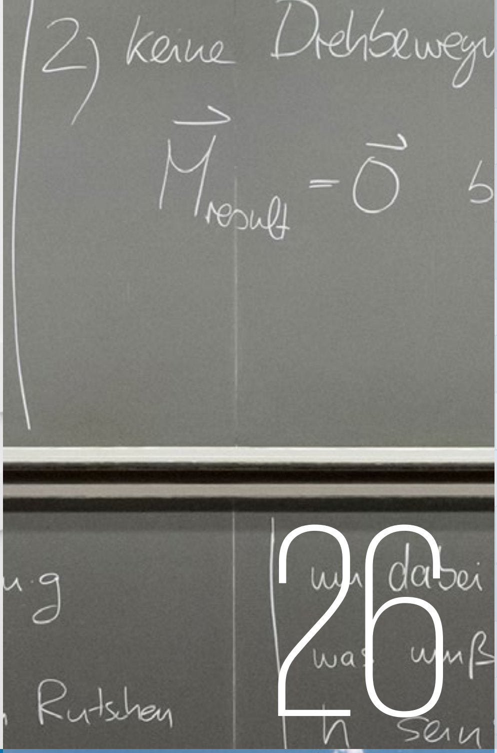
Clarity on Cyber Security

Driving growth with confidence

May 2018

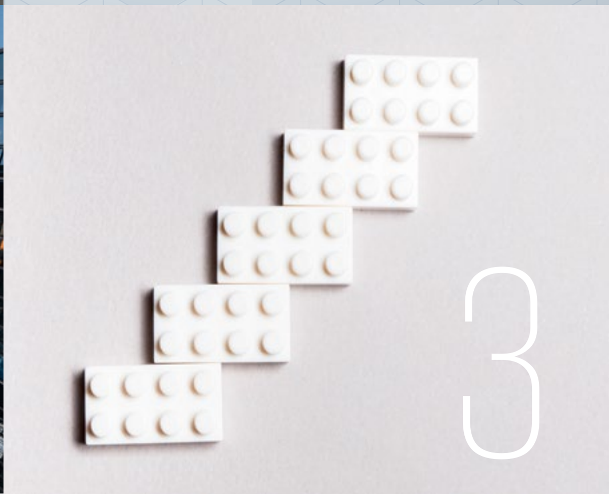
22

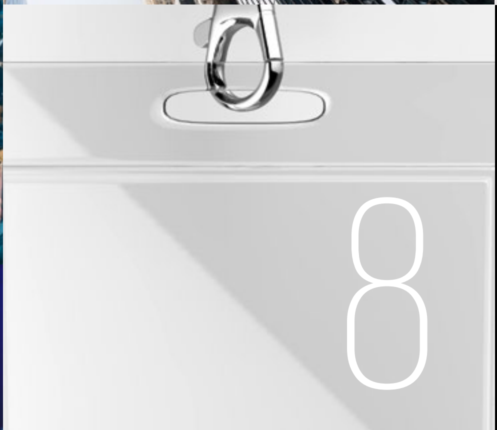

2) keine Drehbewegu
$\vec{M}_{result} = \vec{O}$
ng
Rutschen
um dabei
was muß
n sein
26

12

14

18

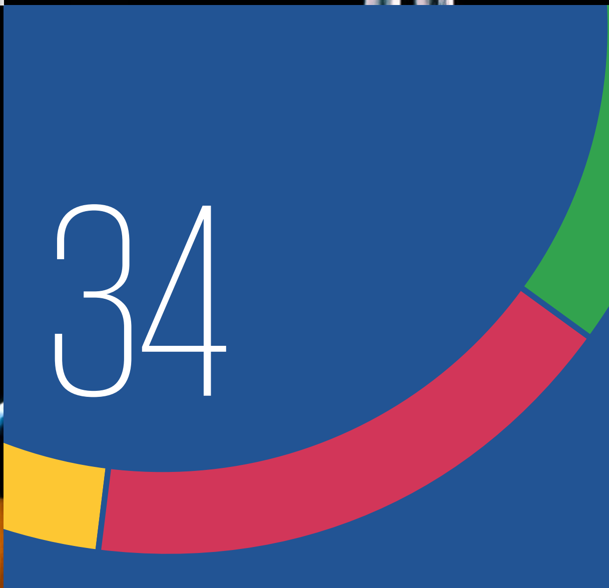

3


8

10

30

6


34

4

CONTENT

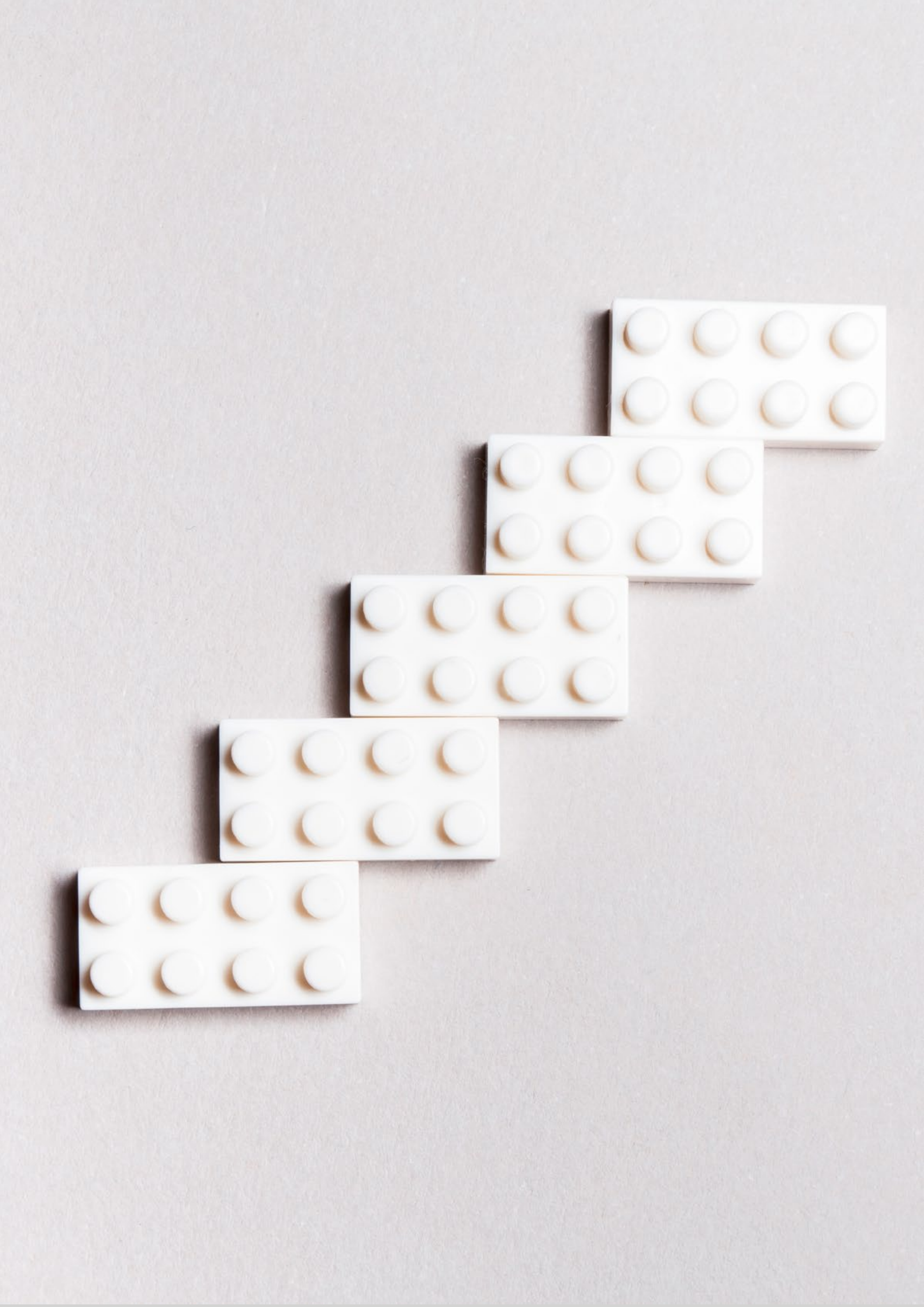
Clarity on Cyber Security

EDITORIAL

INTERVIEWS

SURVEY RESULTS

ABOUT KPMG



EDITORIAL

Driving growth with confidence

Matthias Bossardt
Partner, Head of Cyber Security

Switzerland has a well-earned reputation for trust. The success of some of its key industries such as banking, food, healthcare and life sciences is built on it. But as digitalization gathers pace across multiple aspects of our lives, commerce has become increasingly borderless and some businesses never meet or speak to customers in person. In such an environment, how can companies build and maintain trust? A large part of the answer lies in cyber security.

Many people view cyber security through the lens of threats or risks. Certainly, there are significant risks. But there are also huge opportunities. By approaching cyber security correctly, you can build your business's resilience, creating confidence among stakeholders that data and transactions are secure. This confidence supports trust between company and customer, enhancing competitive advantage and generating additional business. The opposite is also true, of course. A lack of faith in the resilience of a company's systems or products can result in customers or investors going elsewhere. Put simply, resilience and trust are prerequisites for sustainable growth in this digital age.

We believe that not enough Swiss businesses are proactively addressing these issues. Our belief is confirmed by respondents to our survey of 60 Swiss businesses. Organizations may acknowledge the cyber security challenges they face, but too few are taking concrete action. This stark contradiction lies at the heart of many Swiss organizations' cyber strategies.

If cyber security is not already an integral part of your growth agenda, it should be. Because it is by leveraging data and deploying new technologies that you will keep up with your competitors, and by ensuring resilience against cyber threats that you will gain the trust – or indeed even meet the basic expectations – of your customers.

We hope you find this publication thought provoking as you reflect on how your organization is seizing the opportunities presented by cyber security.

M. B

Matthias Bossardt

A study by KPMG Switzerland
with the support of economiesuisse and
the Swiss Academy of Engineering Sciences SATW

economiesuisse

satw it's all about technology

Failing to prepare means preparing to fail

Cyber attacks have become business as usual, and organizations cannot be 100% secure. It is essential to not only invest in prevention and defense, but prepare for adequate follow-up to incidents. Your goal should be the highest level of cyber resilience.

You might be secure, but is your partner?

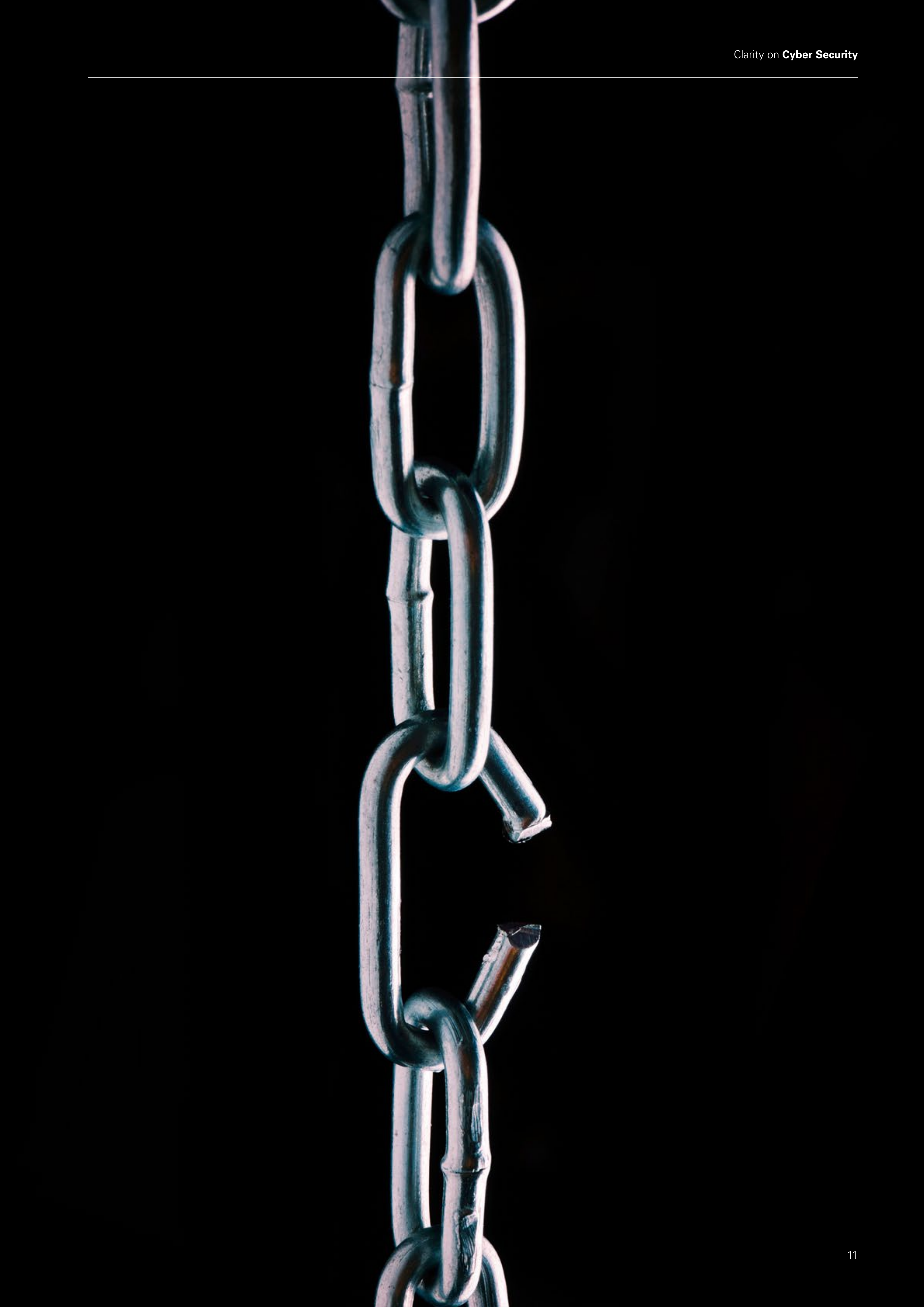
As cyber security recognizes no boundaries in our hyper-connected environment, it is vital to understand the cyber risk positions of parties along your value chain. Cyber due diligence is key to identifying risks when you make an investment. And joint efforts are needed to ensure the ongoing cyber security of you and your business partners.

Nobody knows you're a dog

If you are not entirely certain who you are dealing with in your digital interactions, you are not alone. At the beginning of the online age, one used to say 'nobody knows you're a dog on the internet'. Thirty years later, the quest to have a digital identity is not yet complete but is entering a new phase.

No silver bullet among emerging technologies

New developments such as blockchain may be fascinating concepts for keeping transactions traceable. But serious issues persist such as the concentration of nodes in the network, limited user friendliness of wallets, and vulnerabilities that will occur when quantum computing matures.



Key findings

Genuine threats, real damage

42% of respondents who suffered successful cyber attacks incurred financial losses as a result, 42% experienced disruption of business processes, 33% suffered from disclosure of confidential internal information, and 25% needed to deal with reputational damage.

75% of successful cyber attacks in financial services resulted in financial losses, compared to 25% in non-financial services.

50% of successful cyber attacks in non-financial services resulted in the disruption of business processes, compared to 25% in financial services.

Inadequate scenario plans increase exposure

82% of cyber response plans do not cover incidents such as attacks against suppliers or business partners (60% in financial services and 93% in non-financial services).

Although GDPR requires organizations to have in place a scenario related to personal data breaches,

40% of financial institutions do not have one. At 76%, this is even higher in non-financial service organizations.

Acknowledgment, but limited action

80% of boards consider cyber security to be an operational risk. But only 36% address the topic in their annual report.

Cyber insurance: not yet fit for purpose

28% of respondents have cyber insurance.

68% say the reason why they don't have a cyber insurance policy in place is because it doesn't match their needs, 64% that it is too expensive, and 64% that coverage has too many limitations.

Know your weakest link

Despite increasing attention by regulators, third party risks are slipping off the radar.

44% say they have no instruments to enforce their control framework on suppliers (2017: 32%), and 38% have no contractually agreed binding terms related to cyber risks (2017: 29%).

34% do not require specific cyber security measures in third party contracts (2017: 30%), and 59% of contracts with third parties do not include a right to audit (2017: 40%).

New kid on the block(chain)

48% of respondents (63% in FS and 40% in non-FS) are evaluating the potential of blockchain, and 53% believe its use brings new security risks.

8% of respondents have implemented specific measures to deal with such risks.

Digital ID: clear benefits, but insufficient use

69% of respondents see digital IDs as an important step towards trusted interactions with clients. Only one-third say it is of strategic importance, however. And only one-third have plans to incorporate digital IDs into their products or services.

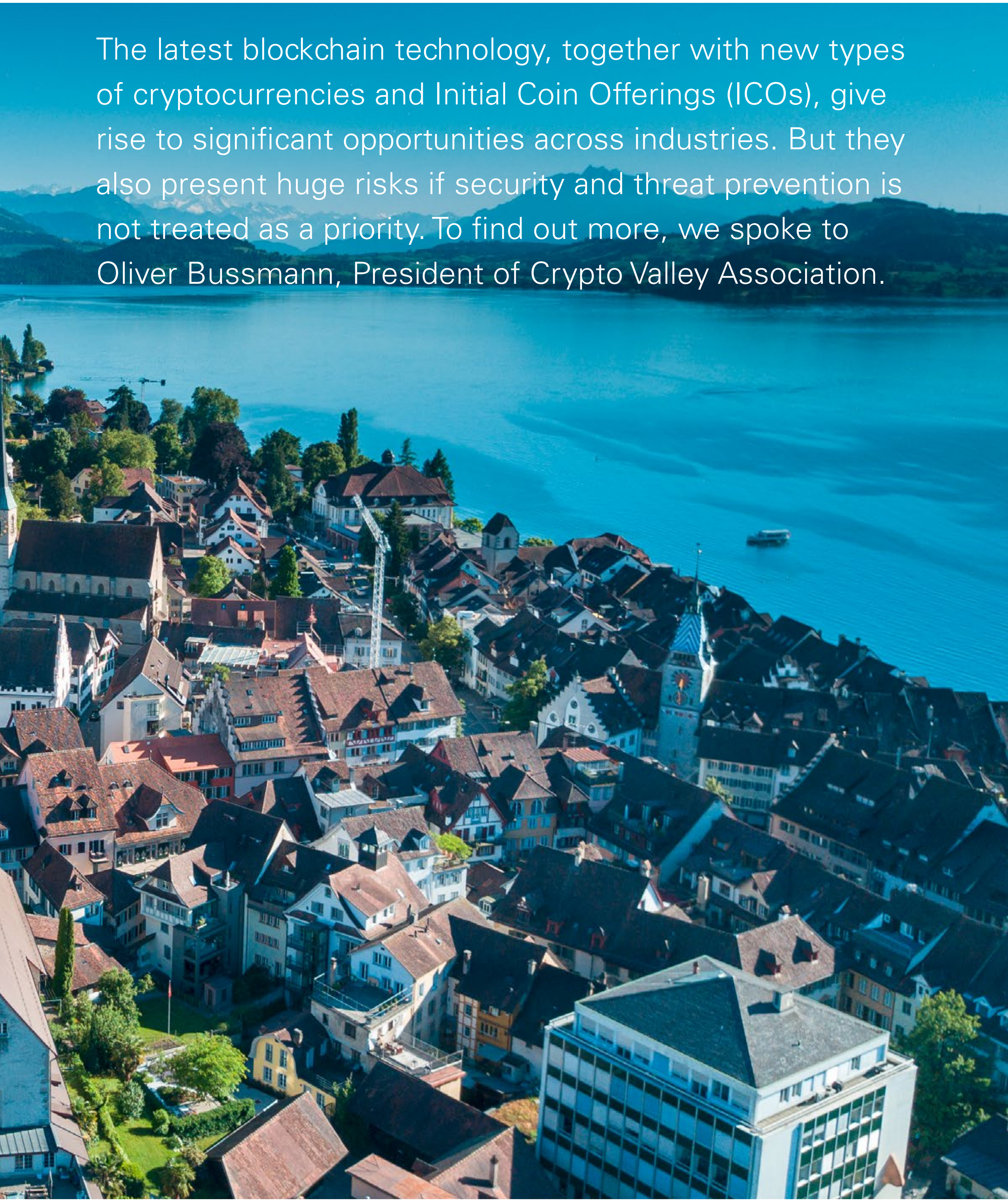
Cyber due diligence is lacking

Cyber security is missing from the vast majority of due diligence approaches when investing in companies or planning a merger.

23% of respondents confirm they include the topic in their due diligence scope.

Entering new territory: the opportunities and risks of blockchain and cryptocurrencies

The latest blockchain technology, together with new types of cryptocurrencies and Initial Coin Offerings (ICOs), give rise to significant opportunities across industries. But they also present huge risks if security and threat prevention is not treated as a priority. To find out more, we spoke to Oliver Bussmann, President of Crypto Valley Association.

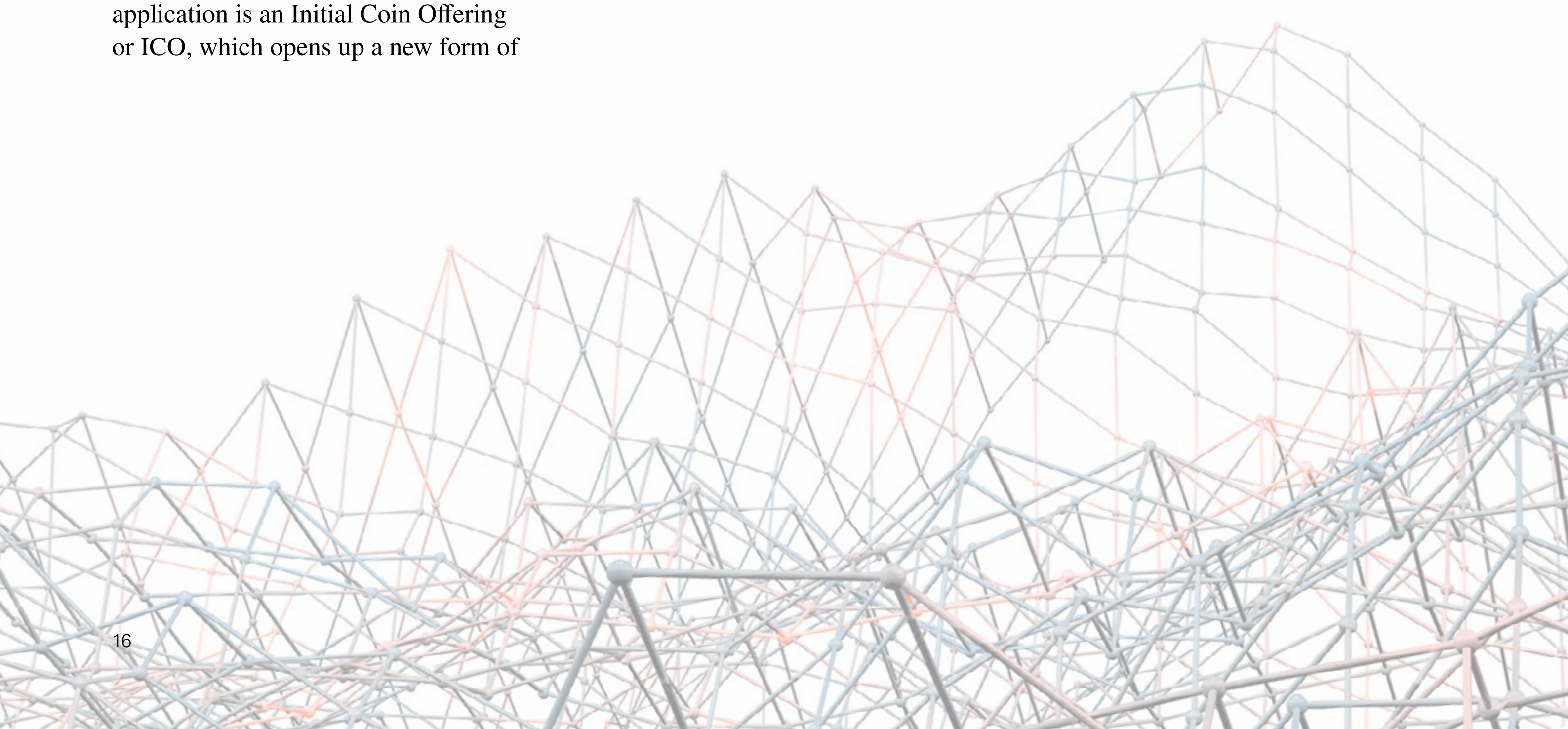


Oliver Bussmann
President of Crypto Valley Association

How do you see the current status of cyber security around blockchain?
With the opportunities offered by blockchain technology, we are forging ahead into completely new business models. They can be understood as open ecosystems. In other words, as economic systems that allow companies to digitalize business processes on a corporation or cross industry-wide basis. One concrete application is an Initial Coin Offering or ICO, which opens up a new form of access to capital markets. Transactions are based on what are known as 'smart contracts' or 'tokens' that describe the exchange of payments. Because these transactions involve large financial sums, they are naturally highly prized and the subject of attacks. ICOs can generate sums in average to the tune of 30 to 50 million US dollars or euros. But the software components used for such transactions are not all programmed according to the latest and most secure standard. When a company is considering an ICO, a prior cyber security audit is of utmost importance.

The blockchain and cryptocurrency community is still very young. How do you rate the maturity of this community in terms of its ability to mitigate or manage such risks?
The maturity level has improved, not least because the entire ICO process is becoming more professional. But there is still a significant need for education on the subject. That's why Crypto Valley Association has joined forces with KPMG to create a cyber security working group to raise awareness of potential risks. If we don't do things properly from the beginning, it can permanently damage the reputation of the new models and processes.

«Innovations in the blockchain field create new value, which in turn attracts threats and massively increases the potential risk.»



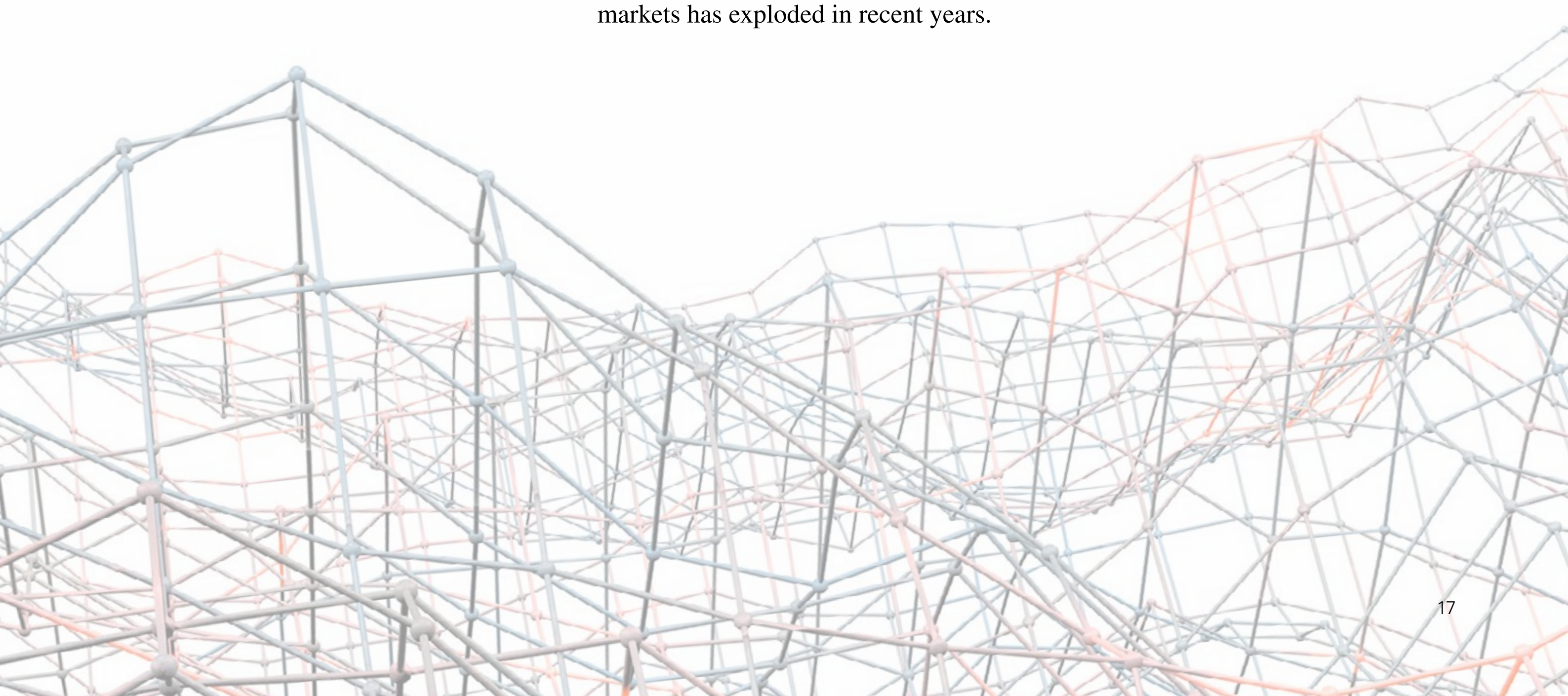
How do you intend to introduce a broader audience beyond cryptocurrency enthusiasts to this unfamiliar topic?
Blockchain transactions such as an ICO involve many different market participants. Our task is to raise awareness across the whole spectrum. One part of that is reaching the partners and companies directly involved in a transaction, but we also work to increase awareness among an expanded circle of investors, regulatory authorities, media and traditional financial institutions. This is where we see the greatest value and benefit of our organization.

As more people consider moving into the world of blockchain and cryptocurrencies, how user-friendly are these areas, and how transparent are the risks and cyber security issues?
It's certainly still very early days in terms of user-friendliness and the whole issue of security with so-called wallet solutions. The next steps will presumably first take place on the level of professional investors such as hedge funds or family offices that invest in crypto assets. Based on that experience, simpler, more secure and scalable asset management solutions will begin to emerge. Switzerland as a whole, and we at Crypto Valley Association, are clearly in a pioneering role when it comes to the further development of solutions, and open and transparent discussions about these issues.

ICOs are the big topic at the moment. What are the upcoming trends and what implications do they have for cyber security?
Yes, a lot of the focus at the moment is on raising capital through ICOs. For the near future, we primarily see a trend toward corporate solutions for areas such as payment, supply chain and trade finance transactions. Regulators and government agencies, in turn, will want to become more actively involved and attempt to guide the new world into orderly and safe structures. In this context, digital identity management of users will become increasingly important. But while this happens it is essential that users retain control of their data.

With regard to data security, to what extent is it possible to draw on experience from the online banking sector and heavily digitalized capital markets?
I've been working in IT for over 30 years now, including at a large bank. The effort and costs involved in controlling cyber risks in financial markets has exploded in recent years. And that trend is set to continue, if for no other reason than that blockchain applications work globally and do not take their lead from country-specific regulations and regulatory bodies. The risks will increase, and we will have to continue to invest a lot in security and threat prevention. Blockchain applications are wonderful things, but massive sums could be destroyed or misused in fractions of a second in just a few incorrect steps or through targeted cyber-attacks.

Do you see an opportunity for Switzerland, Crypto Valley and companies around this cluster of expertise to benefit from this early experience and develop new business models for the future?
Indeed. These innovations in the blockchain field create new value, which in turn attracts threats and massively increases the potential risk. We see our role in the association as a societal function, and we will work together with others to position Switzerland at the forefront as a reliable center of new business models in this sector.



Know your target: how cyber due diligence feeds investment decisions

Christian Unger, Managing Director and Co-Head Industry Value Creation at Partners Group, shares his insights into how cyber due diligence is becoming an integral part of ESG frameworks, and its potential to protect investors and customers alike.

Christian Unger
Managing Director and Co-Head Industry Value Creation at Partners Group

How important are cyber security and privacy risks from an investor's viewpoint, and which risks are key?
In our experience, investors increasingly attribute cyber security to ESG, or Environmental, Social and Governance, aspects. As a result, its importance in both private and public markets grows. There are many examples of well-known firms that have seen their value diminish due to breaches related to cyber security and/or privacy. At Partners Group, cyber security and privacy is important to protect investors but ultimately also the customers of our portfolio companies. The topic of data and its privacy is also becoming more prominent in public discussions and through cross-border regulations and directives such as GDPR and NIS. The priority for Partners Group is to make a thorough assessment of each company we consider investing in, with cyber security as a standard item in our due diligence process. We actively try to lead by example, through board work and other means, once we own these companies. And we take advantage of our global reach and platform to learn from research, industry peers and good practices in incident handling. Our clients and shareholders expect this from us. Through our ESG framework, we are institutionalizing our protocol on this topic to be a standard part of our investment processes.

We have not until recently seen many investors looking at cyber security or privacy risks as part of their due diligence. Do you expect this to change?
For Partners Group, cyber security and privacy risks are key items and discussion points in any due diligence process. We believe more and more investors and shareholders will expect companies to have a clear strategy in this area. As will regulators, even though specific expectations may vary according to the jurisdiction. Expectations and risks will also increase as we see further development and changes happening in the fields of Internet of Things, machine learning and overall digitalization and connectivity. The need for good due diligence will therefore only increase.

How do you balance the depth vs scope and duration of assessments of cyber security and privacy risks in target businesses?
This is a very interesting question. The non-binary outcome of a cyber security and privacy assessment often results in a decision to prioritize, for example, risk exposure related to the business's position in the supply chain (e.g. critical infrastructure) or handling of sensitive (personal) information. Covering all aspects would not only be time-consuming but also very costly and would not give 100% security. At Partners Group,

we first carry out an initial analysis to highlight some of the major risks, from dark-web scanning to vulnerability testing. Based on this initial analysis, we decide where to focus going forward. We have also found that by simply asking the management team cyber security-related questions, we quickly gain a basic but good understanding of the company's cyber security and privacy health. We have also noted in these processes that management teams appreciate an investor who can give them some guidance in a field where they feel growing pressure and where they might lack deep functional expertise.

How do such findings influence your investment decision?
As with other elements in a due diligence process, it is a risk-reward offset. If a potential investment shows clear cyber security risks, we can decide to walk away from the opportunity or we can choose to reflect the risk in our valuation or offer. We have an industry value creation team that works closely with our portfolio companies to grow and develop their businesses. In the case that we choose to move forward with an investment in a company that needs improvement in the area of cyber security, our value creation team would work with management to solve critical issues as a near-term priority. This might include staff training, assessment of the company's culture, cyber response plans etc.

Do you believe investors use cyber due diligence it to its full potential?
Compared to other due diligence elements such as financial due diligence or management assessment, cyber is a relatively new topic. However, the overall understanding of technology and its associated risks is growing rapidly in the investor community. We will see this clearly develop further and become more sophisticated. This will be necessary as the threats and risks will become more difficult to judge. Companies will have to continue to train and develop staff and make sure they have in place the most relevant technical solutions and third party providers.

Looking forward, how do you expect cyber and privacy due diligence to develop?
As mentioned, the market is developing fast and we will see new challenges arise. As with many digital developments generally, it will be important to be agile. This is because remaining 'current' will be a key success criterion in this field. It will be about managing risk, but also sharing best practices between companies or within the investor community. In the future, cyber security and privacy processes and assessments will be included as standard in any ESG framework.

«The overall understanding of technology and its associated risks is growing rapidly in the investor community. We will see this clearly develop further and become more sophisticated.»

SwissID’s quest to provide security, reliability and trust

Growing levels of digitalization bring an urgent need to be able to carry out online activities with confidence. SwissSign CEO Markus Naef shares his views on how Digital IDs can help to achieve this aim.

Markus Naef, CEO of SwissSign

You recently began to introduce SwissID to the Swiss market. Why is this important for Swiss society and the economy?

Because the digital revolution impacts all sectors of society and economy. SwissID and the establishment of an electronic identity is a key factor in Switzerland's ongoing digitalization. For citizens, purchasing goods and services online, managing payments, taking out loans, signing contracts or voting electronically are important actions that can be performed in the digital space – as long as they can be done with confidence. This is exactly what SwissID does: it provides the basis for secure, reliable and trusted e-business processes. In addition, SwissID helps to significantly simplify and streamline processes. This can also be at a financial level: international data show that savings of around 1.5% to 2% of GDP have been achieved following the national roll-out of a digital ID. SwissID helps companies save costs even in the short term. Depending on the complexity of the business, a login currently costs from a few francs to a mid-double digit amount per year and client. It therefore pays for companies to outsource their login service to an external service provider that complies with the latest security requirements.

What are the most important use cases, now and expected in the future?

Digital identities are relevant to a wide range of situations. The number of use cases is almost unlimited. Swiss Post was the first company to use SwissID. Various companies and cantons are set to follow in the second half of 2018. Applications are currently in the business-to-customer and business-to-government sphere, with a focus on using SwissID to access online platforms and for digital administrative processes. In the future, SwissID will enable electronic payments and qualified digital signatures, which will significantly increase the number of possible use cases. Talks are also ongoing in the B2B space, focusing on using SwissID digital identity in conjunction with Internet of Things devices. The classic example from the early days of the IoT – the fridge that automatically orders more of a product when it's running low – has become a footnote. Today, industrial and healthcare companies are thinking on a much larger scale; for example, applications in product manufacturing or eHealth diagnostics. Around 80% of companies believe that the IoT will be very important in the years ahead.

What are the benefits for SwissID users? Why are currently available digital IDs such as from Google or Facebook insufficient?

SwissID makes life easier and safer. If someone uses various online services, they may have many different logins and accounts. Each organization may handle an individual's data very differently, and the users often have no control over, or understanding of, to whom they are giving their information.

«Trust, acceptance and usability are the most important success factors for digital identities. It needs to be easy to use so it does not interrupt the typical way in which users interact. It must be flexible and easily deployed.»

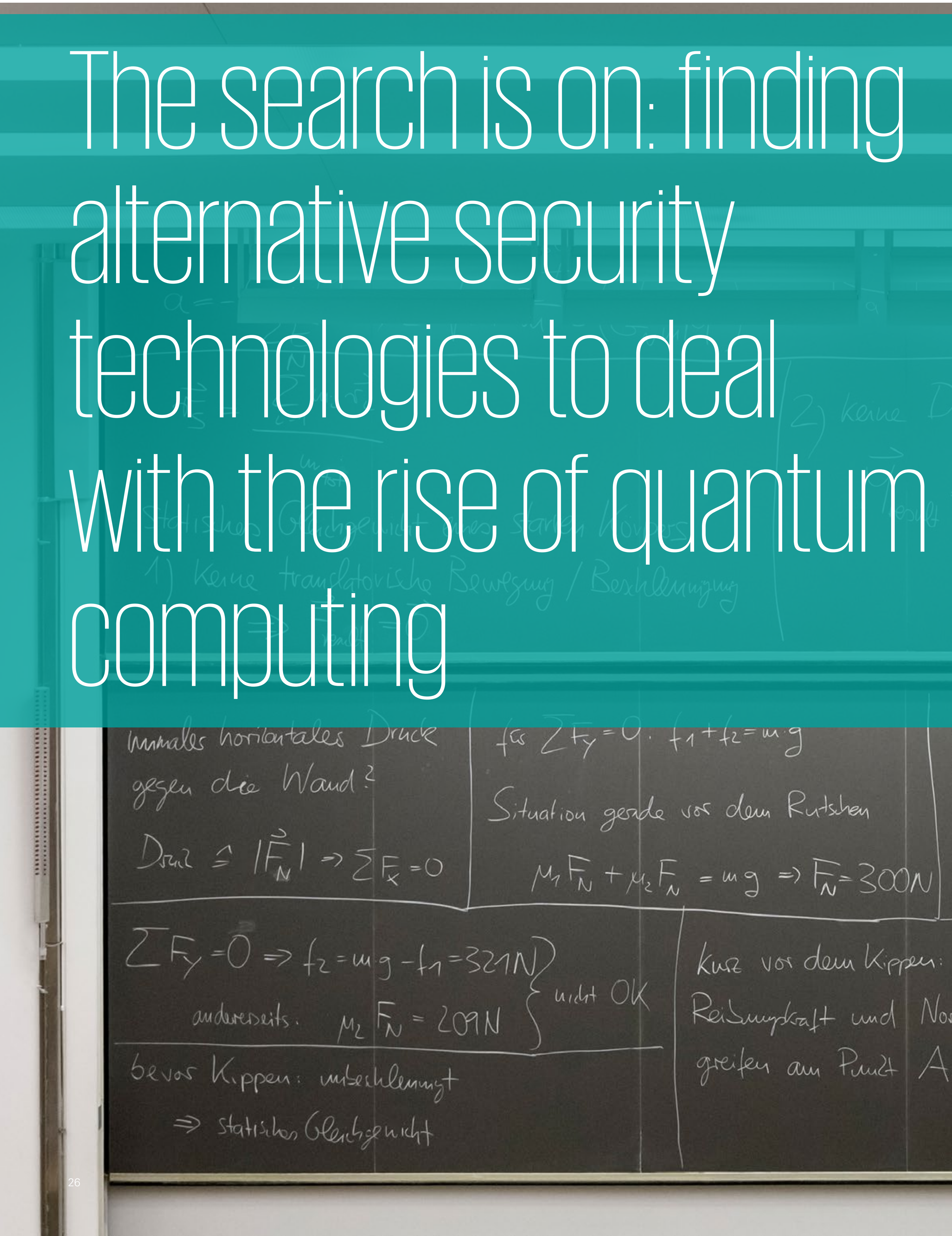
They often forget about security in favor of user-friendliness. However, SwissSign combines usability with security. In contrast to other logins such as Facebook or Google, SwissSign does not use data profiling. The login quality is another differentiator. Unlike SwissSign, sites such as Facebook offer just a self-declared identity and no verified identity. Furthermore, we are transparent and protect our users' personal data, as SwissID gives users full access to, and control over, their personal data and digital identity. The users have to give their explicit agreement for the transfer of any requested information.

SwissID is not the first attempt to introduce a digital identity in Switzerland. What critical success factors will make SwissID more widely adopted?
Trust, acceptance and usability are the most important success factors for digital identities. It needs to be easy to use so it does not interrupt the typical way in which users interact. It must be flexible and easily deployed. Further, an identity that can be trusted by more than one organization will ensure an easier user experience, particularly if the identity can be managed and protected seamlessly and is transparent to the user. However, trust between organizations is difficult to establish as they often have different, sometimes competing priorities. Our shareholders' commitment to use SwissID for their platforms means we can quickly bring a large number of users into the ecosystem. Another bonus is that private individuals can use SwissID free of charge, which naturally increases acceptance.

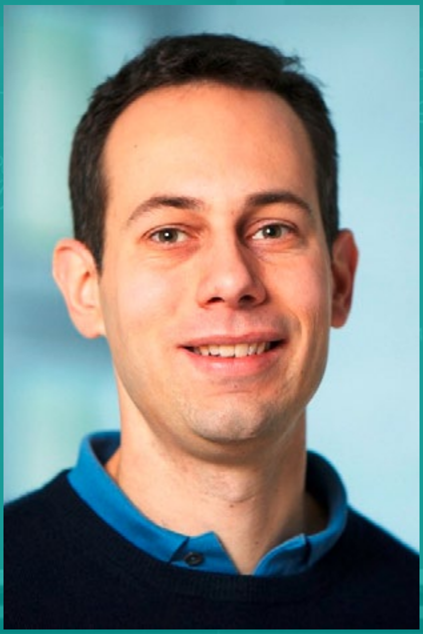
SwissID could be an attractive target for cyber-attacks. How do you ensure it is secure?
Data security is of course our top priority. SwissSign is working with ETH Zurich and other well-known security institutions to identify and combat current and future threats. Nowadays, most users find it difficult to manage their online identity across multiple websites and services. This is due mainly to a lack of understanding of the security risks. An official unified digital identity such as SwissID solves this problem. As services and networks have expanded, threats in the digital world have increased – in particular relating to identity theft. As individuals take advantage of new services, their number of digital identities also expands. In the absence of an effective way to manage all these identities, or a consistent way of protecting them, their vulnerability to identity theft grows. SwissID means individuals must take care of only one transparent and secure digital identity.

There are initiatives to introduce self-sovereign identities based on blockchain technology. Some Swiss cantons are experimenting with them as we speak. What does this mean for SwissID and SwissSign?
We are closely monitoring blockchain and other technologies, and are in constant contact with the developers of these solutions. It's true that blockchain-based IDs are still in the experimental phase, and we do not want to engage in experimentation. Security and usability are our priorities. If blockchain or another technology proves better, more secure and more reliable, we will of course use it for SwissID as well. At present, our experts still believe that the risk of teething problems and system failures with blockchain is too high. In addition to security, SwissID's focus is on usability and instant application – for this, we are best served by the latest, tried-and-tested technology.

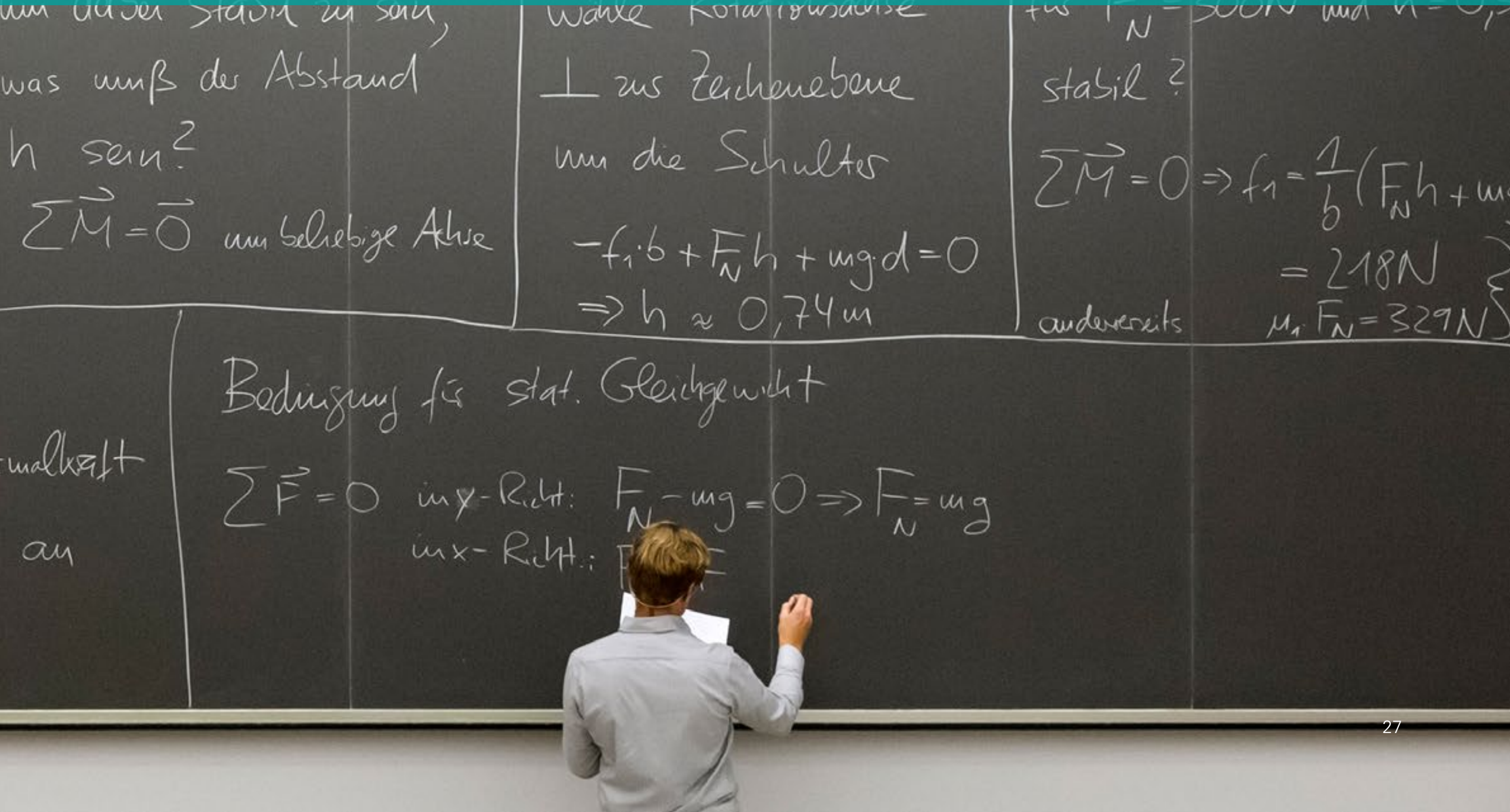
The search is on: finding alternative security technologies to deal with the rise of quantum computing


Statisches Gleichgewicht eines starren Körpers
1) Keine translatorische Bewegung / Beschleunigung
2) keine D
imales horizontales Druck
gegen die Wand?
Druck ≙ |F_N| => ΣF_x = 0
für ΣF_y = 0: f1 + f2 = m·g
Situation gerade vor dem Rutschen
μ1 FN + μ2 FN = mg => FN = 300N
ΣFy = 0 => f2 = mg − f1 = 321N
andererseits: μ2 FN = 209N
nicht OK
Kurz vor dem Kippen:
Reibungskraft und Nor
greifen am Punkt A
bevor Kippen: unbeschleunigt
=> statisches Gleichgewicht

Quantum technology is expected to be a game changer, with enormous impacts on computing and security. With vast sums currently being invested in research and development, the race is on to advance quantum technology and build practical quantum systems and applications. Renato Renner, Professor for Theoretical Physics at ETH Zurich, shares his insights into the future of this critical capability.



Renato Renner,
Professor for Theoretical Physics
at ETH Zurich



What do you see as the major benefits and most promising use cases of quantum computing?

Quantum computers will be able to solve problems that are totally out of reach even for the best supercomputers today. However, a quantum computer is not just a very fast version of a classical computer. One should rather think of it as a computer that has a largely extended set of instructions, which a software engineer may use when programming it. To harvest the extra power of quantum computers, therefore, we first need a new type of software, which one may call 'quantum software'. Since the development of such quantum software is still in its infancy, it is difficult to predict future use cases. But generally, I expect very different types of applications, ranging, for instance, from the design of novel types of materials in physics to the optimization of processes in chemistry, and to improved machine learning.

How will such advances affect approaches to areas such as cyber security and cryptography? And how quickly do you think this will happen?

Quantum technologies will have a major impact on information security, and we will have to act wisely to ensure that it will be a positive one. First of all, there is a threat. Whoever has a sufficiently large quantum computer will be able to break the public-key cryptosystems we are using today, such as RSA. The prototype quantum computers presented recently by IBM and Google are still much too small to run such attacks. But, very likely, the ones we will be able to build in ten years or so represent a real danger. This is definitely something we have to take seriously. But, luckily, the quantum era also opens up new possibilities to counter these threats. One of them is quantum cryptography. It uses an encoding of information into individual light particles, which may then be transmitted over optical fibers. Quantum cryptographic systems offer an extremely high level of security – even quantum computers will not be able to defeat them.

> «One must recognize that even if quantum computers will become available only in, say, 15 years, they are already affecting the long-term security of our current cryptographic schemes.»

How should cyber security practitioners and cyber technology vendors prepare for the rise of quantum computing?

They should start looking for alternatives now! One must recognize that even if quantum computers will become available only in, say, 15 years, they are already affecting the long-term security of our current cryptographic schemes. So, for example if I encrypt a message today using a standard public-key cryptosystem, an eavesdropper may store the ciphertext and, in 15 years, buy a quantum computer and decrypt it. Ironically, the quantum revolution is not only a threat to information security. As mentioned, it also provides a solution. Quantum cryptography could be of interest to all those who worry about long-term security. Even attackers with infinite computing power will be unable to get hold of encrypted secrets. This is due to the distinct feature of quantum cryptographic systems: their security relies on the quantum-physical properties of light particles. The only way to break into them would be to change the laws of physics. But this is clearly impossible – even for the most powerful eavesdroppers we can imagine.

How will quantum computing affect the security of current blockchain implementations, and how should the blockchain community deal with it?

For blockchains, long-term security is obviously essential, even more than for encryption. No-one wants to use a cryptocurrency that will become worthless in 15 years due to a quantum attack. But exactly this could in principle happen — at least we cannot guarantee that it could not. Researchers have only recently started to look into this question. But the results are quite worrying. One of the latest studies claims, for instance, that particular components used by Bitcoin could be broken by a quantum computer as early as 2027. Probably the best possible countermeasure is to insist that blockchain implementations are redundant, so that a successful quantum attack on one of its components does not render the entire scheme insecure. The other is to further push research and development of novel quantum-proof cryptographic methods. Those who invented the blockchain technology we use today most likely didn’t have quantum computers in mind as a serious danger.

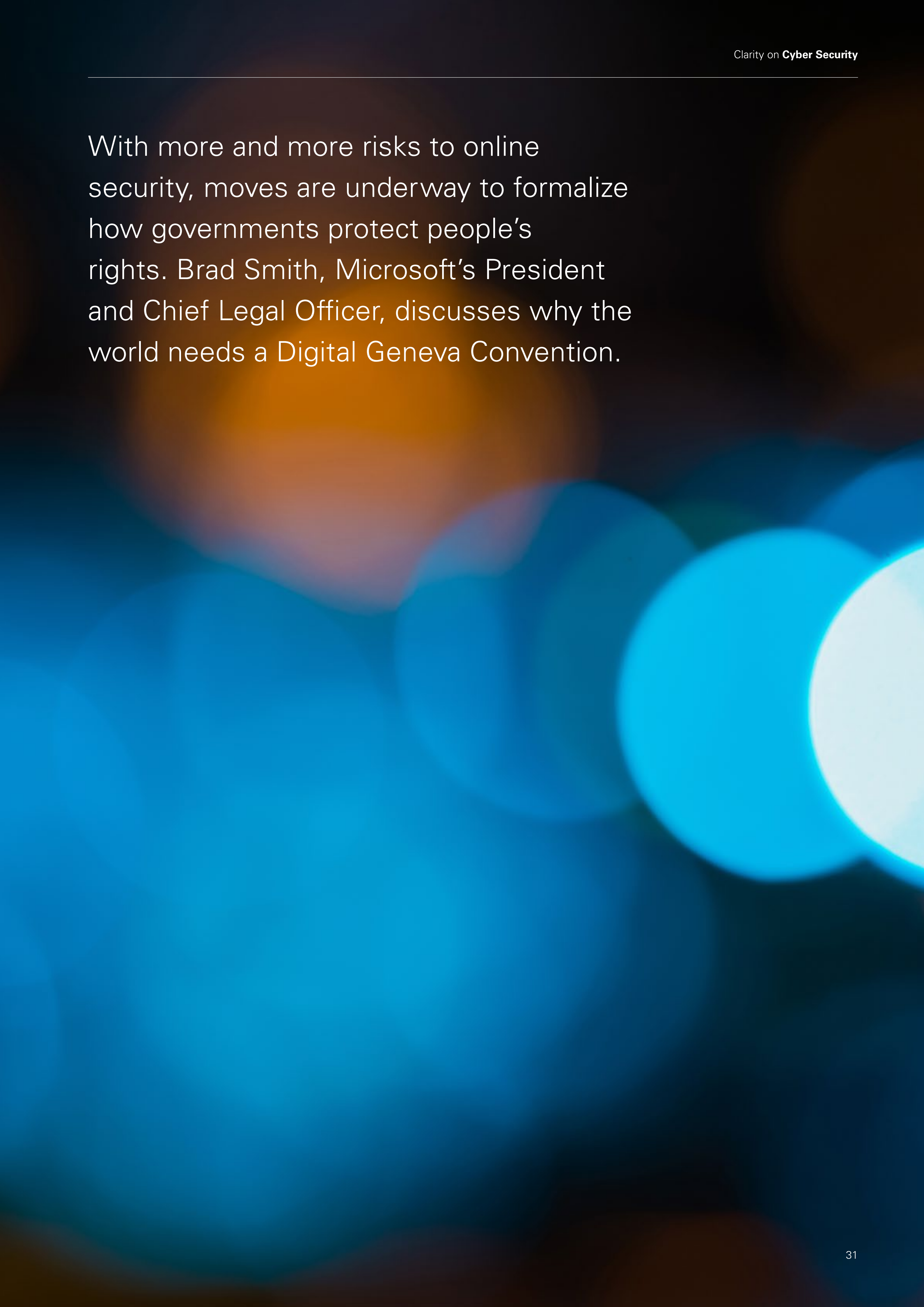
How will companies, security practitioners and society benefit from advances in quantum cryptography?

Current quantum cryptographic systems require special infrastructure such as a direct optical fiber connection from sender to receiver. Quantum cryptography is therefore currently suitable only for high-security applications, where costs are not much of an issue. But rather than trying to predict the impact of quantum cryptography on society, I would issue a warning: Perfect secrecy, in the hands of those with bad intentions, may of course also be a threat.

INTERVIEW

Protecting civilians in cyberspace: the Digital Geneva Convention

Brad Smith
Microsoft's President
and Chief Legal Officer



With more and more risks to online security, moves are underway to formalize how governments protect people's rights. Brad Smith, Microsoft's President and Chief Legal Officer, discusses why the world needs a Digital Geneva Convention.

«The Digital Geneva Convention is about getting governments to protect people in cyberspace the same way they protect them in the physical world, even though we recognize this is probably more difficult.»

Why is the time right for a Digital Geneva Convention?

The online world has become a cornerstone of global society, important to virtually every aspect of our public infrastructure and private lives. As we look to the future, new online technologies will do even more to help address important societal challenges, from improving education and healthcare to advancing agriculture, business growth, job creation, and addressing environmental sustainability. Recent events, however, have put online security at risk. Malicious actors, with motives ranging from criminal to geopolitical, have inflicted economic harm, put human lives at risk, and undermined the trust that is essential to an open, free and secure internet.

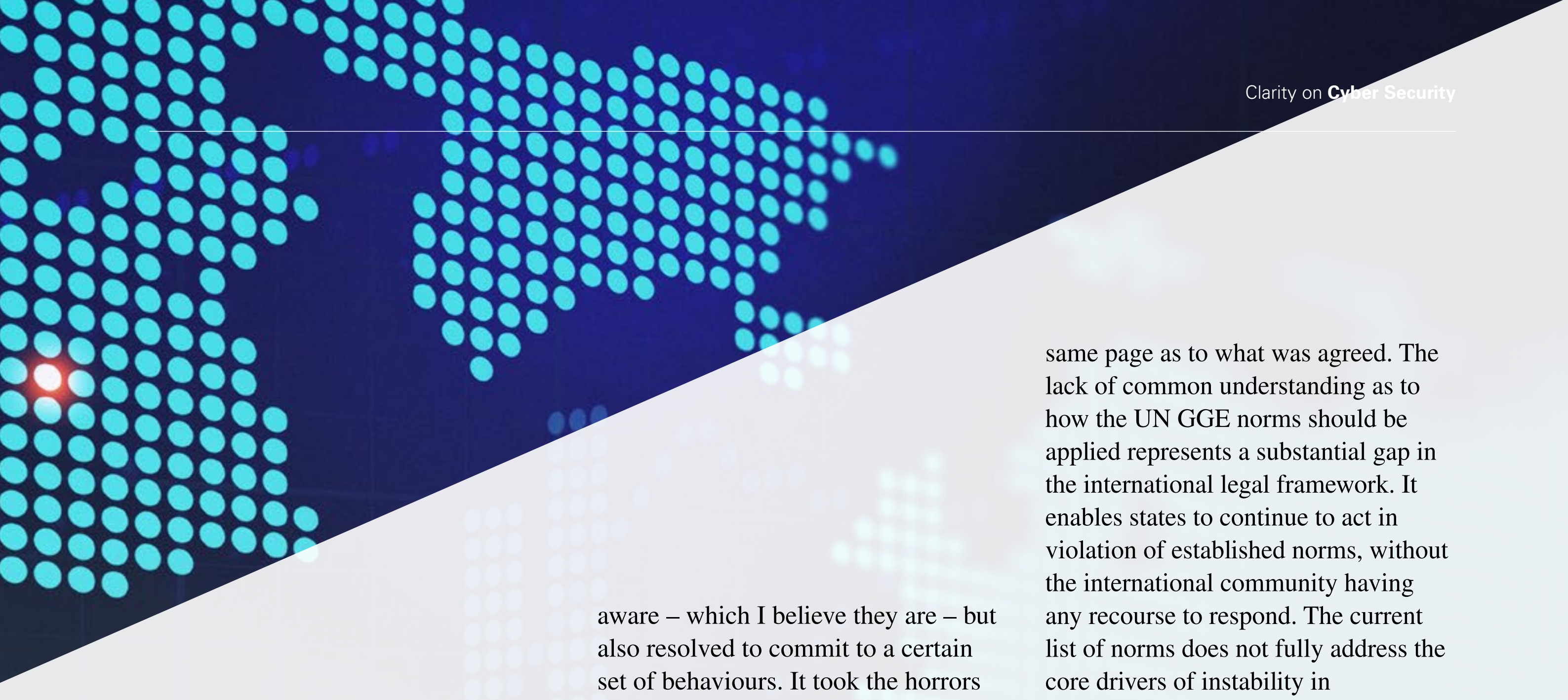
More than 30 governments have acknowledged that they have offensive cyber capabilities. However, unlike with conventional weapons, cyber arsenals are clandestine and intangible. Their source is difficult to track and identify. It is therefore likely that the real number is not only much higher, but will continue to grow.

So, what are the aims of the Digital Geneva Convention and what are its prospects?

The Digital Geneva Convention is about getting governments to protect people in cyberspace the same way they protect them in the physical world, even though we recognize this is probably more difficult. Identifying legal gaps, developing and implementing norms, and agreeing to rules of the road take time and require a multi-stakeholder effort. Just as the world's governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, a Digital Geneva Convention would protect citizens online in times of peace. Moreover, Microsoft acknowledged that no single step will by itself be sufficient to address the problem. We encouraged the tech sector to together do more, given its unique role as the internet's first responders. We commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust.

Is this not the role of nation states or even international organizations such as the United Nations?

Cyberspace is not the domain of government. It is driven by people and technology companies. We live in an internet-dependent world and cannot rely on governments to fix this problem in isolation. Numerous conventions which bind governments today came about as a result of an initiative put forward by a non-governmental organization or a single individual. Just last year the



International Campaign to Abolish Nuclear Weapons, or ICAN, was awarded a Nobel Peace Prize for its work on the Treaty on the Prohibition of Nuclear Weapons. Similarly, the work of a single Swiss businessman Henry Dunant resulted in the first Geneva Convention. Governments sometimes need to be encouraged to act for the benefit of society as a whole. I think the time has come to do so with regard to cyber weapons.

Which stakeholders should play a major role in developing and implementing the Digital Geneva Convention, and are they sufficiently aware and committed?

It is critical that a range of stakeholders are involved in negotiations. These include diplomatic experts from governments, technical and policy experts from global technology providers, civil society and academia, and experts from key international organizations such as the United Nations. While final negotiations would be undertaken by governments, an inclusive and transparent approach that enables a range of stakeholders to participate, exchange, and react to others' expertise and experiences will ensure that the final outcome is practical, implementable, and meaningful. We are at the beginning of this journey. But I am confident that over time stakeholders from around the world and across sectors will not only be aware – which I believe they are – but also resolved to commit to a certain set of behaviours. It took the horrors and devastation of World War II for today's Geneva Convention to achieve global agreement. Technology today has the ability to similarly cause chaos and major disruption. It should not take a catastrophe to bring the world together and establish universally accepted norms.

What are the key challenges to implementing the Digital Geneva Convention?

There are two major obstacles: the state of international relations today and the complexity of the issue. The current political environment does not bode well for any comprehensive international treaty, which take time even at the most opportune moments. Moreover, any movement in this space needs to involve not only governments, but representatives of industry and civil society. Without broader involvement and discussions with technical experts in particular, even well-meaning frameworks can result in counterproductive outcomes that reduce, rather than increase, security.

This sounds like a huge task. How can such massive obstacles be overcome?

To make significant progress, we must move in smaller increments. First, we need to embrace the agreements reached so far, for example through the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). We all need to get on the same page as to what was agreed. The lack of common understanding as to how the UN GGE norms should be applied represents a substantial gap in the international legal framework. It enables states to continue to act in violation of established norms, without the international community having any recourse to respond. The current list of norms does not fully address the core drivers of instability in cyberspace. A limited set of additional cyber security norms must be developed in areas where existing rules are either unclear or may fall short in protecting civilians in cyberspace. This could include norms which explicitly articulate protections for civilians, even if they are implicitly contained elsewhere in international law. Third in this process is the actual implementation of established norms, which would lead to the development of customary international law. In this process, governments need not only adhere to the norms themselves, but hold other nation states accountable – whether through punitive actions such as economic sanctions or by condemnation.

Looking at the journey so far, what are your personal highlights?

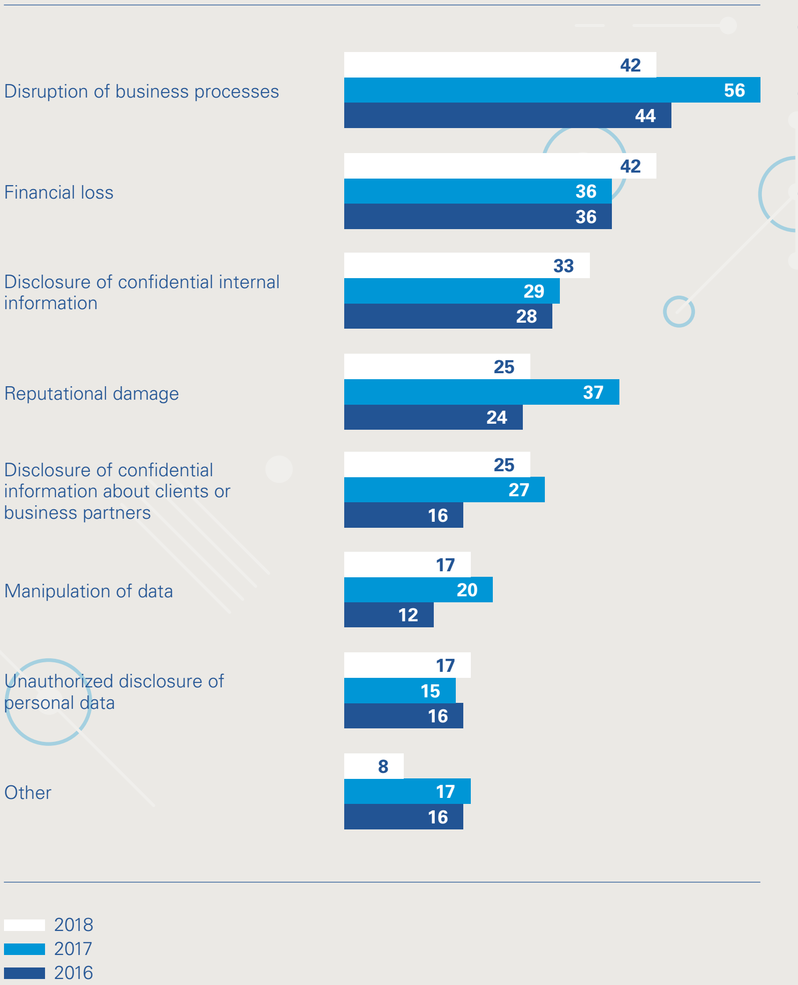
I was particularly touched by the fact that our call for a Digital Geneva Convention resonated so much with young people around the world. The digital natives are much more aware than politicians are of the impact offensive government action in cyberspace can have on all of our lives. Perhaps even more aware than we in the tech sector who are often driven by quarterly results. The response I get when I talk to young people affirms that we are on the right path and that we need to persevere in getting governments to a negotiating table.
It might be difficult and unpopular, but if we are to ensure that generations to come can enjoy the benefits of free and open internet, we need to act now.

How to build resilience and trust in our digital economy

We strongly suggest that Swiss businesses pay greater attention to building cyber resilience, while proactively tackling the risks and seizing the opportunities created by cyber security. In particular, action is needed around four critical success factors for a sustainable growth strategy.

Digitalization enables sustainable growth, but requires trust to secure it

What were the consequences of the successful cyber attack(s) on your business? (in percent)



Our age of rapid and profound technological change means we experience disruptive forces across society. Leveraging these forces for the benefit of your organization and stakeholders is not only about adopting new technological developments, however. It is about embracing the broader digitalization of your business, combining underlying technologies with a better use of data to produce superior solutions and an enhanced customer experience.

As you assess changes to your business model, it is important to revisit how you plan to interact with customers and other stakeholders such as business partners. And how the outcome of transformation efforts will build an environment of trust in which customers are confident in their transactions with you. The resilience of your business – and indeed, your entire ecosystem – is at the heart of inspiring this trust. Business leaders of course understand that successful growth strategies are based on trusted relationships. But while most Swiss respondents to our survey acknowledge the risks presented by cyber security, few appear to be acting on this awareness.

The results could be damaging to your business's growth prospects. Inaction over cyber security will lead to inadequate cyber resilience, which in turn will cause customers and investors to lose

56%
of respondents indicate that their budget for cyber security rose between 2016 and 2017.

confidence. This contradiction between acknowledgment and action must be remedied if growth is to follow. Here are just two of the many reasons why:

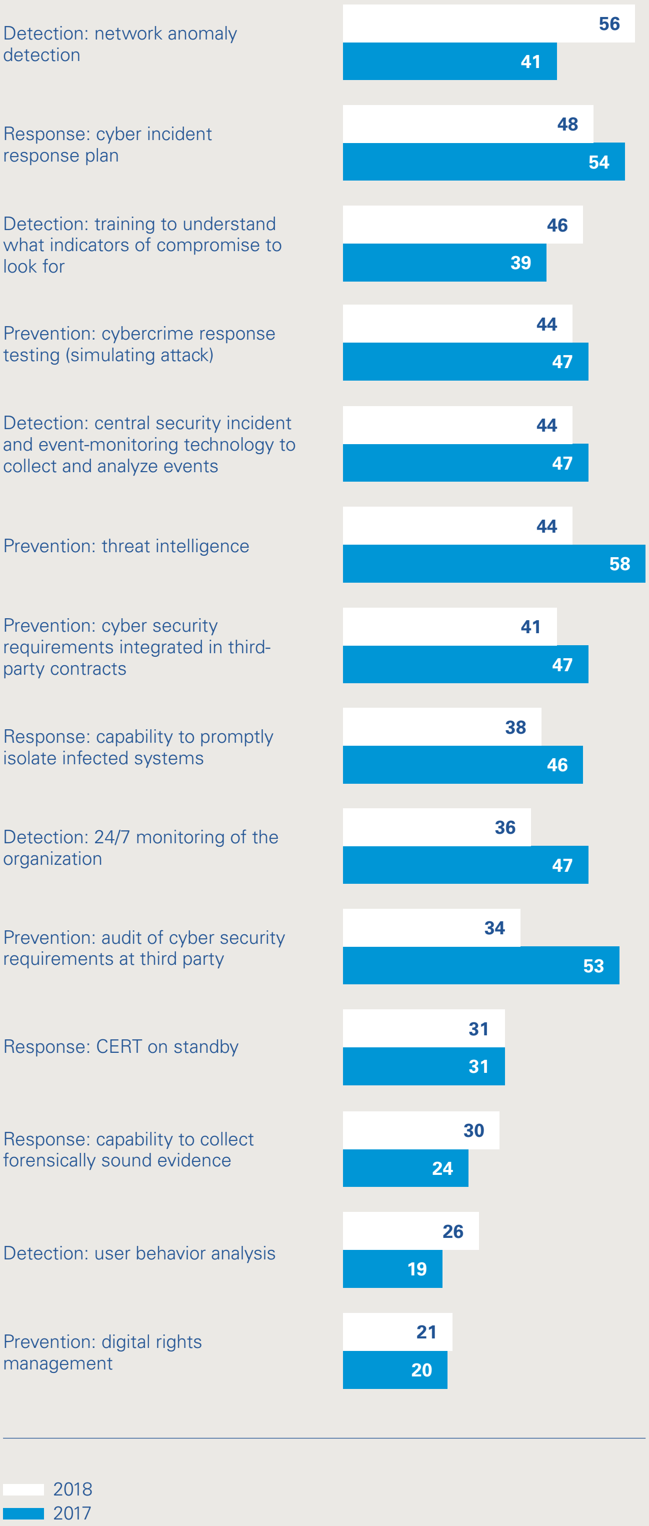
Successful cyber attacks caused financial losses at 42% of businesses

Respondents to our survey confirmed that successful cyber attacks adversely affected their businesses, including the following over the previous 12 months:

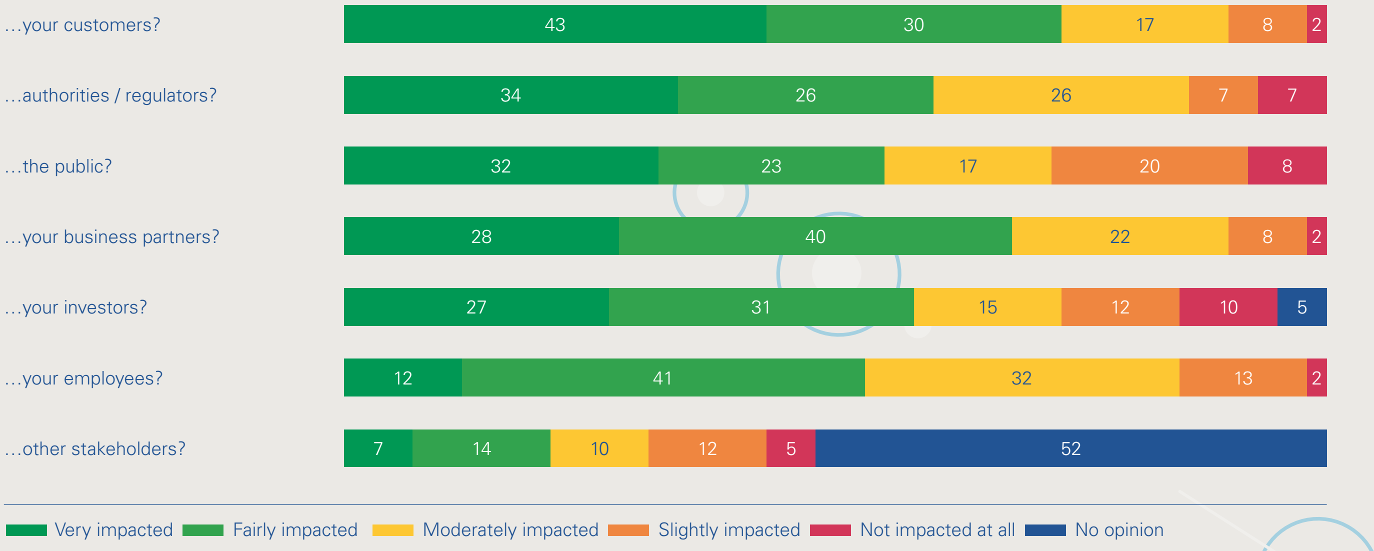
- 42% of businesses suffered financial losses (52% in financial services and 25% in non-financial services)
- 42% suffered disruption of business processes
- 33% suffered from disclosure of confidential internal information.

Criminals are highly creative and rarely pause in their efforts to find new ways to attack systems and make money out of stolen data. Large scale, untargeted attacks are moving from ransomware to crypto mining, which may go undetected except for higher energy consumption and a lower computing power performance. The reputational and financial stakes may help to drive more investment in cyber security. 56% of respondents indicate that their budget for cyber security rose between 2016 and 2017.

Which controls have you implemented in order to prevent, detect and respond to cyber-attacks? (in percent)



How high do you consider the impact of cyber security breaches on the trust of … (in percent)



Cyber security breaches damage trust

73% of respondents believe that customers' trust in an organization is 'very' or 'fairly' impacted by cyber security breaches. And 58% believe it impacts on investors' trust in the business.

In terms of recent regulations, few are as prominent as GDPR. 87% of respondents confirmed that GDPR applies to their organization Unsurprisingly, an overwhelming majority of respondents agree that GDPR places a heavy burden on the organization to protect data and privacy. However, they are also positive about the regulation's potential: 71% say that GDPR is valuable to give individuals control over their own data, thereby contributing to trust.

An insurance product to cover businesses against internet-based risks, and more broadly from technology-related threats will become increasingly important over the coming years. But it seems that Swiss businesses do not as yet see the need – or that current policies don't suit their requirements. 28% of respondents have cyber insurance, 23% are considering purchasing cyber insurance coverage to mitigate the risks. 34% aren't considering purchasing coverage. The onus should be on insurance firms to develop appropriate policies to deal with current and evolving threats, and for businesses to ensure they are adequately covered.

Contradictions remain at the heart of Swiss cyber security plans

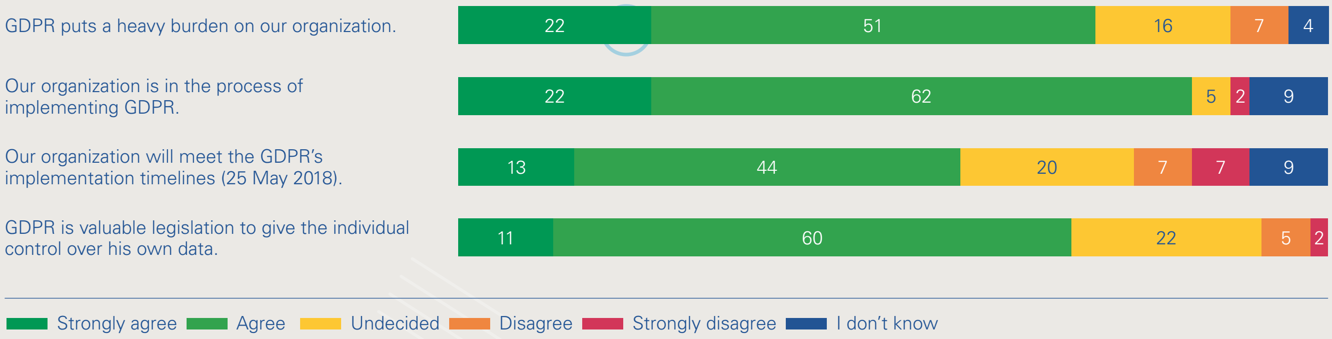
Being aware of the challenges and opportunities is not enough. Radical action is needed.

Take three examples:

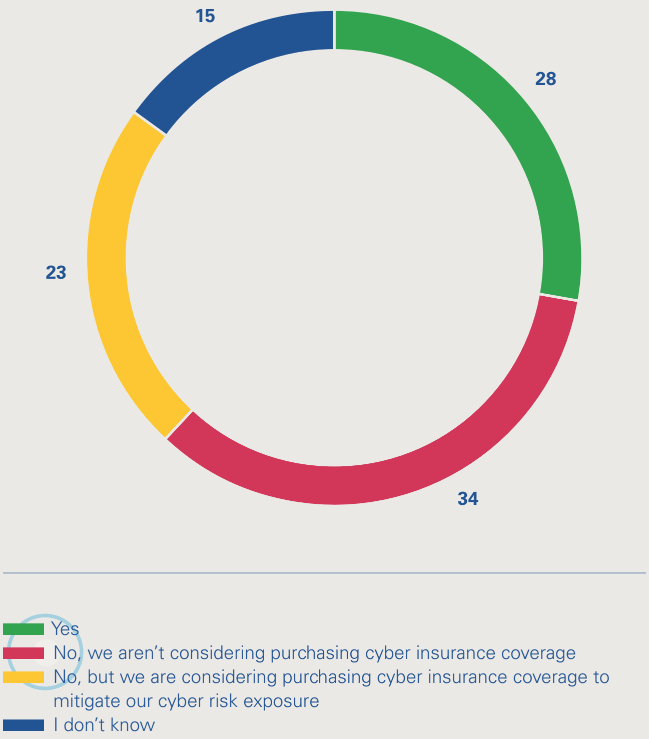
- While 80% of respondents say their board sees cyber security as an operational risk, only 23% of organizations carry out specific cyber evaluations as part of their due diligence in the context of mergers and acquisitions.
- 56% percent think the main issue in managing third party risks is insufficient transparency over the effectiveness of a supplier's control framework. Yet, an overwhelming 82% of cyber response plans do not cover attacks against third parties such as suppliers or business partners.
- The lack of action extends to regulatory issues: while 87% say GDPR applies to their organization, only two-thirds of cyber response plans covering breaches of personal data.

The stark contrasts between knowledge and action are clear and considerable. They cannot be allowed to continue if Swiss businesses are to be resilient in the digital age.

With which of the following statements do you agree? (in percent)

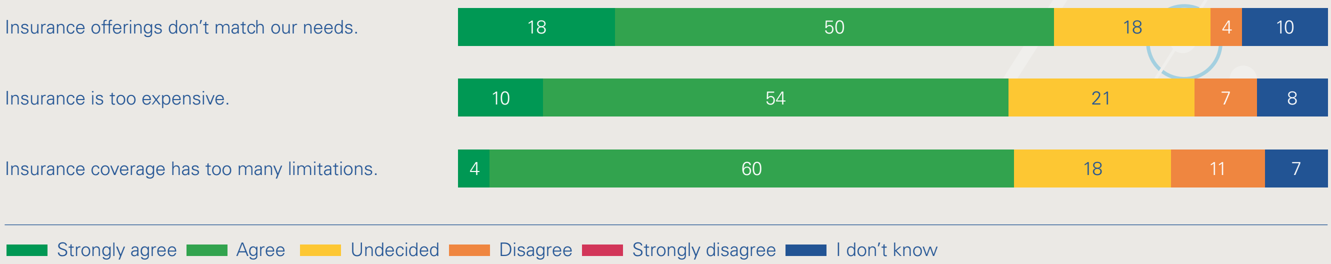


Does your organization have a cyber insurance policy in place? (in percent)



28% of respondents have cyber insurance, 23% are considering purchasing cyber insurance coverage to mitigate the risks.

What barrier(s) prevent(s) you from putting a cyber insurance policy in place? (in percent)



Emerging technologies: great potential but also great exposure

Blockchain. Internet of Things. Cloud services. Three examples of emerging technologies that are creating fresh business opportunities. Their potential is significant, but they can come at a price – increasing the surface area for cyber attacks that exploit vulnerabilities at businesses that are insufficiently prepared. Firms must critically assess their exposure, including what measures they are taking to mitigate the risks. And by doing so, move towards greater resilience and higher levels of trust.

Blockchain

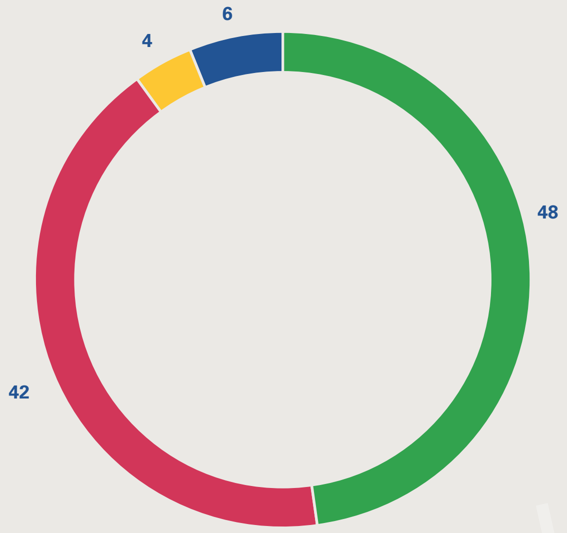
The blockchain is the new arrival in trust concepts. This ultimate decentralized model is generating significant interest, partly because people applaud the emergence of an alternative to existing, mistrusted centralized powers and authorities. Our survey confirms significant interest: 63% of respondents in financial services say their organization is evaluating blockchain, though in non-financial services it is only 39%.

In theory, a blockchain is an intrinsically safe system because it is decentralized, distributed and a public ledger. Data in the blockchain cannot be manipulated because of this structure. Technically, cryptocurrencies and smart contracts on a blockchain are impossible to corrupt.

A secure architecture is built on the assumption of a decentralized community of miners. But in the early days of blockchain, mining was done by individuals. They now tend to gather together in mining pools to increase their computing power as mining has become much more difficult. This concentration into pools poses a risk: if someone possesses more than a half of the network's computing power, it is possible to take control and authenticate transactions of choice. In such a scenario, the whole system would become untrustworthy. And with no central body to oversee it, who will step in to remedy the problems?

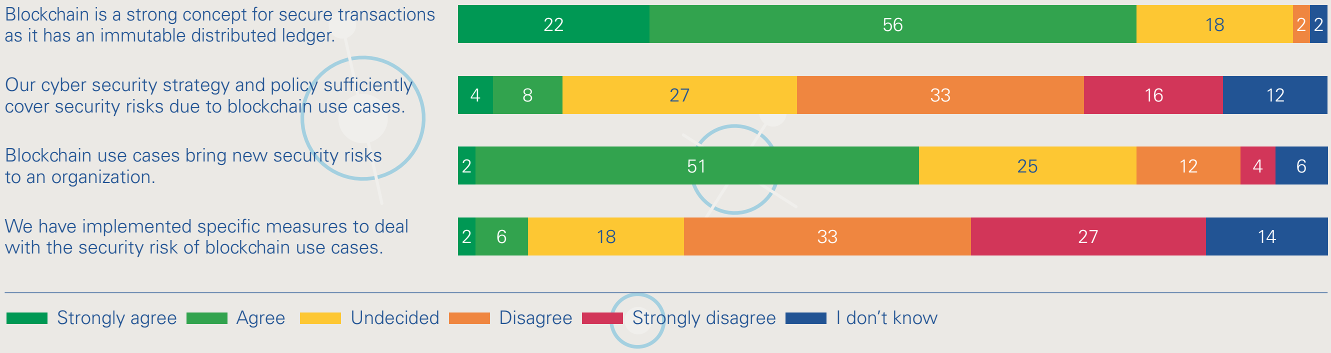
Moreover, the aspect of user friendliness seems to be largely unnoticed in the coverage of blockchain concepts. Blockchain may be an inherently safe concept but this implies that users start managing their private keys in the form of wallets. For many, this will be too much trouble. As a consequence, they will use intermediary parties, introducing new vulnerabilities.

Frontrunners in business are evaluating the use of blockchain technology. Is your organization evaluating this new technology for potential use cases? (in percent)



🟩 Yes
🟥 No
🟨 Not applicable
🟦 I don't know

What is your opinion on cyber risks in relation to blockchain technology? (in percent)



Another critical remark is more future based. Y2Q, the year a large-scale, accurate quantum computer arrives is expected sometime in the next ten years. When it happens, it will be able to break the public-key cryptosystems we currently use. Even the integrity of data on the blockchain may become vulnerable. This makes the development of quantum cryptography essential for long-term security.

All in all, blockchain is no silver bullet for trust. Our survey results indicate that nearly 80% of respondents perceive blockchain to be a strong concept for secure transactions. Half of them also are aware that the use of blockchain brings new security risks. And half acknowledge that their current cyber security strategy does not cover these risks.

48%

are evaluating the potential of blockchain and more than half of respondents believe that blockchain use cases bring new security risks to an organization.

Internet of Things

The Internet of Things is growing at an exponential pace, with connections that don't stop at the digital world. In other words, cyber security is no longer confined to cyberspace. Rather, it encompasses our physical world. More interconnections also mean that the impacts of breaches or failures are growing.

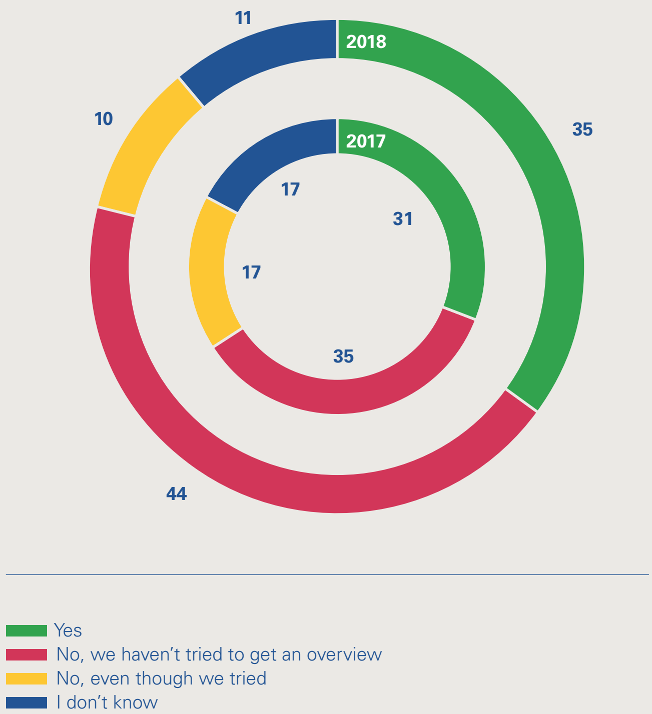
Worryingly, only 35% of respondents have an overview of Internet of Things and operational technology devices deployed in their organizations (2017: 31%). A majority – 58% (2017: 48%) – admits that these are not covered in their current cyber security strategy and policies.

Cloud services

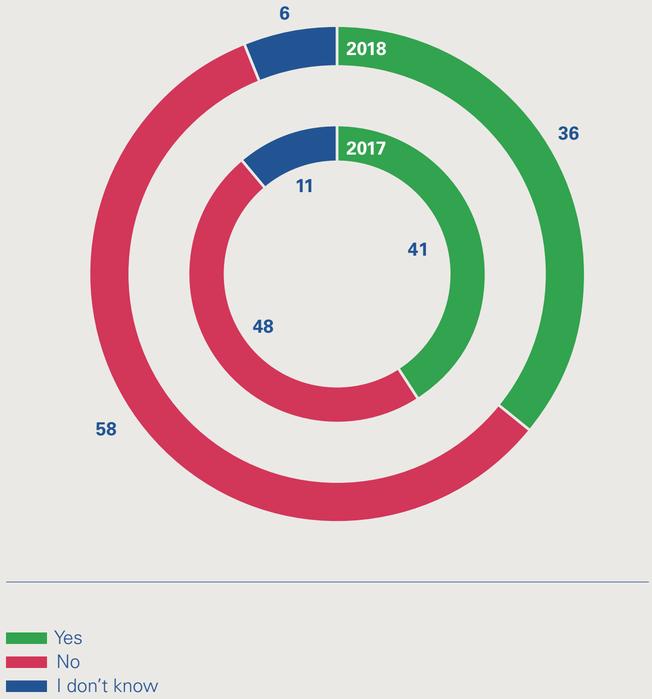
Cloud services are a crucial and rapidly growing element of how we work. Not only do they provide access to latest technologies such as Artificial Intelligence, they are also of enormous help in making businesses more agile – meaning businesses can interact with each other and their customers more simply and swiftly.

However, respondents seem to be undecided if cloud services are sufficiently secure. Fifty-six percent believe cloud services imply a privacy risk. On the positive side, 60% think that the situation regarding cyber risks associated with cloud services has improved in the past few years.

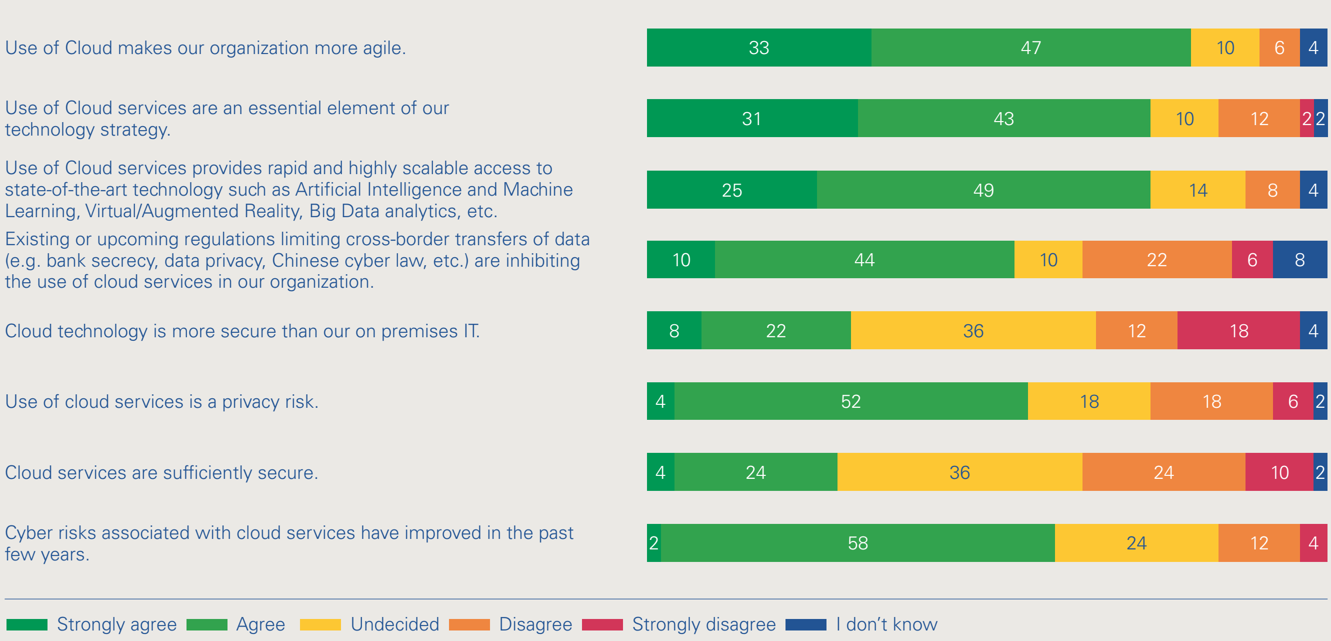
Do you have an overview of all Internet of Things (IoT) and operational technology (OT) devices deployed in your company? (in percent)



Does your cyber security strategy and policy include Internet of Things (IoT) or operational technology (OT) assets? (in percent)



Cloud services have matured over the past few years. What is your opinion on the following statements (in percent)



Combining trust with ethics to protect society

Emerging technologies have consequences far beyond processes and technical capabilities. They reach deep into issues of trust and ethics. For example, the Internet of Things has generated significant discussion around the extent to which devices (or more accurately, the organizations supplying them and operating the underlying platforms) can hear, store and use what users do and say. Not to mention the dangers of larger scale infrastructure such as power plants being maliciously hacked to disrupt supply.

Society as a whole needs to agree on shared values – what is good and what is bad. And therefore what is acceptable as we move forward. This involves assessing new risks, including those beyond cyber security – such as the impacts on ethical design.

A number of bodies are looking at issues such as integrating societal values into technological systems. For instance, the Institute of Electrical and Electronics Engineers (IEEE) has just launched the second version of its Ethically Aligned Design guide. The document is intended to encourage developers to clearly incorporate ethical considerations into artificial intelligence in a way that prioritizes human wellbeing and values.

Such a move complements initiatives such as the Digital Geneva Convention. With the aim of protecting civilians in times of peace against the effects of state-sponsored attacks, it is an important step towards protecting us all in cyberspace. The need for such protection is particularly acute given the rise in cyber attacks that impact organizations and individuals alike. As the online world reaches into every corner of our lives, from education to healthcare, more robust safeguards are a necessity.

In terms of individual firms' business and operating models, the overarching consideration must be how to provide a secure and trusted environment for companies, customers, investors and others along the value chain. This involves collaborating and sharing insights between your organization and third parties to ensure your entire ecosystem is resilient.

Third party risks: addressing your entire value chain

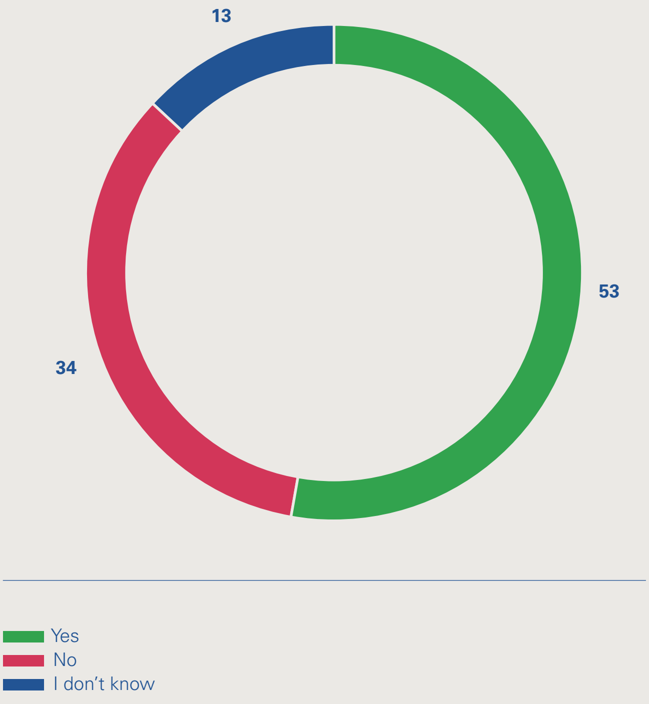
As the world becomes more hyper-connected, businesses are building strength on the basis of their ecosystem, collaborating and leveraging the respective strengths of third parties in their value chain. These business ecosystems are becoming more complex and close knit, increasingly via open APIs.

The stakes of maintaining trusted interfaces are higher than ever, however. Increasingly close relationships mean that more and more risks are outside a company's direct control, and assets become more susceptible to attack. A resilient ecosystem is key.

But while the management of third party risks has grown in importance, figures from our survey give little peace of mind that Swiss businesses are actively addressing them: 44% of respondents say they have no instruments to enforce their control framework on suppliers. And 38% have no contractually agreed binding terms related to cyber risks.

The lack of a systematic approach to assessing and mitigating third party risks could be costly. Just one weak link can break the chain in a tight ecosystem. And the risks become even greater with possible reputational contamination as regulation and public scrutiny intensify.

Do you require specific cyber security measures in third-party contracts? (in percent)



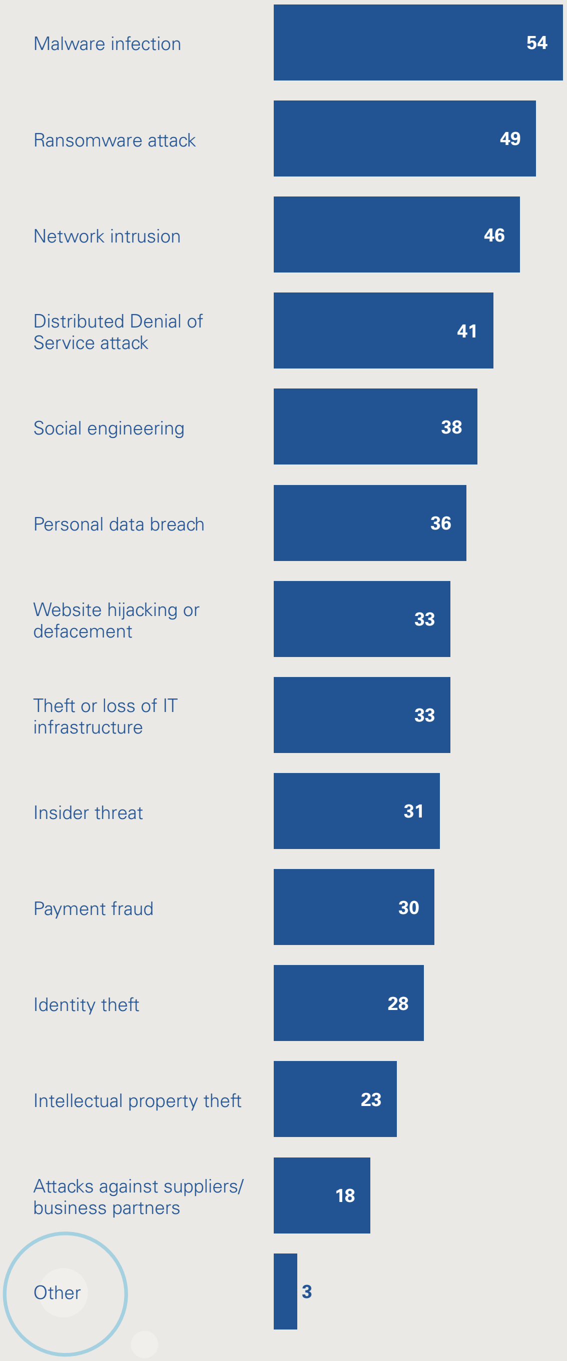
56%

of respondents believe the main issue in managing third party risks is insufficient transparency over the effectiveness of a supplier's control framework.

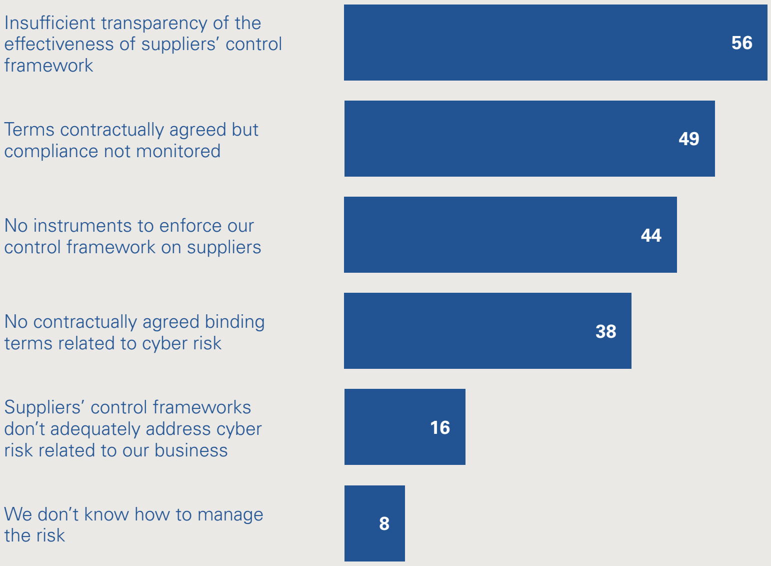
18%

of cyber response plans cover attacks against suppliers or business partners.

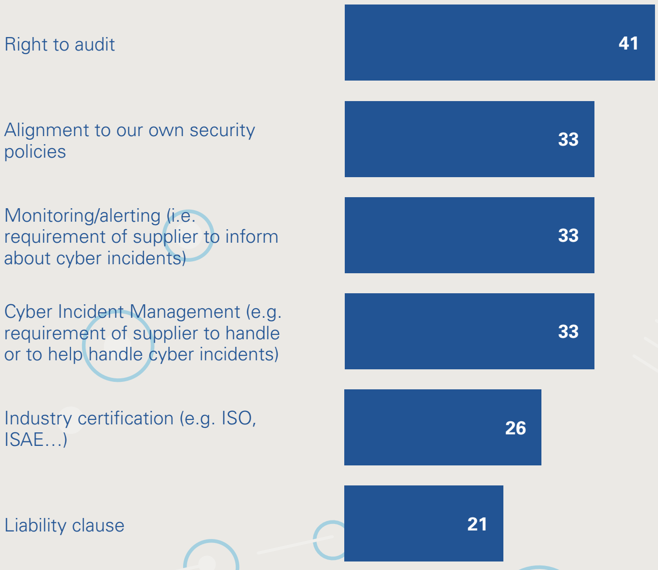
Which scenarios does your Cyber Incident Response Plan cover? (in percent)



In your opinion, what is the main issue related to managing third-party cyber risks? (in percent)



What cyber security measures do you require in third-party contracts? (in percent)



Cyber due diligence: achieving better investment decisions

Extensive financial and commercial due diligence has long been routine in the context of mergers and acquisitions. Acquiring a business without asking extensive questions about its financial performance, business plan, customer concentration risk or IT framework would be foolhardy. Yet, despite the risks it can pose, cyber security appears to be overlooked by the vast majority of Swiss businesses during a due diligence process.

> **In fact, only 23% of respondents say their company carries out specific cyber security evaluations as part of their due diligence when investing in another company or entering into a merger. It seems that investors are prepared to commit to corporate acquisitions without investigating what cyber risks the investment could expose them to.**

With data breaches and privacy issues attracting considerable scrutiny by the media and public, ensuring that potential risks are identified is an essential first step in mitigating those risks. The due diligence should cover matters such as the target business's cyber security framework and resilience. Crucially, questions should be asked not only about its internal resilience but also about how it addresses possible weaknesses in its value chain.

Put simply, cyber due diligence is critical to identifying potential pitfalls so that more informed investment decisions can be reached. Conversely, not undertaking cyber due diligence prior to investing in a business can prove costly in both financial and reputational terms – especially if there follows a breach of customer privacy and data.

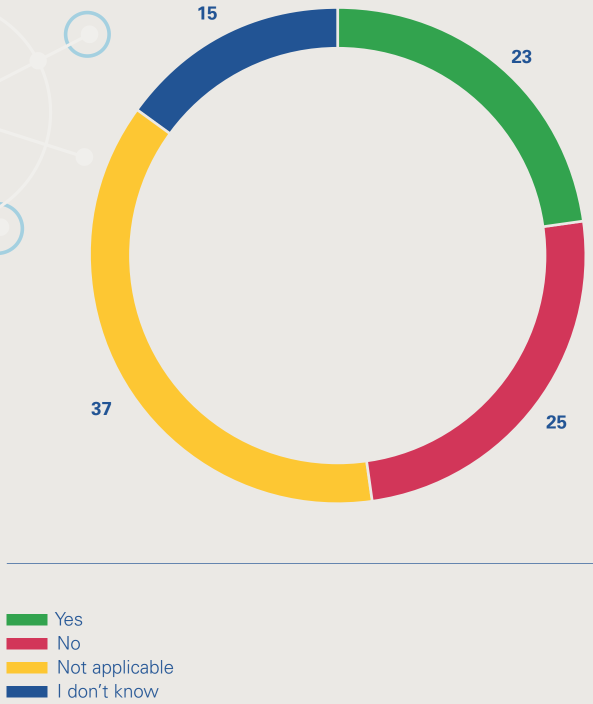
80%

of respondents say their board sees cyber security as an operational risk. But only

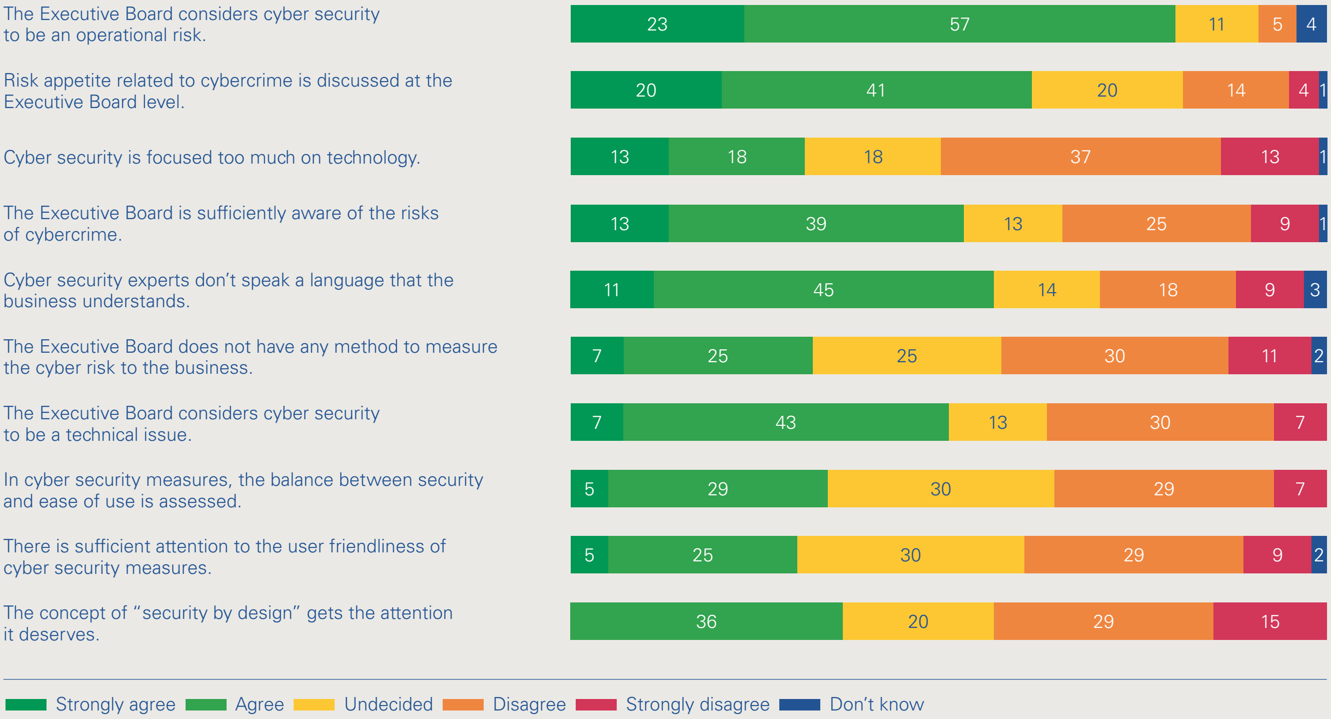
23%

carry out specific cyber security evaluations as part of their due diligence when investing in a business or entering into a merger.

When your company invests in another company or enters into a merger, does it systematically carry out specific cyber security evaluations as part of the due diligence? (in percent)



With which of the following statements do you agree? (in percent)



Digital ID: helping to deliver the benefits of digitalization

The famous internet meme went "On the internet, nobody knows you're a dog." Many years after this cartoon was first published in the New Yorker, the quest for a proper digital identity is still on. One could change the meme to: "On the blockchain, nobody knows you're a fridge". As we enter the next phase of hyper-connection, it is of paramount importance that we are able to verify the identity of both users and devices. Managing digital identities is the lifeline to sure interactions.

The concept of identity is not new, of course. We have historically used evolving credentials, from wax seals to passports, to verify who we are. The ways in which humans, devices and other entities interact in the digital economy requires up-to-date changes in how we manage identity. The original design of internet was not built on the concept of user identity. As a consequence, we must now deal with fragmented solutions and, in many cases, workarounds. The result is a low level of trust.

Re-establishing trust is essential for us to safely use services and participate in society. Identity is the first step in every transaction between parties. Transactions between two identities need a credential, and the verification and authentication of an identity. These steps have not changed over time. But the methods have.

We currently see many new – competing - concepts for digital identity. It is hard to predict which will gain most momentum in the market. Our survey shows that 69% of respondents believe that the digital ID is an important step towards secure and trusted digital interactions and would result in higher levels of trust. However, only one third thinks a digital ID is of strategic importance to their organization – and only one third plans to support digital ID in products and services.

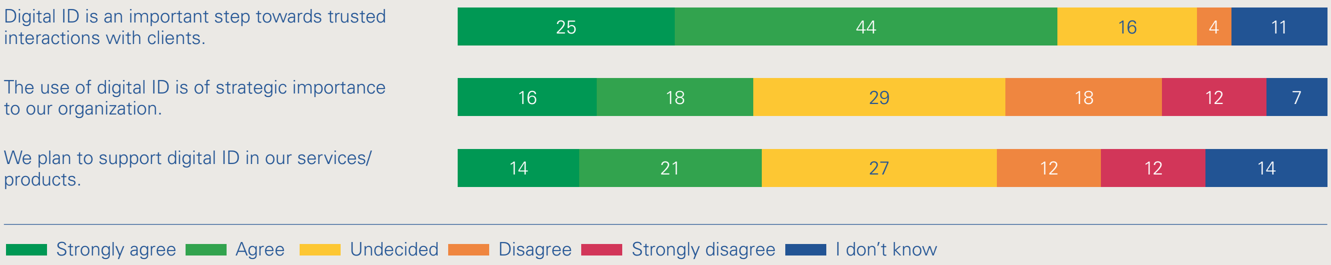
69%

of respondents see digital ID as an important step towards trusted interactions with customers. But only

35%

plan to incorporate digital ID into products or services.

What is your opinion on digital ID (the electronic equivalent of an individual's identity card)? (in percent)



Business success in the digital age

The stakes are high in today's fast changing economy. Organizations must deal with the challenge of creating and nurturing a secure and resilient environment for stakeholders. To this end, there are four critical success factors that should be addressed as a priority:

Emerging technologies

Artificial intelligence, the Internet of Things, blockchain… to name just three of the more prominent technologies. Each gives rise to new business potential. But also greater scope for cyber attacks. As business executives, you must ensure the robust management of your exposure to cyber risks if you are to benefit from emerging technologies. And put in place measures to mitigate the risks in your products, services and infrastructure.

Third parties

Resilience is not only an internal matter. With value chains being increasingly complex and interconnected, the reality is that you need to know whether one of your suppliers or business partners is exposed to cyber risk. A breach of security at a third party can have consequences for your own organization. Mitigation measures include knowing how you will collaborate with third parties to respond to a cyber incident.

Cyber due diligence

This is essential on any investment, acquisition or collaboration to identify possible weaknesses prior to your commitment. As with other aspects of due diligence, understanding the cyber risk of a target business can affect the enterprise value you attribute to it, and hence the purchase price. As well as avoiding unwelcome surprises following your investment.

Digital IDs

Customers expect their interactions with businesses to be seamless and secure, and the pressure for businesses to deliver will grow further. Robust, risk-based digital IDs are critical to achieving this. They foster trust in your systems and products, improving the customer experience and encouraging them to undertake more, higher value, transactions online.

By successfully bringing together plans and actions across these four areas, your business should achieve greater resilience, as well as generate further trust among your customers. Both are key enablers of your ability to deliver sustainable growth in this digital age.

Distribution of survey participants by sector

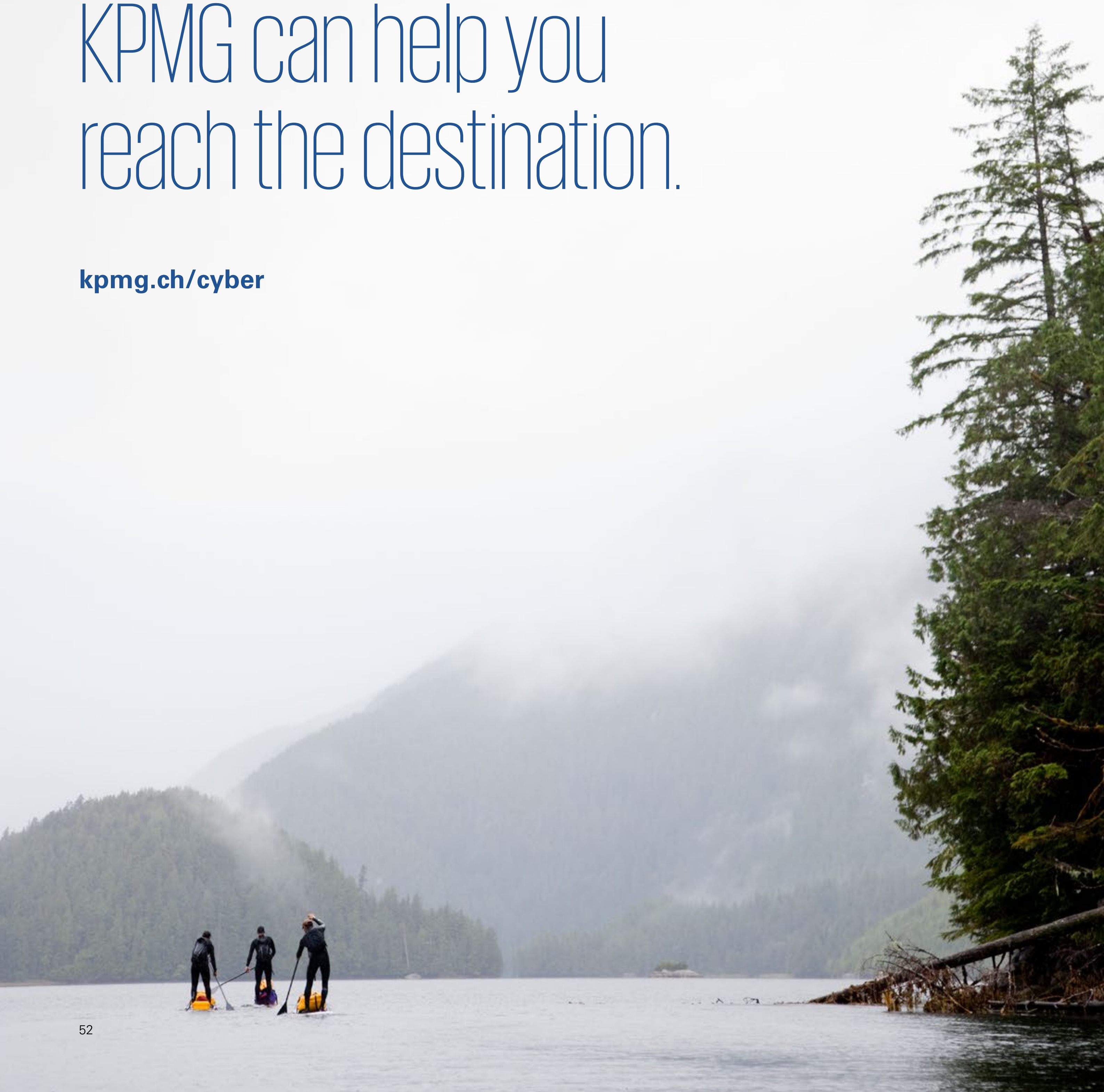
33%	Financial Services
5%	Professional Services
25%	Consumer/ Industrial Markets
3%	Communication/ Entertainment
13%	Energy and Natural Resources
2%	Infrastructure
12%	Government
7%	Other

Survey methodology

This study is based on a survey of 60 representatives of companies located in Switzerland. These include 26 large companies (those with headcount in excess of 5,000) and 34 small and mid-sized companies (those with headcount of 5,000 or less). The typical respondent profile was CISO, CIO or CTO. In addition, interviews on selected topics were conducted with subject matter experts at Microsoft, SwissSign, Partners Group, ETH Zurich, and Crypto Valley Association. The views of these interviewees, together with insights from KPMG, are reflected in the study. The survey and interviews were carried out by KPMG Switzerland between January 2018 and March 2018.

No matter where you're at your cyber security journey, KPMG can help you reach the destination.

kpmg.ch/cyber



KPMG's Cyber Security services

KPMG helps you understand, prioritize and manage your cyber security risks. Enabling you to take control of uncertainty, increase your agility, and turn risk into advantage.

Strategy & Governance

- Cyber strategy
- Cyber governance
- Cyber in the boardroom
- Cyber risk management
- Data privacy strategy
- Data privacy governance

Transformation

- (Customer) identity access management
- Security architecture
- Data privacy implementation and tooling
- Cloud/digital/mobile
- Education and awareness

Cyber Defense

- Red teaming
- Penetration testing
- Cyber scenario exercises
- Incident response
- Application security

Assessments & Assurance

- Cyber maturity assessment
- Data privacy assessment
- Third party cyber risks
- Anticipating emerging technology risks

Certifications

- Digital identity and qualified signatures (ZertES, eIDAS)
- e-Patient records systems (EPDG)
- e-Voting
- Data privacy (VDSZ)
- ISO 27001

(Industrial) IoT Cyber Security

1f yOu c4n r34d 7h15 yOu 5hOuld 4pply fOr 4 jOb w17h KPM6!

kpmg.ch/cyberjobs

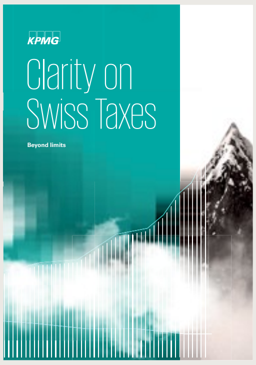
THInKER

PINBOARD

"Clarity on" publications

This series of publications from KPMG Switzerland provides insights, analyses and studies on a range of topics. All publications are available online. For more information, please contact **kpmgpublications@kpmg.com**

Latest issues

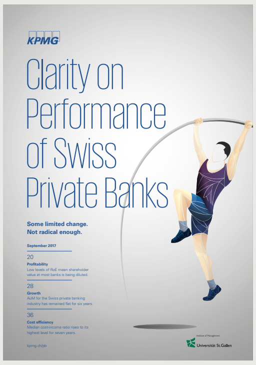


Clarity on
Swiss Taxes

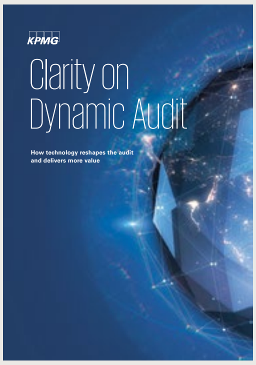
KPMG
Clarity on Mergers & Acquisitions
The growing appetite of Swiss dealmakers

Clarity on
Mergers & Acquisitions

Clarity on
Digital Labor


KPMG
Clarity on Performance of Swiss Private Banks
Some limited change. Not radical enough.

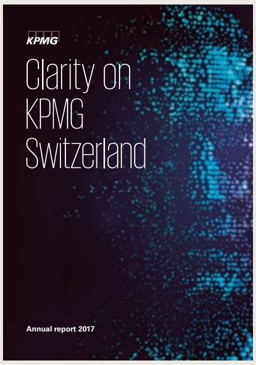
Clarity on
Performance of Swiss Private Banks



Clarity on
Dynamic Audit

KPMG
Clarity on Insurance Digitalization
Achieving agility: Towards a new business model

Clarity on
Insurance Digitalization



Clarity on
KPMG Switzerland

Clarity on
kpmg.ch/clarity-on

KPMG Knowledge App

Get instant access to our experts' knowledge with our KPMG Knowledge App for iPad, iPhone and Android phone.

Download on the App Store

GET IT ON Google Play

CONTACTS & IMPRINT

For further information on
Clarity on Cyber Security
please contact:

Matthias Bossardt
Partner,
Head of Cyber Security
+41 58 249 36 98
mbossardt@kpmg.com

Thomas Bolliger
Partner, Head of Information
Governance and Compliance
+41 58 249 28 13
tbolliger@kpmg.com

Nico van der Beken
Partner, Forensic Technology
and Cyber Response
+41 58 249 75 76
nvanderbeken@kpmg.com

Publisher
KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich
+41 58 249 31 31
kpmgpublications@kpmg.com

Study and editorial team KPMG
Matthias Bossardt
Yves Bohren
Michele Daryanani
Michael Nordhoff

Concept and design
Sabine Lorencez, KPMG
Andi Portmann, Grafikagentur konkret

Print
PrintCenter Hergiswil

Pictures
Shutterstock
iStock
Getty Images
[Page 30–33]
© ETH Zürich / Alessandro Della Bella

Illustrations
[Page 1]
van Beusekom design & brand solution

FSC
www.fsc.org
MIX
From responsible sources
FSC® C010670

PERFORMANCE
myclimate
neutral
printed matter
No. 01-14-569853 – www.myclimate.org
© myclimate – The Climate Protection Partnership

Articles may only be republished with written permission from the publisher and by quoting the source "KPMG's Clarity on Cyber Security".

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

→ **Clarity on Cyber Security**
kpmg.ch/cyber