eraneos

Research paper 2022/2023

Cyber readiness. Ensuring corporate maturity and the controllability of digitalization

Study results 2022/2023

Preface

The broad-based survey provides in-depth insights into the cyber readiness of of the administrations and companies of a country in Europe. The survey focused on the orientation and the technical requirements for strengthening cyber resilience as well as the maturity of the organizational structures already established for this purpose.

The study comprises four main topics: The first part deals with the current cyber readiness of the study participants. The second part is dedicated to cyber resilience and examines the resilience of companies against incidents in the cyber environment, while the third and fourth parts focus on cyber governance and the challenges along the way to increasing cyber maturity. The data was collected on the basis of a structured questionnaire. We also looked at the subject areas addressed in more depth by interviewing selected participants.

> "Despite the legal requirements of the EU and the revised information security and data protection laws, the board of directors and the management do not yet assume leadership responsibility for information security in many places."

Adrian Marti, Partner, Eraneos Switzerland AG

The authors

Adrian Marti
Partner
Zurich

Ernst Zeller
Managing Consultant
Bern

Contents

Ensuring corporate maturity and the controllability of digitalization

→

The progressive digitizing of business processes requires harmonized and comprehensively coordinated principles that make it possible to define information and data protection at any time that is suitable for the current situation and can be effectively controlled at all organizational levels.

This requires corporate maturity orchestrated across the organization and coordinated at all hierarchy levels. Cyber readiness is based on an intelligent organization form that identifies risks both preventively and effectively and reduces these through efficient measures coordinated with stakeholders in the ecosystem. Companies and administrations organized in this manner constantly analyze the threat situation and the impact of their measures, improving these in a continuous learning process. They employ a consistent measurement system to assess the progress achieved internally and through external audits. Information security and data protection together form an integrated component of the digitalization of their processes.

The study participants

→

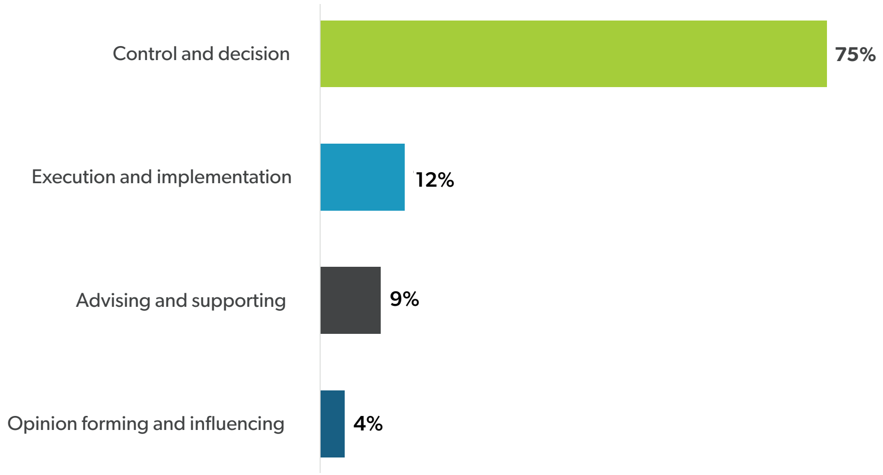


Figure 1: Functional distribution of the study participants

The results explained below are based on the evaluation of the responses of the companies and public administrations surveyed in that country. It is satisfying to note that with a share of 75%, three-quarters of the answers came from those responsible for security management.

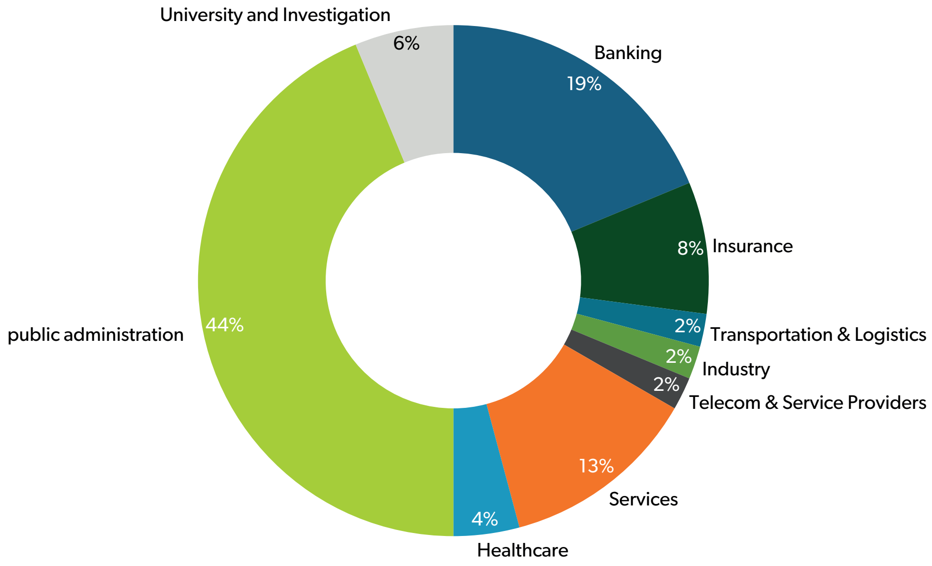


Figure 2: Industry-related distribution of the study participants

A total of 54 decision makers took part in the survey. Important players on the market were surveyed, including not only large and medium-sized companies but also the public sector, which accounted for 42% of the study participants. 17% of the companies surveyed come from the banking sector, followed by service providers with 11% and the insurance industry with 10%.

> “The National Cyber Security Center (NCSC) of the federal government pursues the cyber readiness approach as an opportunity. The public has been made fully aware of the topic of security and can thus increase trust. In this sense, the topic is proactively promoted.”

Interview partner
federal administration

Chapter

Results and findings of the study

Topic 1: Current status of cyber readiness

→

Today, every organization is vulnerable to cyber security risks and should take proactive measures to mitigate threats before they become successful attacks.

Sound cyber readiness management includes tailored, proactive preventive measures that effectively protect a company's reputation, operations and financial performance.

To what extent is cyber security considered a critical success factor?

Although the management levels now largely considered cyber security indispensable, there is still some uncertainty as to how to counteract the increasing cyber threats and which investments provide the quickest and most effective results. Specifically, in this year's study, 78% of those surveyed considered cyber security to be a critical success factor. This corresponds to an increase of 8,43% compared to the survey in 2020.

The development and implementation of effective, company-wide cyber readiness continues to be a major challenge for the majority of those surveyed. In many places, an established information security management system is still not anchored in the organization and implemented at all levels.

Who are the owners of the cyber risks?

Two-thirds of the respondents stated that the board of directors (19%) or the senior management (47%) are the owners of cyber risks. In contrast, more than a quarter of the respondents still assign management of cyber risks to IT or individual departments.

As cyber risks are now classified as the greatest threat to companies and represent a significant proportion of business risks, these should no longer be delegated exclusively to IT. On the contrary, they should absolutely be on the agenda of corporate management. Our survey has shown that many companies are still a long way from achieving this, as cyber readiness is still not viewed uniformly but is understood as a purely technical challenge.

Where is the CISO (Chief Information Security Officer) embedded in organizational terms?

In order to ensure that the CISO is able to consider all aspects of the company when performing their duties and that they have the necessary assertiveness to do so, it is important that they can report to senior management without facing any conflicts of interest. Embedding the CISO in IT can create conflicts of interest with the CIO or limit the focus on system security.

As part of our study, only 19% of those surveyed stated that the CISO is organizationally embedded in management. For more than a third (38%) of the study participants, the CISO is located in IT. This can be observed in the public sector in particular.

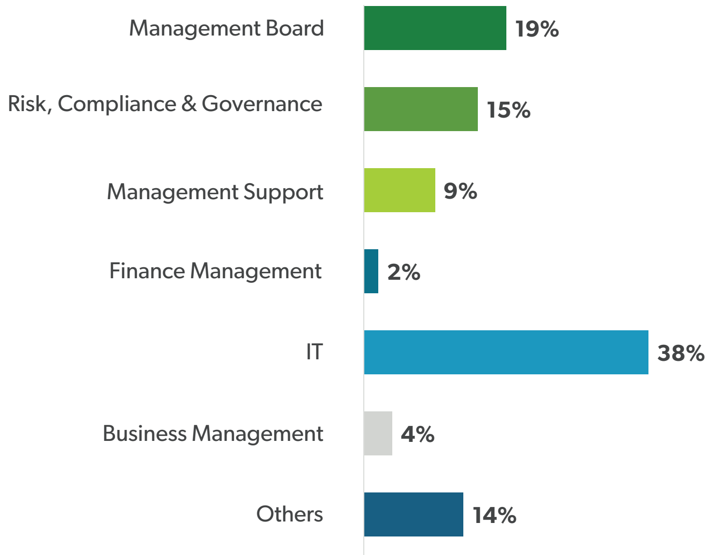


Figure 3: Embedding of the CISO in the organization

What are the most relevant cyber risks and threats?

From a technical point of view, the distribution of the relevance of cyber threats has changed little since the last survey in 2020. Ransomware remains the most cited cyber risk. Successful attacks can damage the company image, cause financial losses and may even have legal and regulatory consequences.

Be it intentional or accidental, insider threats now account for 43% of all security breaches according to the 2022 WEF Global Risk Report. To better account for such risks, some companies are responding with a greater segmentation of digital systems. However, this can negatively impact employee efficiency as it makes access to data and information less seamless.

There is an acute need for action with regard to the fulfillment of legal regulations, including data protection. In addition, compliance is now a must for every company in order to effectively contain the risk of legal proceedings or fines.

> “Our national logistics company evaluates all corporate risks based on standardized measurement methods. In addition, to promote uniformly controllable cyber readiness, there is an overall risk map that makes it possible to strategically address the defined focal points.”

Interview partner
national logistics company

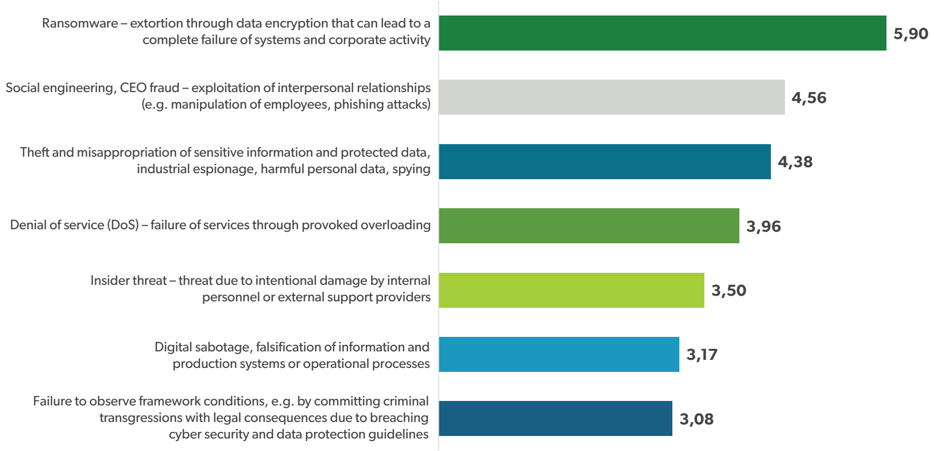


Figure 4: Most relevant cyber risks and threats

What are the top cyber security topics?

Overall, in this year’s study, 74% of those surveyed considered cloud security to be the number one security topic. That is an astounding 16% more than the survey from two years ago. For industries and financial service providers in particular, ensuring secure cloud applications is the most frequently mentioned topic for ensuring information security. At 66% (compared to 46% in 2020), the other top cyber security issues include preventing the outflow of sensitive information and data worthy of protection as well as organizational cyber maturity, i.e. the efficient and effective control of information security within the organization and the associated ecosystem.

Amazing developments can also be seen in the safe use of mobile devices. This was still a top issue for 63% of those surveyed in 2020, while only 30% of the study participants rated the issue as a high priority this year. IoT security, which was of great importance for 45% of those surveyed in 2020, has also dropped significantly, with the security of digitally networked products now only being a top issue for 14% of participants in the current study.

As the cyber resilience study from two years ago already revealed, mobile end devices primarily play a central role in healthcare, mobility and logistics. Cloud services, security measures, attack detection and data protection, on the other hand, are of great importance, especially in highly exposed industries and for operators of critical infrastructures such as banks and service companies, while IoT security is primarily important for industry and energy suppliers.

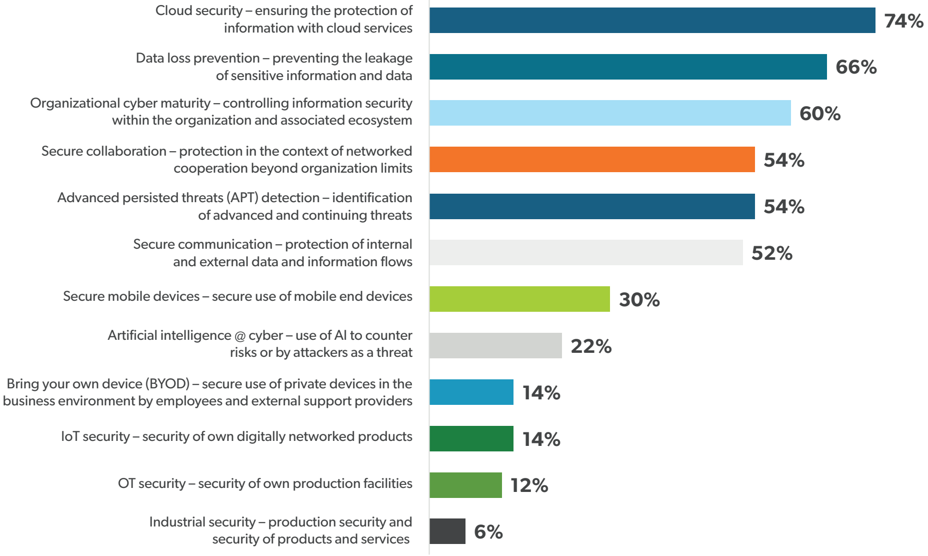


Figure 5: Top cyber security topics

Topic 2: Cyber resilience

ISO 22316 defines resilience as the ability to adapt to a changing environment. More resilient organizations can anticipate and react to risks and opportunities due to sudden or gradual changes in an internal and external context.

What are the greatest challenges faced when implementing a resilience strategy?

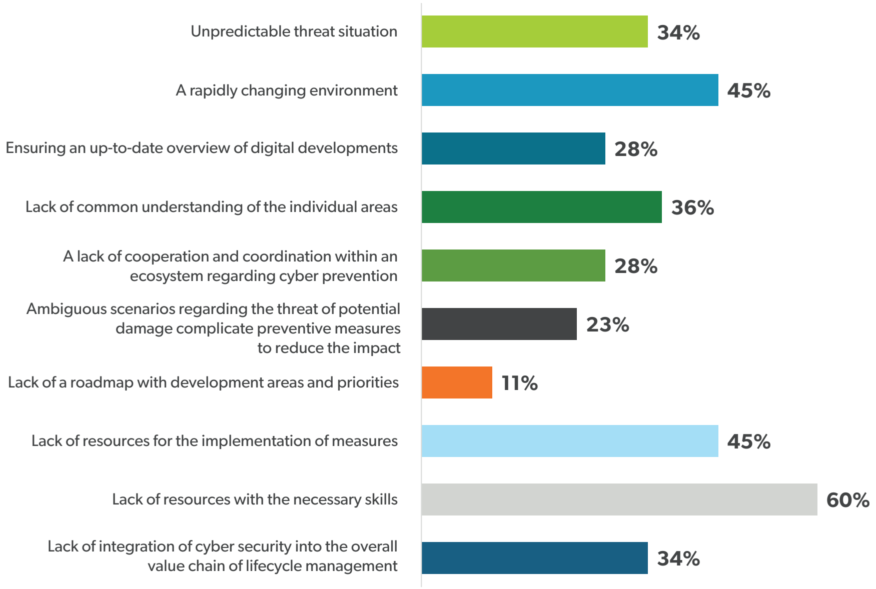


Figure 6: Challenges in implementing a resilience strategy

The ability to react to unpredictable threats and risks in an environment that is constantly changing is one of the greatest challenges for the study participants. In addition to a lack of effective cyber governance, there is also a lack resources with the necessary skills, as well as resources for implementing the defined measures. In practice, there are often major discrepancies between the requirements of the departments and the available resources with the appropriate know-how and the necessary experience. The budget, on the other hand, is usually the lesser problem.

The prevailing shortage of qualified IT and cyber security professionals who can take on leadership roles in cyberspace, testing and securing systems, and training people in digital hygiene is severe. This has consequences: buying a tool is relatively easy. Using it properly, however, is less so. This requires the right resources to carry out analyses and evaluations.

Overall, little has changed compared to the Cyber Resilience Study 2020.

How important is cyber resilience to the organizations surveyed?

A little more than half (54%) of those surveyed still classify cyber resilience as mission critical to ensure that the entire organization is not affected in the event of an attack so the mission and business operations can continue. 23% of the study participants also stated that cyber resilience must be ensured across the entire ecosystem. In practice, however, only 2% of those surveyed actually implement such practices. It was also surprising that only 10% stated that cyber resilience is part of the digitalization strategy and is firmly anchored in the organization.

Even more surprising was the fact that 7% of those surveyed stated that cyber resilience is a negligible requirement and that the topic plays a subordinate role. This is especially true considering that in the survey two years ago, all the participants stated that they were focused on cyber resilience.

The need for action is particularly high for system-critical authorities and companies such as utilities and hospitals in order to ensure a coordinated organizational and technical cyber readiness in every situation so they are fully prepared to defend against cyber attacks.

Are incidents monitored in your own organization to enable the derivation and implementation of measures to enhance cyber resilience?

62% of those surveyed stated that measures to increase cyber resilience had already been defined and implemented as a result of specific events, while just over half analyzed such incidents and discussed them with management in order to derive organizational and technical measures for the future. It is astonishing that around 15% of the study participants still do not practice cyber resilience management and see no need for action in this regard.

Basically, when evaluating the study results, it is apparent that industries and authorities learn more quickly from incidents in an environment with strict legal requirements and controls by external auditors. This gives organizations a clear lead over industries that do not have an actual and verified information security management system (ISMS).

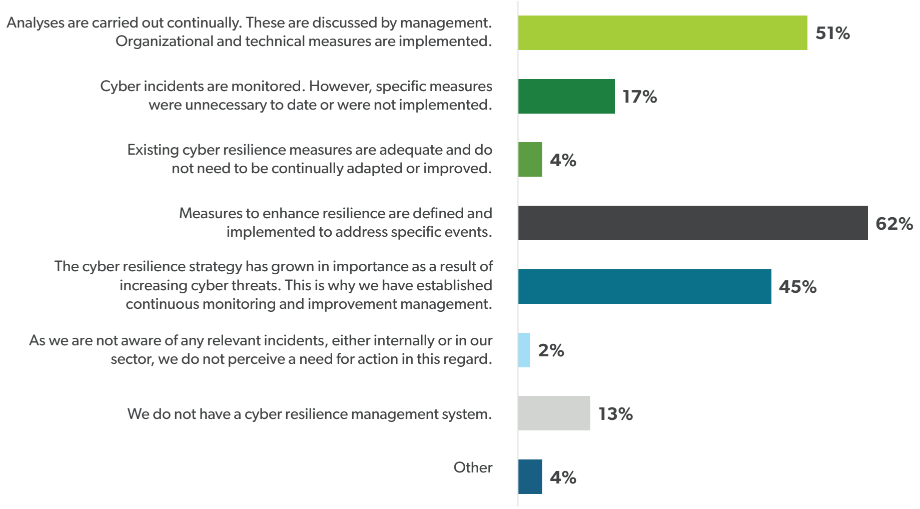


Figure 7: Measures to increase cyber resilience

As the occurrence of a cyber incident can hardly be prevented any more, the ability to recover rapidly is a critical success factor. Are there continuity and recovery plans to maintain critical business processes in the event of an incident?

Cyber incidents can disrupt, interrupt or completely paralyze operations. This can lead to a significant drop in sales or, in extreme cases, to the complete closure of a company. With a business continuity plan (BCP), the likelihood of the organization quickly recovering from a cyber incident increases exponentially. As the occurrence of a cyber event becomes less and less preventable, the ability to recover quickly is increasingly becoming a critical success factor. A plan to ensure business continuity should therefore be part of the basic framework for sensible risk management.

> "The critical processes must be defined. BCM plays a decisive role here and, dependding on the situation, it must be possible to reduce it to system-relevant missions. It is also important to consider BCM measures as an integral part of all departments and to define them uniformly."

Interview partner
regional administration

According to the study, 28% of those surveyed stated that appropriate continuity and recovery plans have been defined and are regularly reviewed and trained. 89% of the organizations surveyed have defined continuity requirements for critical business processes. Nevertheless, 11% (compared to 12% in 2020) still do not regularly review these requirements. Furthermore, 22% (compared to 27% in 2020) of those surveyed said that they act ad hoc in the event of an incident.

Most surprising about this question was that an astounding 11% of those surveyed did not know whether or not appropriate preparatory measures had been taken in their organization. In 2020, only 3% of the survey participants said they were unaware of any continuity and recovery plans.

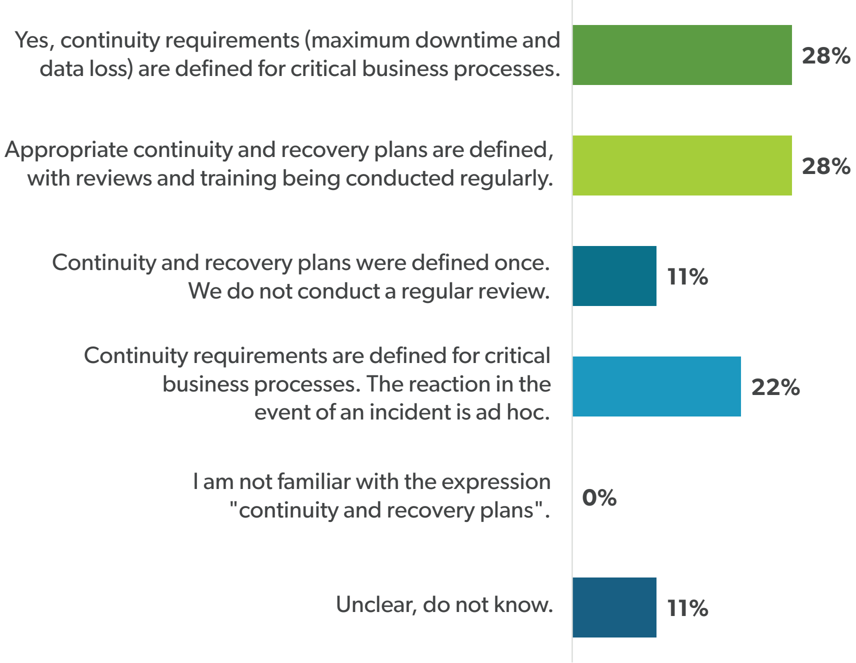


Figure 8: Business continuity measures

Assumption: You are attacked. How does your company react?

For 25% of those surveyed, the management is informed and oversees the measures taken together with those responsible internally and the service providers. 11% have defined measures to contain possible damage caused by an incident and have recorded them in scenarios that can be implemented on the basis of the developed emergency plan. In contrast, only 2% of the study participants have a clear communication concept for the entire ecosystem that is implemented by management, while 13% currently have no scenarios for a surprise attack.

Basically, this shows that comprehensive control of cyber security in ecosystems and in larger companies has not (yet) been implemented in many places.

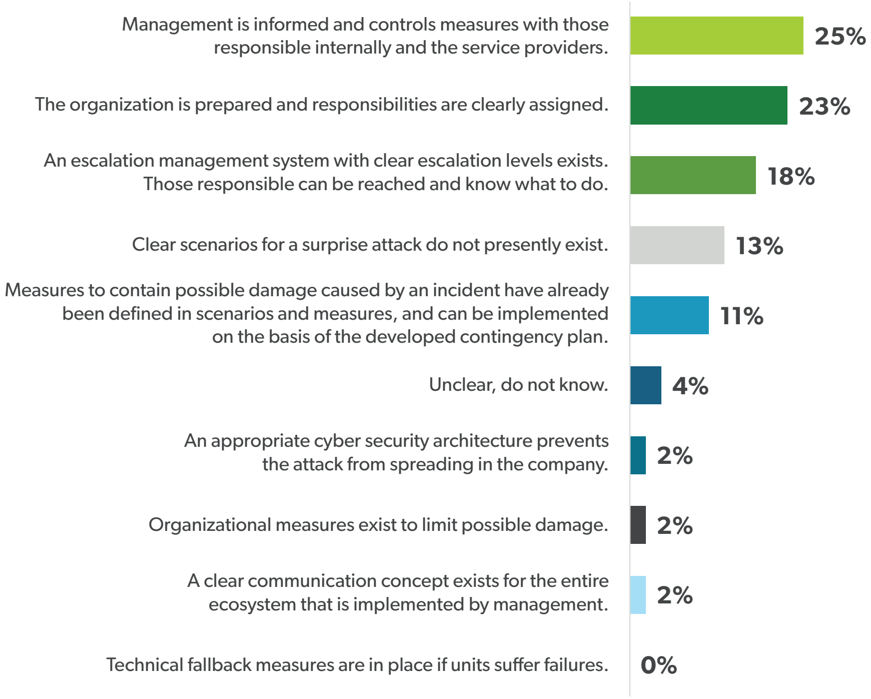


Figure 9: Readiness to react in an emergency

Topic 3: Cyber governance

→

Effective cyber security governance focuses on risk management and security awareness to reduce the scope of the risk landscape. It helps the organization to define its risk appetite and monitor risk mitigation activities. A strong governance program also establishes an accountability framework and establishes who is responsible for making decisions to ensure risk mitigation.

What percentage of IT spending for digitalization do you use for cyber security?

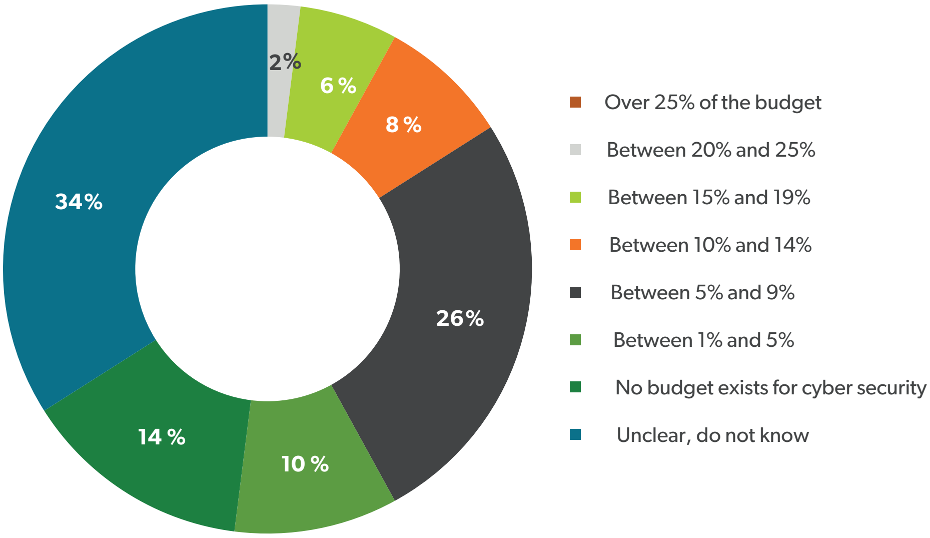


Figure 10: Available budget for cyber security

An astounding 34% of the study participants did not know the amount budgeted for cyber security, while 14% said no such budget exists.

A little over a quarter of the companies surveyed use 5% to 9% percent of IT spending on cyber security. Only 2% use between 20% and 25% of their IT budget for cyber security. More than 25% of the budget is not used for cyber security in any of the companies or administrations surveyed.

Who controls cyber governance in the company?

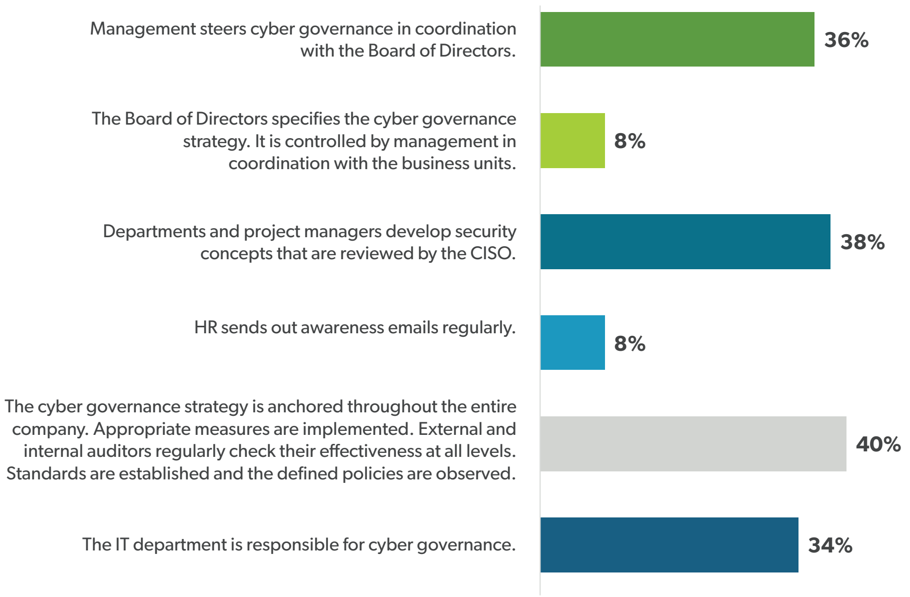


Figure 11: Responsibility for controlling cyber governance

Successful cyber governance requires both a strong drive from the top and a company-wide perspective. It is therefore correspondingly important that the decision makers, i.e. the Chief Information Security Officer (CISO), the CEO and the board of directors, set the tone when it comes to decisions about which measures are to be taken and how they are to be implemented in the organization.

However, our study shows that overall company-wide control of cyber governance by the board of directors and the executive board is a common challenge that many organizations have not yet mastered. It is particularly surprising that more than a third of those surveyed still delegated cyber governance to the IT department.

> **"The Executive Board proposes the strategy for managing cyber risks to the Board of Directors and is responsible for how this is implemented, while the Board of Directors determines which measures are to be implemented."**

Interview partner
CISO insurance group

How are measures to reduce cyber risks in the company controlled?

The belief that cyber readiness can be controlled using forms and documents with the help of security concepts is widespread. In addition, there is all too often a failure to review the effects of the measures implemented, even in a system-critical environment.

It is particularly surprising that cyber governance is not yet a business issue for 20% of those surveyed and that the concrete management of cyber risks has not yet been established. Banks and insurance companies are leading the way in implementing appropriate measures. As these are sectors that are very heavily regulated by the government, this result is not surprising.

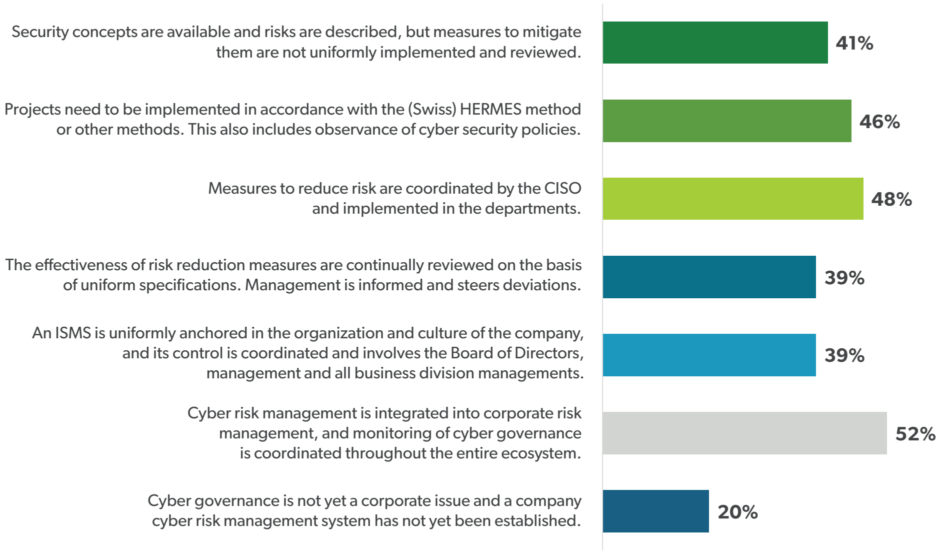


Figure 12: Control of measures to mitigate cyber risks

In the cyber environment, the question of when I will be targeted is increasing over time, displacing the question of whether I will be affected. How important is cyber security to the participants in the study?

Cyber security is an issue that management has been intensively involved with for some time now. However, the pressure to act for effective cyber readiness in one's own organization is still low. This is particularly evident from the fact that cyber security has only recently been on the agenda of 18% of those surveyed and is still not a top issue.

The fact that more than a third (38%) of the study participants deal with the topic and coordinate the needs of IT users and the specifications of the security forums also confirms that cyber security is still not a top priority in many places.

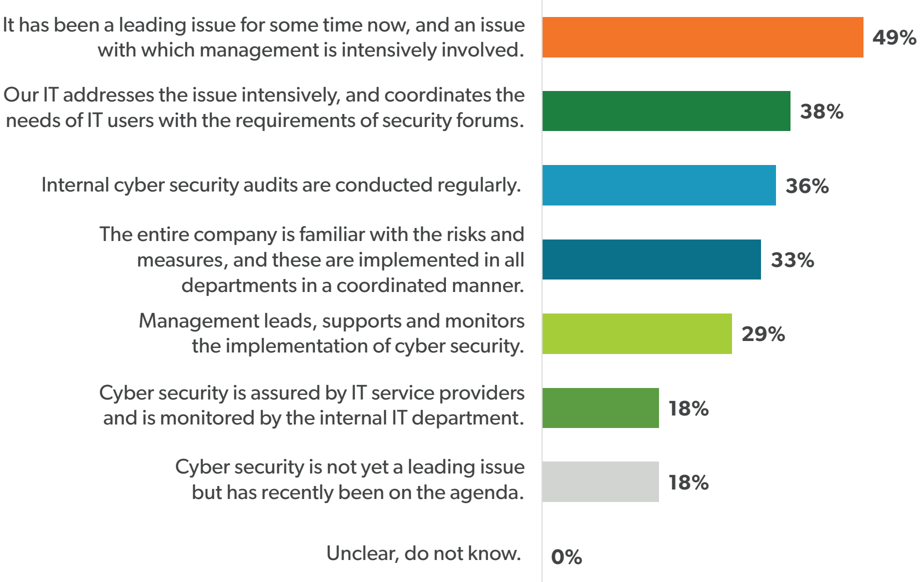


Figure 13: Importance of cyber security in the organization

Topic 4: Cyber maturity

The degree of cyber maturity in an organization depends significantly on the corporate skills and prerequisites designated and measured as organizational maturity. The following questions will help us to understand better the challenges companies are faced with when increasing their cyber maturity.

Cyber maturity differentiates between the following maturity levels with regard to the organization:

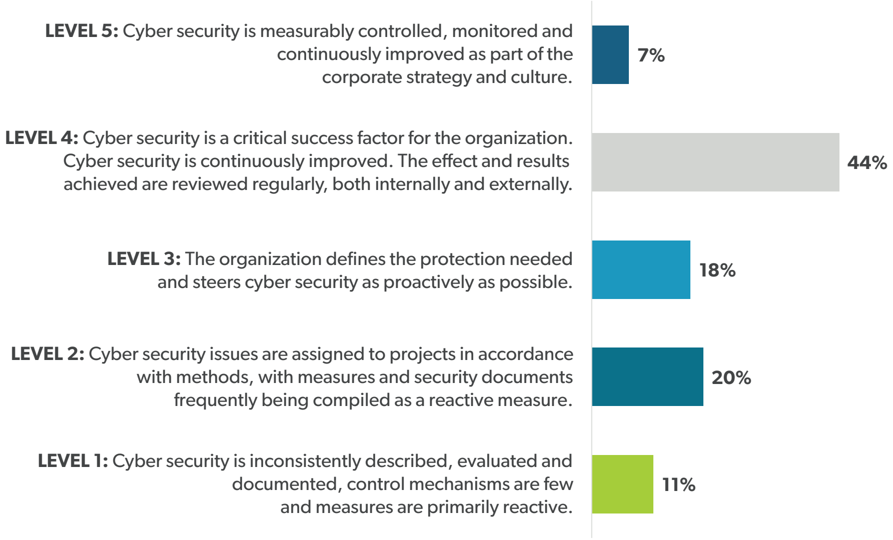


Figure 14: The five levels of cyber maturity

A low maturity level describes an organizational state in which information security risks are known, but in most cases no measures to reduce the risks are defined or they are not implemented and controlled. The highest level of maturity is achieved when measures are implemented in the organization in a measurable and assigned manner, they are continuously lived and controlled, and the organization is constantly learning and improving.

So-called “intelligent companies” are based on a maturity level 5. They are often more resilient and agile in the face of change and threats. At the same time, they are usually more competitive and more successful in their market and can fulfill their mission more agilely and better than comparable organizations.

At 31%, almost half of the respondents in our study rated their level of cyber maturity between 1 and 2. Especially in system-critical companies and organizations, a maturity level at these levels is a major cluster risk for the economy, the population and the country concerned.

What, in your opinion, are the greatest obstacles that need to be cleared to successfully promote cyber security in your organization?

Cyber readiness is based on an intelligent organization form that identifies risks both preventively and effectively and reduces these through efficient measures coordinated with stakeholders in the ecosystem. The ongoing further development and optimization of the defined measures as well as a clear allocation of responsibilities and a binding cross-departmental cyber security framework are just as important.

At the same time, effective cyber readiness as a continuous process requires that both your own digital ecosystem and the ecosystems of the third parties involved are continuously monitored. This is the only way to ensure an accurate assessment of the digital resilience of your own organization and an effective defense against cyber risks in the long term.

Due to the serious lack of resources and numerous other hurdles that still have to be overcome, a harmonized and effectively practiced and proven cyber readiness is still a long way off in many organizations. The hope that it will only affects others is still dominant.

> "Our biggest challenge at the moment is the increasing dimension of cyber threats, which have to be managed with the few resources available."

Interview partner
public utility company

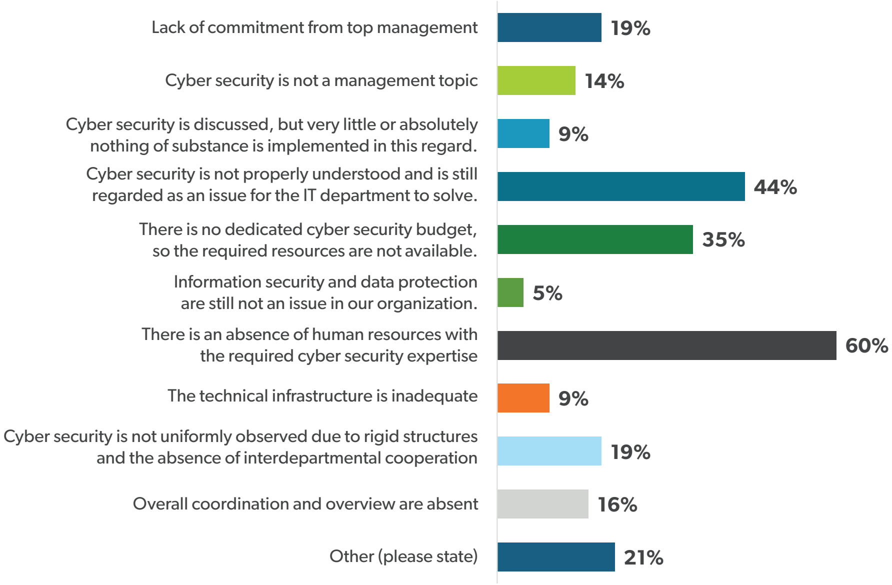
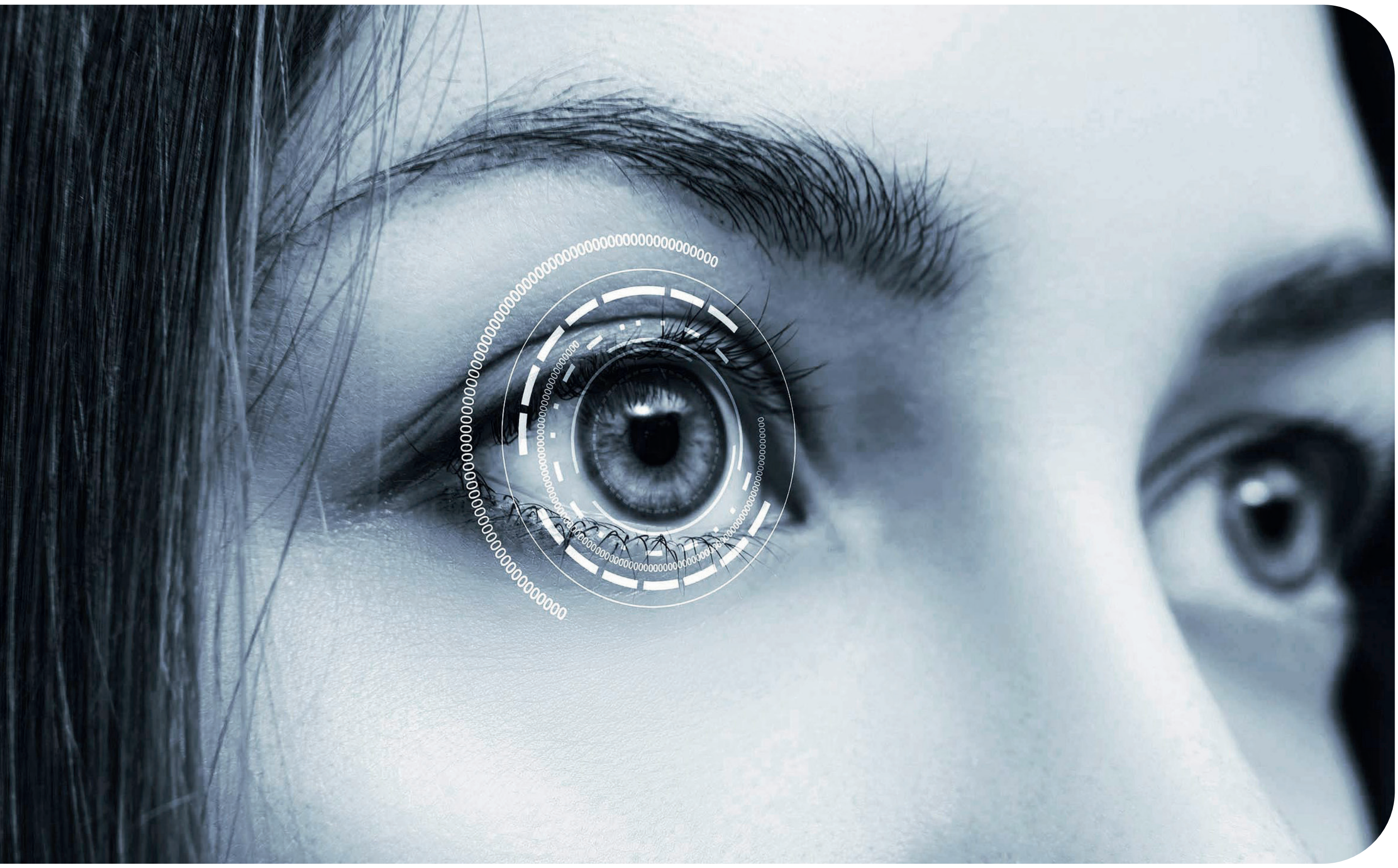


Figure 15: The biggest hurdles on the way to more cyber readiness



eraneos

Experienced in a wide range of industries

About Eraneos Switzerland AG
Eraneos Switzerland AG (formerly AWK Group AG) is an international management & technology consulting firm. It specializes in supporting its clients with the development of digital business models and complex transformation projects which enable clients to fully exploit the potential of digitalization.
As a member of the internationally networked Eraneos Group, which stretches from Switzerland, to Luxembourg, Germany, Austria, The Netherlands, China, Singapore, and the USA, the firm ensures their clients retain access to the more than 1000 highly qualified experts, along with their extensive knowledge.
The unique combination of competencies in the areas of Digital Business & Innovation, Organizational Excellence & Transformation, Data & AI, Cyber Security & Privacy, Sourcing & IT Advisory, and Technology & Platforms is applied to all industries and sectors, enabling the firm to provide comprehensive support to a full portfolio of clients.
Local Swiss offices in Zurich, Basel, Bern and Lausanne employ over 550 professionals.
Eraneos Switzerland AG is a repeated recipient of the "Great Place to Work" award.

Contact us >

Visit our website >

Join our Company >

eraneos.ch