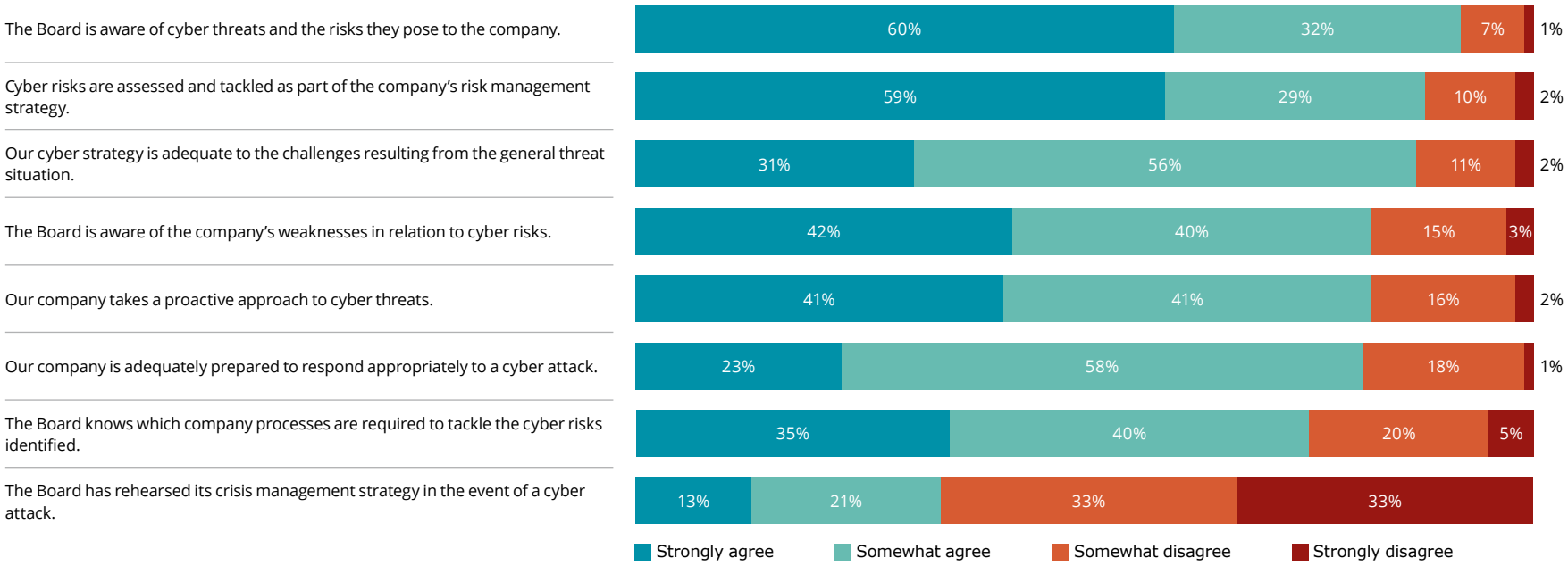
The Board of Directors and cyber resilience

Chart 5 shows that a majority of Swiss Board members believe they and their companies are well informed about cyber threats and well prepared to tackle this issue. More than nine out of ten Board members (92%) strongly agree or somewhat agree that their Board **is aware of cyber threats and the risk they pose to their company.** A similar proportion agree that **cyber risks are assessed and tackled as part of the company's risk management strategy in at least some cases** (88%) and that **the company's cyber strategy is adequate to the challenges resulting from the general threat situation** (87%).

A majority of Board members also strongly agree or somewhat agree that their Board is **aware of the company's weaknesses in relation to cyber risks** (82% of respondents), that their company takes a **proactive approach to cyber threats** (82%), and that their Board **is adequately prepared to respond appropriately to a cyber attack** (81%). Three-quarters of all Board members surveyed (75%) strongly agree or somewhat agree

Chart 5. Self-assessment of the Board of Directors regarding cyber resilience

Question: Please indicate your response to the following statements in relation to your Board of Directors.



that their Board **knows which company processes are required to tackle the cyber risks identified**.

All the responses indicate that Board members from large companies are more likely than average to strongly agree or somewhat agree with statements, while those from small companies are less likely than average to strongly agree or somewhat agree. This suggests that cyber resilience is a more systematic and institutionalised part of how large companies and their Boards operate than it is in small companies.

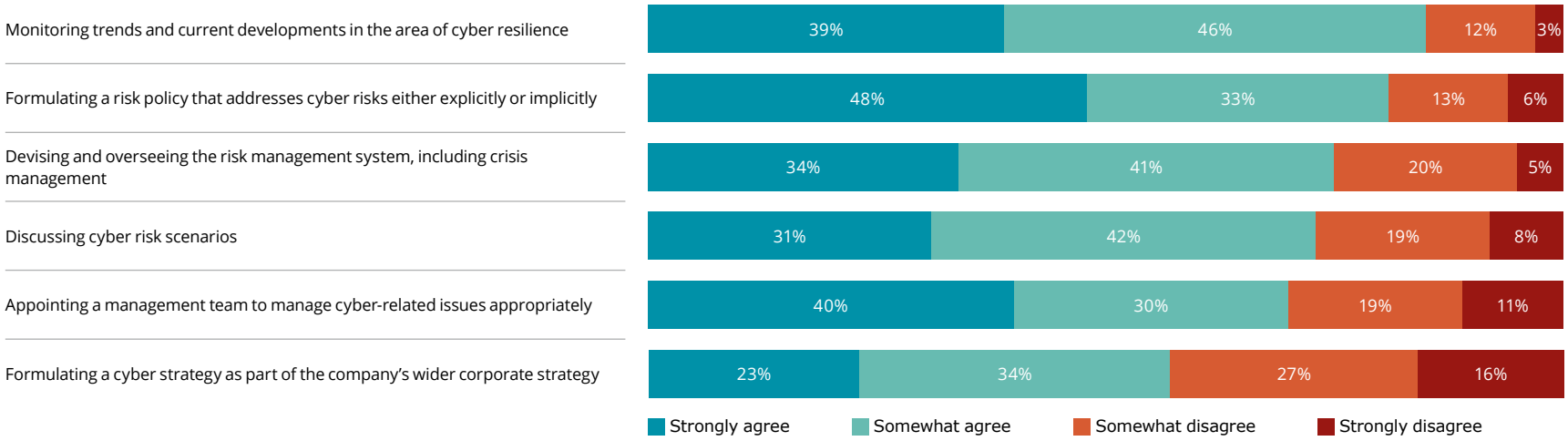
Just one Board member in three – 34% – says that their Board has **rehearsed its crisis management strategy in the event of a cyber attack**, at least to some extent. Board members from large companies are more likely to strongly agree or somewhat agree with this statement than those from small companies (45% and 26% respectively). Almost half of Board members in the financial services sector (45%) agree, compared with only around a quarter (24%) of those in the corporate services sector. The figure is lower still, just one in five respondents (19%), in the retail and consumer goods sector.

Chart 6 paints a mostly positive picture in relation to the Board's role and responsibilities. A very large majority (85%) of Swiss Board members strongly agree or somewhat agree that their Board **monitors trends and current developments in the area of cyber resilience**. Slightly fewer (81%) strongly agree or somewhat agree that their Board is **responsible for formulating a risk policy that addresses cyber risks either explicitly or implicitly**.

A majority of Board members strongly agree or somewhat agree that their Board also **devises and oversees the risk management system, including crisis management** (75% of respondents), **discusses cyber risk scenarios** (73%), and **appoints a management team to manage cyber-related issues appropriately** (70%). Only just over half of Board members surveyed (57%) say their Board **formulates a cyber strategy as part of**

Chart 6. Tasks/roles of the Board of Directors regarding cyber resilience

Question: To what extent does your Board perform the following cyber resilience tasks/roles?



the company's wider corporate strategy. Here, too, there is a correlation with company size: more respondents from large companies indicate their Board carries out such roles than those from small companies.

Chart 7 shows Board members' responses in relation to whether they receive regular cyber reporting or reports from management on a range of cyber issues. Just over half of respondents say they receive reports on **cyber-related incidents within the company** or on **the need for action and/or investment** in cyber resilience (56% and 53% of respondents respectively). However, only a minority of Board members say they receive reporting on **the general threat level** (43% of respondents), **cyber resilience measures** (42%), **an overview of the most serious cyber risks** (33%) or the company's **cyber strategy or cyber programme** (32% of respondents). As with other aspects, Board members from large companies are more likely to receive reporting on these issues than those from small companies. There are few differences between sectors.

Chart 7. Cyber reporting to the Board of Directors

Question: On which issues does your Board receive regular cyber reporting or reports from the management team? (Please select all that apply.)

Organisational issues within the Board of Directors

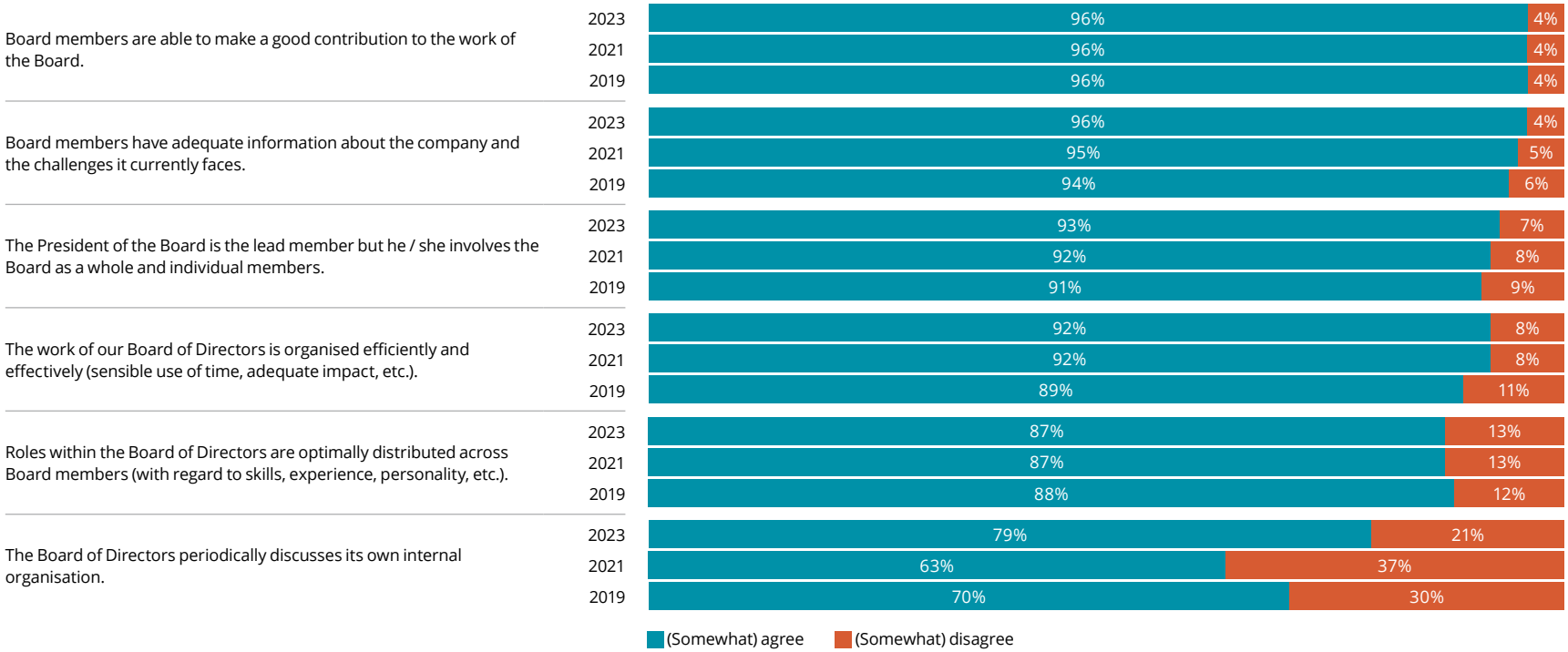
Internal organisation within the Board of Directors

The internal organisation of the Board of Directors includes in particular the allocation of roles within the Board and the influence individual members have within the Board. In general terms, Swiss Board members rate their Board's internal organisation positively (see Chart 8). This mirrors the findings from two years and four years ago, when this question was last asked (swissVR Monitor II/2019 and swissVR Monitor II/2021). Overall, Board members' views are very similar to those expressed in the earlier surveys, giving a robust longitudinal picture of their views.

Almost all Board members surveyed (96%) strongly agree or somewhat agree that **Board members are able to make a good contribution to the work of the Board**. The same percentage think that they and their colleagues **have adequate information about the company and the challenges it currently faces.** Slightly fewer – 93% – strongly agree or some-

Chart 8. Internal organisation of the Board of Directors

Question: Please indicate your agreement with the following statements.



what agree that **the President is the lead member but involves the Board as a whole and individual members**. Similarly high proportions of Board members say that **the Board's work is organised efficiently and effectively** (92%) and that **roles are optimally distributed across Board members** (87%).

79% of Board members strongly agree or somewhat agree that **the Board of Directors periodically discusses its own internal organisation**. While lower than for other statements, this figure is markedly higher than in the 2019 and 2021 surveys, which suggests that the situation has improved. There are only very small differences regarding company size and sector on these issues.

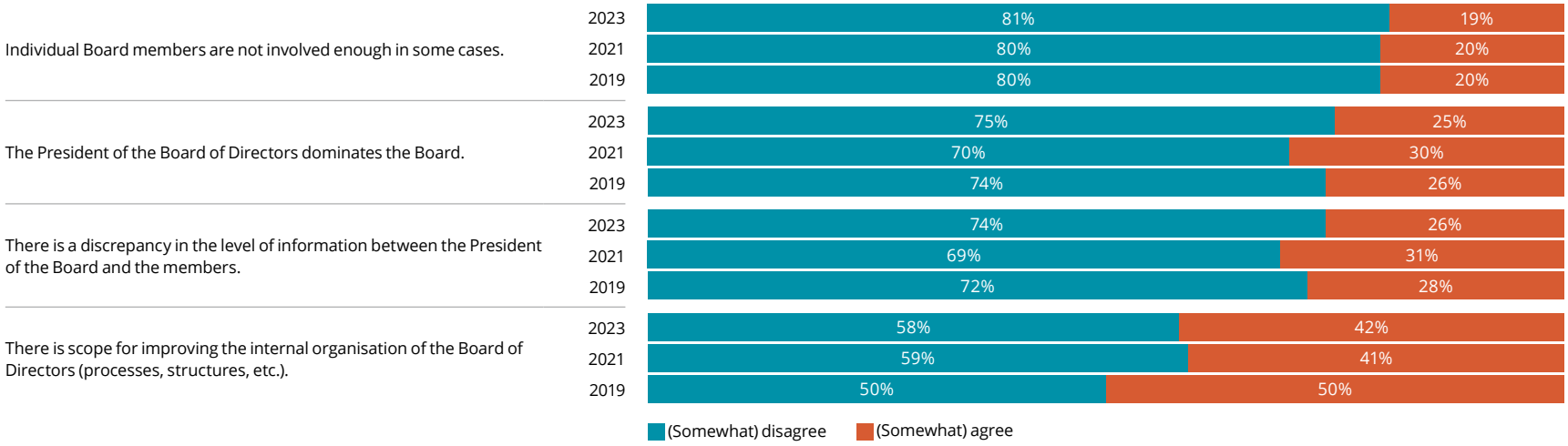
Challenges facing the Board of Directors

Boards face a number of challenges in carrying out their work cooperatively. As Chart 9 illustrates, their responses to statements relating to these challenges confirm the generally positive view Board members have of their Board's internal organisation but also suggest room for improvement.

As in swissVR Monitor II/2019 and swissVR Monitor II/2021, just under one Board member in five (19%) strongly agrees or somewhat agrees that they or their colleagues on the Board are not involved enough in some cases. Around a quarter of Board members see the **dominance of the President of the Board** and the **discrepancy in the level of information between the President and the members** as a challenge (25% and 26% of respondents respectively). A relatively high proportion of Board members – two in five (42%) – strongly agree or somewhat agree that **there is scope for improving the internal organisation of the Board** (processes, structures, etc.). Despite the generally positive views expressed by Board members, these findings point to a need for improvement in the way Boards of Directors are organised and work together. The findings are broadly consistent across companies of differing size and across sectors.

Chart 9. Challenges facing the Board of Directors

Question: Please indicate your agreement with the following statements.



Special responsibilities and committees

Nearly two-thirds of all respondents (63%) report that their Board allocates **special responsibilities or areas to individual members** (see Chart 10). This figure is almost identical with the findings of the two previous surveys that asked this question (59% in swissVR Monitor II/2019 and 62% in swissVR Monitor II/2021).

The proportion of Boards that allocate special responsibilities or areas to individual members depends on the size of the company. Boards do so in 70% of large companies compared with 58% of small companies. The main reason for this is that Boards of large companies tend to have more members than those of small companies (an average of seven members and four members respectively). Sectoral differences are also particularly marked: Boards in the commerce and consumer goods sector are more likely than the average to allocate special responsibilities or areas to individual members, while those in the manufacturing/chemicals sector are less likely than the average to do so (76% and 51% of Boards respectively).

Around four out of ten respondents (43%) report that their Board has **set up committees**. This figure is nearly identical with the findings of the two previous surveys that asked this question (41% in swissVR Monitor II/2019 and 43% in swissVR Monitor II/2021).

Differences between companies of differing size and in different sectors are more marked than is the case with allocation of special responsibilities

Chart 10. Special responsibilities / areas and committees

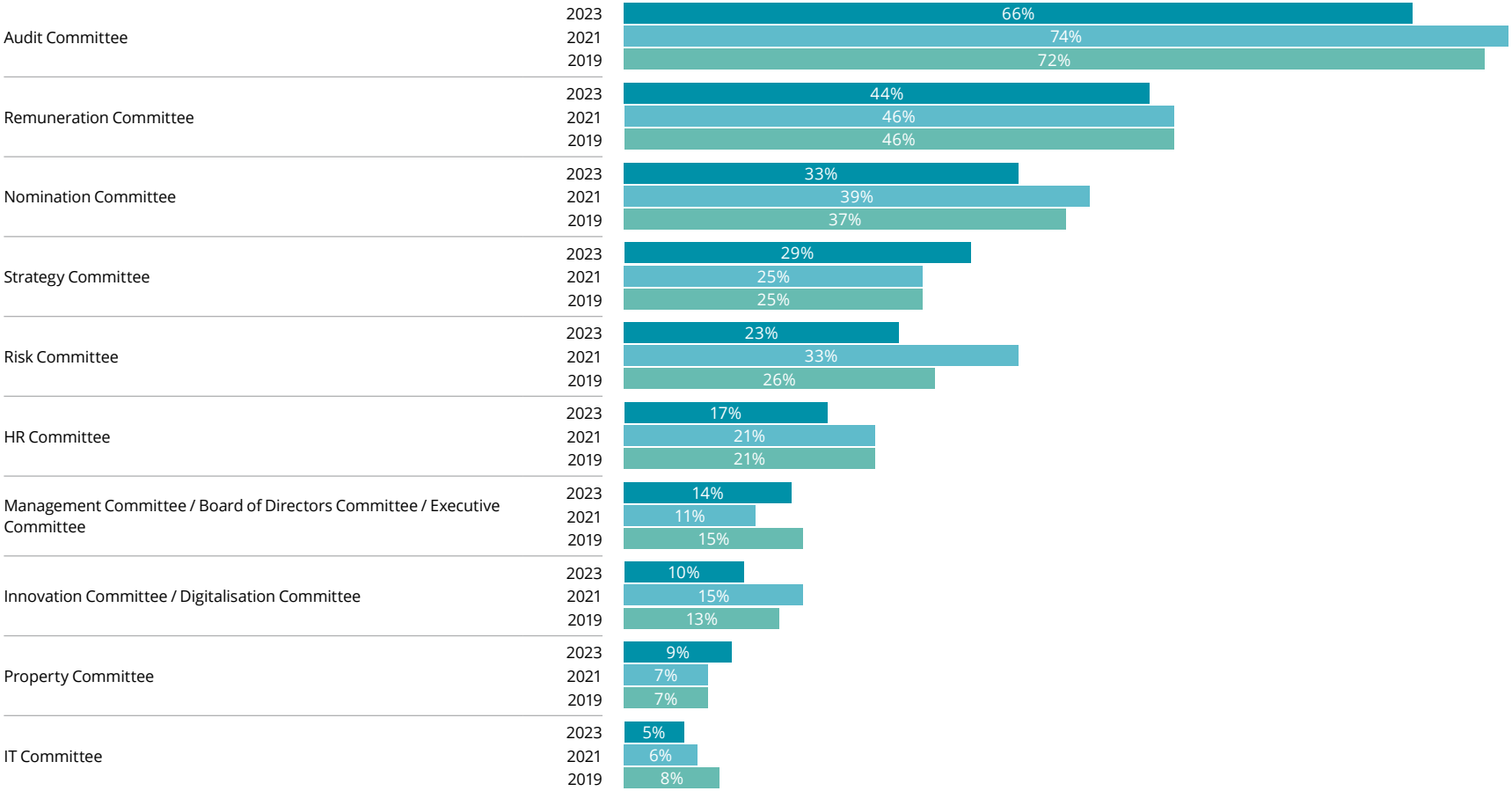
		We have allocated special responsibilities or areas to individual Board members	We have set up committees within the Board of Directors
Total II/2023		63%	43%
Total II/2021		62%	43%
Total II/2019		59%	41%
By company size (II/2023)	Small companies	58%	20%
	Medium-sized companies	63%	35%
	Large companies	70%	75%
By selected sectors (II/2023)	Corporate services	56%	18%
	Commerce / consumer goods	76%	41%
	Financial services	65%	75%
	Pharma / life sciences / medtech / health	65%	43%
	Manufacturing / chemicals	51%	38%
	Information and communications technology	65%	15%
	Construction	60%	35%

or areas. Three-quarters of Boards in large companies (75%) have set up committees, a marked contrast with just 20% of Boards in small companies. Committees are particularly numerous in the financial services sector, where 75% of Boards have set them up. One reason for this is that Switzerland's Federal Financial Markets Supervisory Authority (FINMA) requires all banks with a given number of employees to set up an Audit and Risk Committee. By contrast, Boards from the corporate services and ICT sectors are the least likely to set up committees (just 18% and 15% respectively of Boards in those sectors).

Of Boards with at least one committee, two-thirds (66%) report that they have an **Audit Committee** (see Chart 11). This makes Audit Committees

Chart 11. Types of committees

Question: Which committees does your Board have? (Multiple answers possible, n=170)

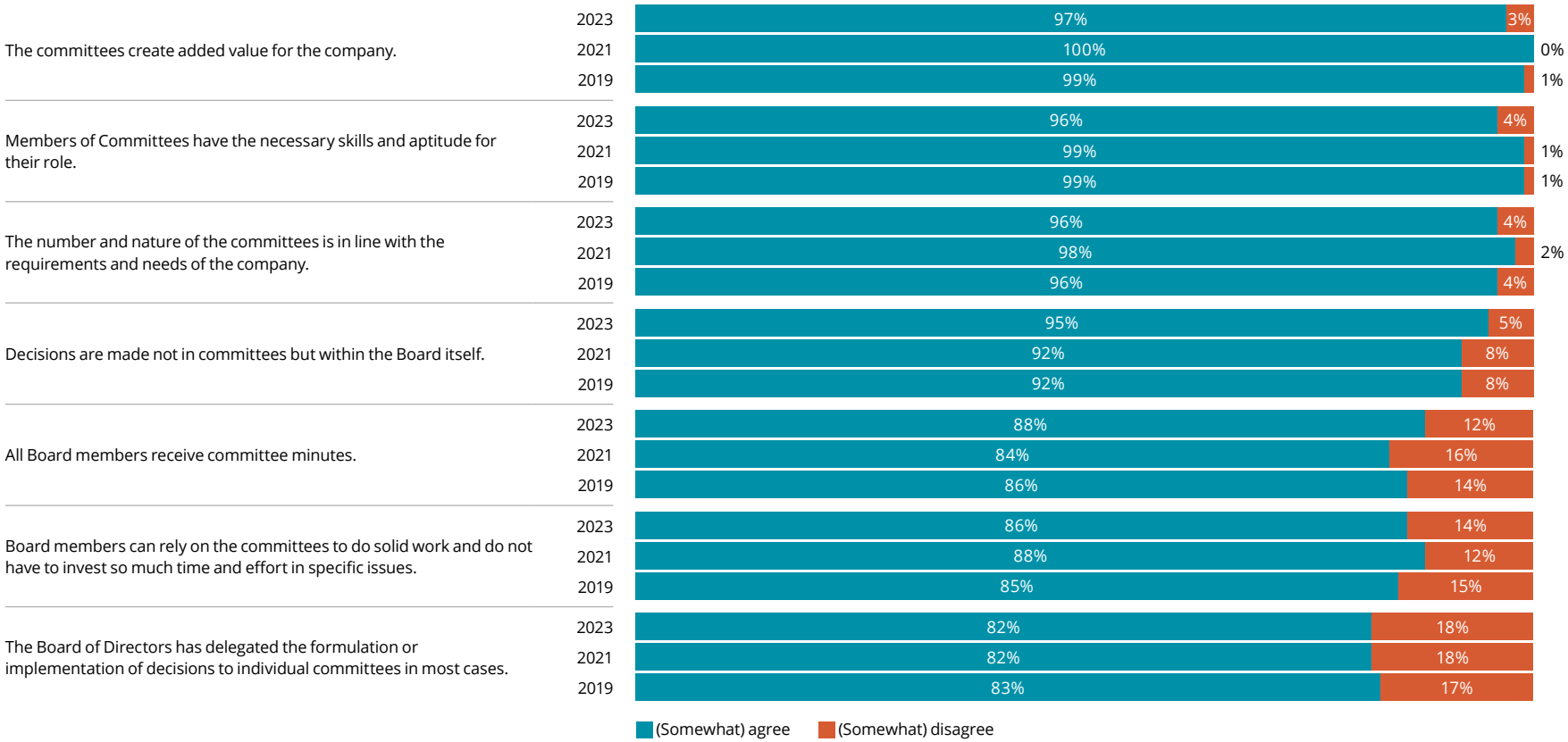


by far the most common type of committee, reflecting both the workload of such committees, the recommendations for good governance in listed companies (issued inter alia by Economiesuisse), and the requirements of regulators, including FINMA. The findings in relation to **Remuneration Committees** – set up by 44% of Boards – are similar: a Remuneration Committee is a statutory requirement for listed companies in Switzerland. Boards have a very wide variety of other committees, reflecting the differing needs of individual companies and their Boards.

Overall, the figures for the range of committees are fairly similar to the findings of previous surveys conducted two years and four years ago. The marked fall in the number of **Risk Committees** is striking: 23% of Boards now have a Risk Committee, down from 33% two years ago, when this question was last asked. This is rather surprising, as it is at odds with the reported rising importance of risk management, both in the area of cyber risk (Chart 3) and in relation to geopolitical risk (see swissVR Monitor II/2022). However, this suggests that risk management is now less likely to

Chart 12. Evaluation of committees

Question: Please indicate your agreement with the following statements about Board committees. (n=170)



be delegated to a committee and more likely to be addressed by the full Board of Directors.

As Chart 12 shows, Board members rate the work done by committees very positively. Almost all Board members surveyed (97%) believe that the committees set up within their Board **create added value for the company**. Almost the same proportion (96%) believe **members of committees have the necessary skills and aptitude for their role** and that the **number and nature of committees is in line with the requirements and needs of the company**.

Almost all Board members (95%) strongly agree or somewhat agree that **decisions are made not in committees but within the Board itself**. This reflects the statutory framework: under Swiss law, the Board has certain non-transferable duties but "may assign responsibility for preparing its resolutions or monitoring transactions to committees or individual members" (Swiss Code of Obligations 716a/2).

88% of Board members strongly agree or somewhat agree that **all members receive committee minutes**, 86% that **they can rely on the committees to do solid work**, and 82% that **they have delegated the preparation or implementation of resolutions to individual committees in most cases.** While slightly lower proportions than for other statements, these levels of agreement are still very high. Overall, Board members' rating of the work of committees is very similar to that recorded in the 2019 and 2021 surveys. swissVR Monitor therefore provides a reliable and robust barometer of the views of Boards of Directors over time.

Interviews

The Board of Directors' role in cyber resilience

Maya Bundt, Chair of the Nomination and Remuneration Committee of Valiant Bank and member of the Board of Bâloise and APG|SGA

"It's important that managing cyber risk or digital risk isn't seen as just an IT problem but is recognised as a company-wide issue to be tackled as part of the company's corporate strategy. Major strategic decisions almost always have an impact on the company's cyber footprint."

swissVR Monitor: What can you tell us about the latest trends in cyber attacks on companies?

Maya Bundt: Figures from Switzerland's National Cyber Security Centre (NCSC) show that fraud is by far the largest type of attack; that's fraud against both individuals and companies, and it's been a major issue for many years. The media, though, tend to focus on other types of attack, particularly ransomware attacks, which have become more frequent over the last few years, both with and without the theft of data.

In a ransomware attack, criminals use a kind of malware to encrypt a company's data and then demand payment of a ransom for its return. Recent ransomware attacks have also seen data being stolen and the fraudsters threatening to make it public unless the company pays the ransom. This puts companies under pressure to pay up. And there has also been a lot of coverage recently of 'distributed denial-of-service' (DDoS) attacks; these involve criminals flooding websites with requests for data, overloading systems and resulting in legitimate users being unable to access the site.

Maya Bundt is a senior leader and experienced Board member with a passion for cyber, innovation and people. In a career with the global reinsurer Swiss Re spanning almost 20 years, she had a variety of roles in IT, Strategy and Reinsurance. From 2014, she was responsible for developing its cyber insurance strategy and successfully built the Cyber and Digital Solutions function and team. She also chaired the Swiss Re Cyber Council. Maya Bundt left Swiss Re in summer 2022 to focus on her Board mandates. She supports several national and international initiatives around the digital economy and cyber risk and has published several articles on the topic. She engages with the community as the Chair of the Cyber Resilience Chapter of the Swiss Risk Association, a member of the Cybersecurity Committee of digitalswitzerland, a contributor to the Geneva Dialogue, and partner for Governance of Digital Risks at the International Center for Corporate Governance.

This happened very recently, in June, when a number of federal agencies and the Swiss rail network (SBB) were offline for a few hours following a DDoS attack.

swissVR Monitor: So what is the role of the Board of Directors in cyber resilience?

Maya Bundt: In general terms, the Board lays the foundations for sustainably managing the company in relation to its shareholders, and that includes cyber resilience. So the Board's role is to assess the opportunities and risks that digitalisation represents for the company and its business. But crucially, data is never 100% secure! So alongside traditional measures

to protect their systems, companies also need to ensure that they can detect unauthorised individuals on their website. And Boards need to be prepared for the worst-case scenario so that they can resolve a crisis as quickly as possible and without lasting damage.

This means that the Board is responsible for ensuring that risk management, organisation and budgets are in place to enable the company to protect itself and its business model against cyber risk and is equipped to survive a cyber attack.

swissVR Monitor: What measures do you advise Boards to take to ensure their cyber resilience?

Maya Bundt: It's important that managing cyber risk or digital risk isn't seen as just an IT problem but is recognised as a company-wide issue to be tackled as part of the company's corporate strategy. Major strategic decisions almost always have an impact on the company's cyber footprint, whether that's expanding into a new market, M&A activities, creating a digital ecosystem or ongoing digital transformation more generally.

The Board also needs to be aware of the areas where the company is most at risk of a cyber attack, how much of a threat these risks pose, and how they can be avoided, minimised or transferred. It's also important to assess the company's appetite for risk, so that decisions on things like cyber security or cyber insurance can be based on fact.

I always urge Boards to be aware of who in the company is responsible for data security, usually the Chief Information Security Officer (CISO). There are a number of good reasons for this. Having a CISO means there is a permanent member of staff looking after data security for the company. Having the CISO regularly in attendance at Board meetings also means a greater focus on the strategic and operational aspects of cyber security. And finally, the Board can build a relationship with this key individual, something that I think is as important as its relationship with senior risk and HR management more generally.

The Board should also be thinking about how to boost its own cyber expertise, for example by appointing members with specialist knowledge or providing existing members with ongoing training in this area. I think a certain level of cyber expertise is part of any Director's basic toolkit these days. In-depth knowledge and, in particular, an interest in this area will also help ensure that the issue doesn't get lost in the welter of things the Board has to think about and that there is always someone who is asking the relevant questions.

swissVR Monitor: How would you define appropriate reporting to the Board on the issue of cyber resilience?

Maya Bundt: Many companies have a committee – usually the Risk Committee – that is responsible for cyber risk, though some also have a Technology and Cyber Committee. Having a committee is important, because it usually has more time for discussion than the full Board, and its members can consider issues in greater depth.

Generally speaking, reporting must be relevant, clear and appropriate for the Board. It can often be useful for the CISO to keep their contribution fairly general, setting out risks and how to tackle them rather than going into technical detail. Alongside company-specific information and KPIs, it can be interesting and useful to assess the overall picture and benchmark the company with others.

swissVR Monitor: And what is your view of cyber risk insurance? Are there circumstances in which such policies can be useful?

Maya Bundt: I'd start by saying that cyber insurance is part of a company's broader cyber risk management strategy but can never replace that strategy. It sends shivers down my spine when I hear people say things like "Well, we don't need to worry about cyber security. We'll just take out insurance against cyber attacks". I don't think that's the right way to see it. I'd also argue that no insurance provider can offer a company cover if the company itself hasn't already taken certain basic measures.

Risk management includes avoiding, reducing, transferring and finally accepting risk, so taking out cyber risk insurance requires the company to understand and quantify its risk properly before deciding whether to transfer part of the residual risk to an insurance company. In other words, companies assess their appetite for risk and then transfer those aspects that their own risk mitigation measures cannot tackle. Other companies,

though, may weigh up these factors and ultimately decide against taking out cyber insurance.

Many cyber insurance policies also include services that can provide practical help in a crisis. If, for example, a company has been the victim of a ransomware attack, its insurance policy provides an emergency telephone number to ring for immediate support. For some companies, that sort of support alone is a convincing reason for taking out cyber insurance.

Cyber threats in 2023 and the measures companies should be taking

Florian Schütz, Federal Cyber Security Delegate, head of the Swiss National Cyber Security Centre (NCSC) and, from 1 January 2024, Director of Switzerland's new Federal Office for Cybersecurity

"All companies are at risk, regardless of size and sector. However, many SMEs lack the financial and human resources to take effective cyber security measures, so their expertise and infrastructure is limited or even non-existent."

Florian Schütz, the Federal Cyber Security Delegate, is responsible for implementing the national strategy for protecting Switzerland against cyber risks and coordinating all cyber activities of the federal administration. He serves as the point of contact for the cantons, business and academia on cyber issues and heads the Confederation›s centre of excellence, the National Cyber Security Centre (NCSC). Florian Schütz holds a Master›s degree in Computer Science and a Master of Advanced Studies in Security Policy and Crisis Management from ETH Zurich and has more than ten years of management experience in IT security in the private sector.

Image: Keystone-SDA / Gaëtan Ballyt.

swissVR Monitor: How has the importance to businesses of cyber resilience changed over recent years? And how do you rate the general level of cyber threat in 2023?

Florian Schütz: Over recent years, we have seen an increase in awareness of cyber security, and many companies are now aware of cyber risks. However, their response varies: some are taking cyber security very seriously and putting the necessary measures in place, while others are doing little, if anything, to protect themselves in this area.

Reports to the NCSC of cyber-related incidents are currently running at a high level – around 700 per week, on average. One reason for this is greater public awareness, but we are also seeing a slight increase in the number of cyber attacks. Attacks involving fraud are particularly frequent at the moment: fake extortion emails threatening recipients with legal action if they do not comply currently account for about one-third of all reports to the NCSC.

We've also been seeing a slight uptick in the number of ransomware attacks over recent weeks, and it is likely that the numbers will continue to rise. One reason for this is that the war in Ukraine initially slowed down ransomware attacks as some groups of hackers turned their attention away from extortion to engage with the war. However, it's highly likely they now need to get back to raising money, so we expect ransomware attacks to pick up again.

swissVR Monitor: We hear less in the media about cyber resilience in small and medium-sized enterprises (SMEs). Are SMEs less vulnerable to cyber attacks than larger companies?

Florian Schütz: All companies are at risk, regardless of size and sector. However, many SMEs lack the financial and human resources to take effective cyber security measures, so their expertise and infrastructure is limited or even non-existent.

It's also the case that cyber criminals make a cost-benefit analysis, aiming to cause as much damage as possible with the least possible effort. From that perspective, SMEs are an obvious target, because it is easier to attack their IT systems than the more complex IT infrastructure maintained by large companies. Many SMEs are also reluctant to go public about a cy-

ber attack, often because they are concerned about reputational damage. Large companies, though, are increasingly taking a different view, and a number have recently gone public, attracting media coverage.

swissVR Monitor: What steps do you advise companies to take to improve or increase their cyber resilience?

Florian Schütz: Cyber security needs to be taken seriously at the most senior level in the company! It is vital that senior management discusses the issue and that every company has a risk management strategy for cyber-related incidents in place. Management must also be aware of and document any residual risk and ensure that the finance is available to devise and implement crucial measures. Companies may feel that this involves substantial investment, but the changes don't have to be implemented in one go. It's important, though, that companies prioritise, with an absolute focus on keeping systems up to date: most successful ransomware attacks target known weaknesses for which patches are available but have not been applied.

As well as basic protection, creation of back-ups and regular updating, it is also important that companies raise their employees' awareness of cyber security. Cyber attacks often start not with the company IT infrastructure but with a single individual who works for the company. Such social engineering, as it's known, is designed to persuade staff to open an unsafe email attachment, for example, or divulge their password.

swissVR Monitor: What are the government and the NCSC doing to support companies with their cyber resilience?

Florian Schütz: The NCSC website offers lots of guidance and checklists to help companies protect themselves against cyber attacks and sets out what to do if an attack does take place. The NCSC also provides regular updates via its website and social media channels, such as LinkedIn, on new types of attack, security vulnerabilities and so on.

For its part, the Swiss government has worked with a number of partners to launch a nationwide awareness raising campaign, known by its German acronym as S-U-P-E-R. The campaign focuses on five specific aspects of cyber security: backing up data, updating programs and apps regularly, keeping antivirus and malware systems up to date, using strong passwords for log-ins and reducing vulnerability. The site provides a host of tips for companies wanting to protect themselves against cyber threats.

swissVR Monitor: Switzerland's new data protection legislation comes into force on 1 September and will take effect immediately, without a transitional period. How will the new legislation change the position for companies in relation to cyber resilience?

Florian Schütz: The new Federal Act on Data Protection will ensure that Swiss legislation is compatible with European law. This is important because it will ensure that the EU can continue to recognise Switzerland as a third country with an appropriate level of data protection; without this, additional measures would be needed to continue to transfer data across borders. The new legislation is therefore important for Switzerland as a business hub and for its competitiveness.

The measures the new legislation sets out, such as the requirement to notify data security breaches promptly to the Swiss Federal Data Protection and Information Commissioner (FDPIC), will make a major contribution to increasing cyber resilience.

The human factor in cyber resilience

Sonja Stirnimann, Chair of the Audit Committee of Glarner Kantonalbank and member of the Board of Directors of Apiax

"We've been living with 'cyber' for at least 40 years, yet for many Boards, it is uncharted territory compared to other operational risks. What I find, though, is that the fear factor and taboo tend to die away if the problems are discussed in a safe space with like-minded people at Board and/or management level."

swissVR Monitor: Many companies don't seem to see the importance of increasing their cyber resilience until they actually become the victim of a cyber attack. Do companies tend to ignore or underestimate cyber risks?

Sonja Stirnimann: I still see Boards tending to leave cyber security largely to their IT function rather than recognising it as a part of their strategic responsibility. I think that's the wrong approach. This is a really important issue, because it affects the company's – and the Board's – assets, reputation and ability to operate. Cyber resilience is one of the most important competitive advantages any company has, but many Boards still underestimate it when thinking about how to prevent serious disruption.

I wouldn't presume to judge whether they are consciously ignoring the risk or simply underestimating it, but it's human nature to sidestep an issue when we lack expertise in it. This may be unconscious but in the context of cyber resilience, it can have fatal consequences. And purely from the perspective of the Board's responsibilities, it is essential that this issue receives the proper attention.

swissVR Monitor: So what role does the human (risk) factor play in cyber resilience?

Sonja Stirnimann is an economist and auditor. She has an eMBA in Financial Services & Insurance from the University of St. Gallen and the International Institute for Management Development (IMD) Board Director Diploma. She is also a Certified Fraud Examiner (CFE). As an expert in the areas of governance, risk and audit, Sonja Stirnimann advises companies on corporate integrity and crisis management in relation to non-compliance and business and cyber crime. She has more than 30 years' experience and has worked for global companies including LafargeHolcim, UBS, Deloitte, and EY. She is also an independent Board member and Chair of the Audit Committee of several private and listed companies. Sonja Stirnimann teaches at global institutions, universities and professional associations as well as advises international companies. The English version of her book *The Executives' Risk of the Human Factor in White Collar Crime: Resistance and Resilience in the Event of Fraud, Non-Compliance and Cybercrime* is published by Springer.

Sonja Stirnimann: Resilience is not the same as resistance. Resistance tends to focus on IT security, the company's IT infrastructure and preventive measures, including monitoring. Resilience, on the other hand, focuses on how quickly the company can be up and running again for its stakeholders after a crisis.

Cyber attacks often pose a severe threat to a company's ability to operate, and in exceptional circumstances like a cyber attack, that ability depends hugely on the reactions of its Board. But not all Board members – or companies themselves – have received professional training to prepare them for such a crisis. It is one of the core responsibilities of the Board and senior management to ensure that the company can continue to operate, so it can also be a good idea to rehearse for such a crisis, with lessons learned fed back into processes to improve them. Cyber resilience is therefore all about an organisation's ability to recognise cyber attacks, respond to

them and recover from them while maintaining its ongoing operations. The difference between resistance and resilience can be illustrated by the life cycle of cyber crime incidents.

Resistance primarily means preventing or stopping attacks that could cause damage to the company, such as security measures including firewalls, intrusion detection systems and cyber security rules. But while resistance is important, it cannot completely prevent a cyber attack. And these days we have to assume that we are all under attack all the time, so resistance covers preventive measures that mitigate or minimise that risk.

Resilience on the other hand is about an organisation's ability to react rapidly to an attack or to disruption to its systems, to recover and to continue operating. This includes detecting attacks, responding rapidly and restoring systems so that it can continue to do business. By contrast with resistance, which relies on preventing attacks, resilience is about limiting the impact of and damage caused by attacks. And the ability to continue operating is the central objective.

swissVR Monitor: Companies tend not to discuss cyber attacks publicly. How can we persuade them to stop seeing the issue as taboo and be more transparent?

Sonja Stirnimann: We've been living with 'cyber' for at least 40 years, yet for many Boards, it is uncharted territory compared to other operational risks. What I find, though, is that the fear factor and taboo tend to die away if the problems are discussed in a safe space with like-minded people at Board and/or management level. And this means having not just that safe space but also the willingness to share experiences and to learn. I've found that Boards appreciate this openness and can learn a huge amount from each other. And it can help if such discussions take place across different sectors.

swissVR Monitor: So who within a company is responsible for cyber resilience? Where is that responsibility located?

Sonja Stirnimann: Many companies still don't see this as an issue requiring action or have only recently recognised its importance, so I think cyber resilience – and the upstream cyber resistance – need to be recognised and tackled as an operational risk at Board and management level. Depending on the company's and Board's level of maturity, they may also need to go on a learning curve, which can be steep. The Board and management are role models, in cyber resilience as in many other areas.

swissVR Monitor: You advise companies to start by raising awareness. What does that mean in the context of cyber resilience?

Sonja Stirnimann: Awareness raising starts with active discussion, information and training – at all hierarchical levels. We learn from analysing and discussing case studies and using them to identify our own risks, which requires openness and recognition that any of us could be affected, sooner or later. These discussions often take place only once there has been an attack, rather than preventively before an attack can happen. But my experience is that companies that think strategically before an attack with a view to enhancing and securing their competitive advantage do better in terms of protecting their assets.

Contacts and authors

swissVR

Cornelia Ritz Bossicard
President swissVR
+41 41 757 67 11
cornelia.ritz@swissvr.ch

Dr. Brigitte Maranghino-Singer
CEO swissVR
+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
Research Manager
+41 58 279 64 35
dlaude@deloitte.ch

Hochschule Luzern

Dr. Mirjam Durrer
Lecturer at the Institute of Financial Services Zug (IFZ), Lucerne University of Applied Sciences and Arts
+41 41 228 41 73
mirjam.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, the association contributes to professionalising Board member activities in Switzerland. swissVR enables its members to share their experience with Board members from all sectors of the Swiss economy. It also offers its more than 1,200 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 / www.hslu.ch/cas-vr / www.hslu.ch/ifz

Deloitte AG is an affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee. DTTL and its member companies are legally independent and stand-alone companies. DTTL and Deloitte NSE LLP themselves provide no services to clients. A detailed description of their legal structures can be found at www.deloitte.com/ch/about. Deloitte AG is a supervised audit firm approved by the Federal Audit Authorities (RAB) and FINMA, the Federal Financial Markets Supervisory Authority.

The Hochschule Luzern is the University of Applied Sciences and Arts of the six Central Swiss cantons. It is the largest educational institution in Central Switzerland with around 8,300 students attending courses and 5,200 in continuing education programmes. It is currently engaged in 400 research projects and has a staff of around 2,000. The Institute of Financial Services Zug (IFZ) of the Hochschule Luzern – Wirtschaft focuses on governance, risk and compliance and offers continuing education for Board members in these areas, including the Certificate of Advanced studies for members of Boards of Directors (CAS Verwaltungsrat). Detailed information can be found at www.hslu.ch/ifz-verwaltungsrat / www.hslu.ch/cas-vr / www.hslu.ch/ifz

swissVR®

Deloitte.

Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern