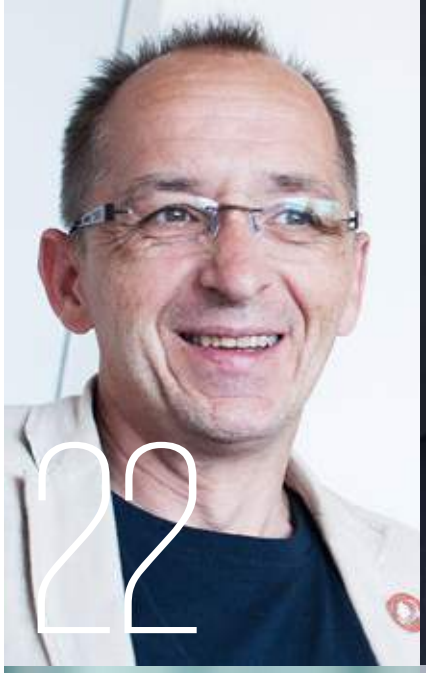
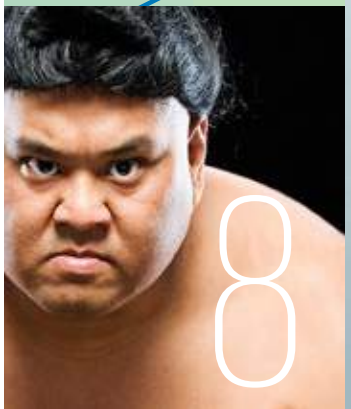
Clarity on Cyber Security

Never a dull moment

May 2016





CONTENT

Clarity on Cyber Security

While classic cyber security challenges have not yet been mastered, new ones are emerging on the horizon.

EDITORIAL

Never a dull moment

Matthias Bossardt
Partner, Head of Cyber Security

Gerben Schreurs
Partner, Cyber Security

In 2015 we published our first Clarity on Cyber Security in Switzerland. Our objective was to get insights on the state of Cyber Security in Switzerland and to share these insights with our stakeholders. Based on the response and the media exposure, we seem to have hit the right spot with this study. As a consequence, we decided to continue our research in this area in 2016, as we believe that the domain of Cyber Security is evolving at a rapid pace. This year's Clarity on Cyber Security shows that a number of "classic" challenges in Cyber Security are still valid, although a range of new challenges are emerging on the horizon. In fact, the challenges continue to evolve rapidly. One cannot afford to become complacent – the next step must be anticipated. That's why we chose "Never a dull moment" as the title. You will find our takeaways on both the "classic" and new issues in the following chapters.

We hope that you will be inspired by our findings on the state of cyber in Switzerland, the views of opinion leaders and our own experiences. It goes without saying that we're more than happy to deepen the dialog on this theme, which is so vital for business success in a rapidly transforming society.

Matthias Bossardt

Gerben Schreurs

Two speeds in Switzerland – outrider and late starter

A number of Swiss organizations manage to at least keep up with the speed of the evolving threat landscape. The most advanced succeed in reducing the risk and leverage cyber to enable new business and operating models (for instance digitalization). Others struggle to keep up with the rapidly evolving threat landscape. They won't be able to develop their business into Industry 4.0.


60
5
10
50
40
20
30
50
10
45
0,2 s
15
40
20
35
30
25

Build networks, break down silos

Attackers operate in ever changing networks and coalitions that disseminate knowledge at high speed. Organizations must do the same to be well prepared. Seamless cooperation and knowledge exchange with peers and within the security industry become a business imperative.

Know thy enemy

An understanding of the motivation, intent, strategy, tactics and the tools of the attackers is critical in order to anticipate threats and effectively prepare for, prevent, detect and respond to attacks. Bespoke correlation of technical and non-technical information is a must. Practice shows that few organizations have understood how to distill the relevant intelligence from the myriad information feeds available in and outside their organization.

Fourth industrial revolution raises the stakes

The Internet of Things grows with exponential pace and leads us to a new reality where Cyber Security directly affects the resilience of our organizations, our economy and our individual health and safety. A reality in which Cyber Security is no longer confined to cyber space but also comprises our physical world.


PACEMAKER

Business as usual

54%

suffered from a cyber attack in the past 12 months, of which 44% had to deal with disruption of business processes. Malicious software, social engineering and phishing are the most usual methods.

Working on response capabilities

60% have a cyber response plan, and they tend to be satisfied with the effectiveness, resources and know-how in this domain (2015: 55%). 82% of them normally review this plan as part of their yearly review cycle.

Insider threat

80% of respondents do not have a proper insider threat management program; in particular, they do not have technical monitoring of suspicious activities (named by 60%), appropriate data classification (51%) and multidisciplinary coordination (49%).

Third-party risks

93% of FS institutions require right to audit, and 65% of NON-FS institutions require right to audit in third-party contracts.

100% of NON-FS institutions require third parties to notify cyber incidents, while 79% of FS institutions insist on it.

33% of FS institutions report that understanding, visibility and control of Cyber Security has worsened when outsourcing to third parties, while only 8% of NON-FS institutions report this.

Key Findings

Join forces

95% were looking for more cooperation in 2015. One year later, 66% say that they have actually done that. Sharing threat intelligence (named by 88%), sharing lessons learned (83%) and sharing preventive measures (78%) are the most common goals of collaboration.

Perception of cloud

81% of FS institution respondents believe that leveraging cloud technology will not reduce security while only

46% of NON-FS institutions state the same.

The 4th industrial revolution challenge

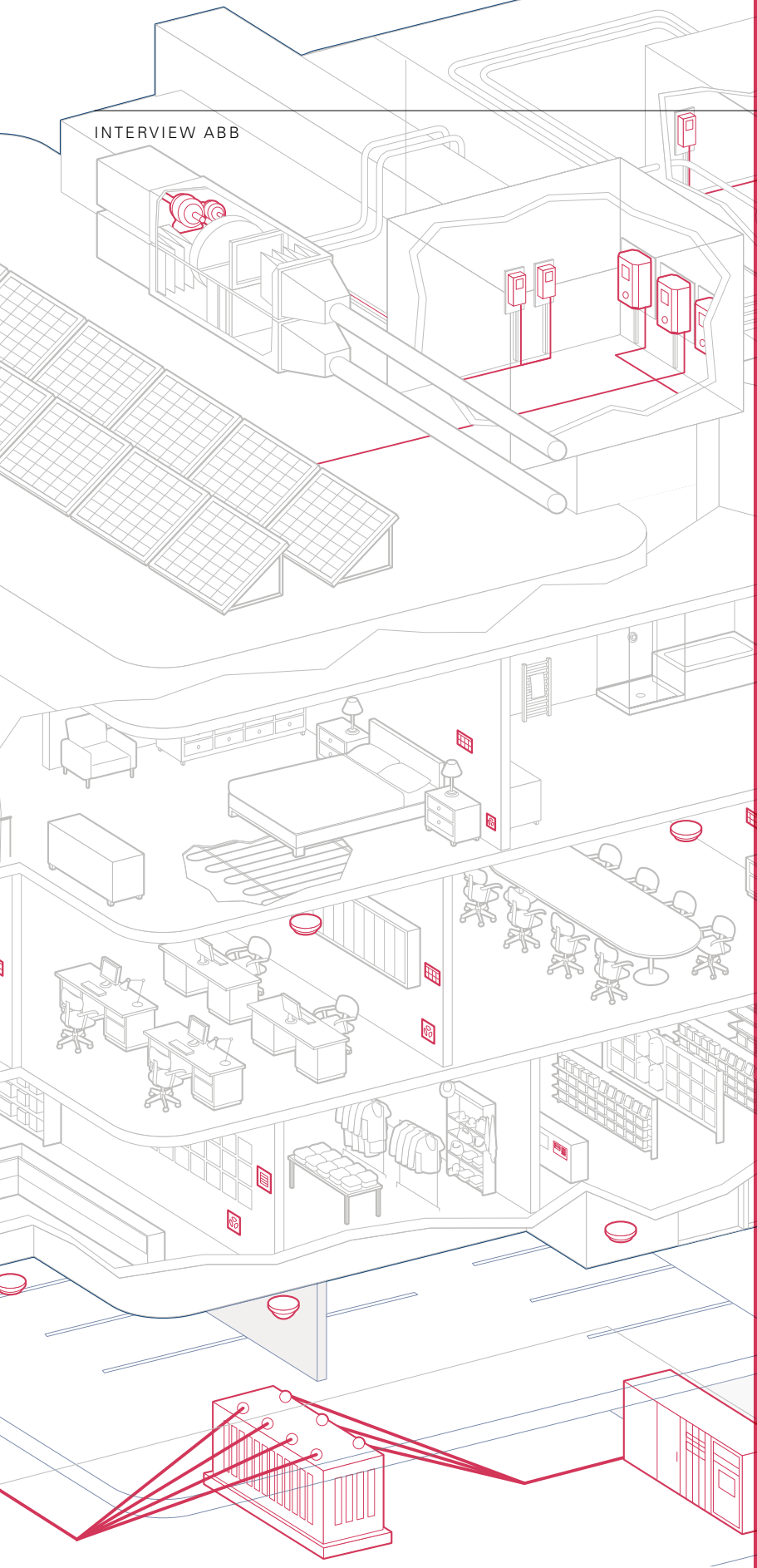
53% do not have an overview of Internet of Things devices. Approximately one third of respondents that say the Internet of Things is relevant to them do not leverage the concept of security by design.

Lack of insight

38% do not have any method of measuring cyber risk, which is a slight deterioration compared with 2015 (44%). Awareness of the damage significantly improved: 17% of large companies lack insight into the damage caused by cyber attacks (2015: 50%).

The "Internet of Things" is really about services and people

Markus Braendle is Group Head of Cyber Security for ABB. Reliable and secure digital interfaces between industrial components and installations have been an important part of ABB's business for many years. The goal of Braendle's team is to ensure that ABB's offerings support customers' Cyber Security needs. He makes a strong argument that we should not promote security for the sake of avoiding painful incidents but should instead focus on the business value that secure products and services can offer.



The challenge is to talk about the business value of Cyber Security ...

KPMG *There is very little doubt that security will play a vital role in the "Internet of Things", a world where nearly everything will be interconnected and where the physical world will increasingly merge with the digital domain. The million-dollar question is: How do we make sure that this new reality – often cited as the fourth industrial revolution – is reliable and secure?*

Markus Braendle First of all, at ABB we don't talk about the "Internet of Things". We talk about the "internet of things, services and people". Because that's what it's basically about. Connecting stuff to the internet is a means to an end – what really matters is what you do with it. We also think that the fourth industrial revolution is an evolution rather than a revolution. The degree of interconnectedness has been increasing for many years now. Having said that, of course it's undoubtedly essential to guarantee security in this domain. I am convinced that, in order to achieve security in this new and highly complex environment, we must not focus too much on security's technological side. There's a wealth of technological solutions around and a large part of this has, in fact, become a commodity. I believe that the real challenge lies in making sure that Cyber Security becomes a seamless part of the risk management approach and earns its place in the hearts and minds of companies' management teams.

Awareness doesn't really seem to be a problem nowadays, with numerous incidents being widely reported in the media. How can we ensure that this awareness translates into the effective mitigation of cyber risk?

Generally speaking, many organizations and their management teams still largely base their Cyber Security investments on a fear of incidents. This often results in ad hoc budgeting and, more importantly, is not a very effective approach. The challenge lies in talking about the business value of Cyber Security instead of merely responding to incidents and new threats. Business leaders should be aware that a very interesting new dynamic full of opportunities is emerging and should ask themselves how they can get the most out of it in a controlled manner. How can they increase customer value and customer satisfaction by offering cyber-secure products and services? For instance, by maximizing uptime or by improving the efficiency of maintenance programs. When it comes to Cyber Security, however, we traditionally tend to talk in technical lingo. We must translate that into business lingo.

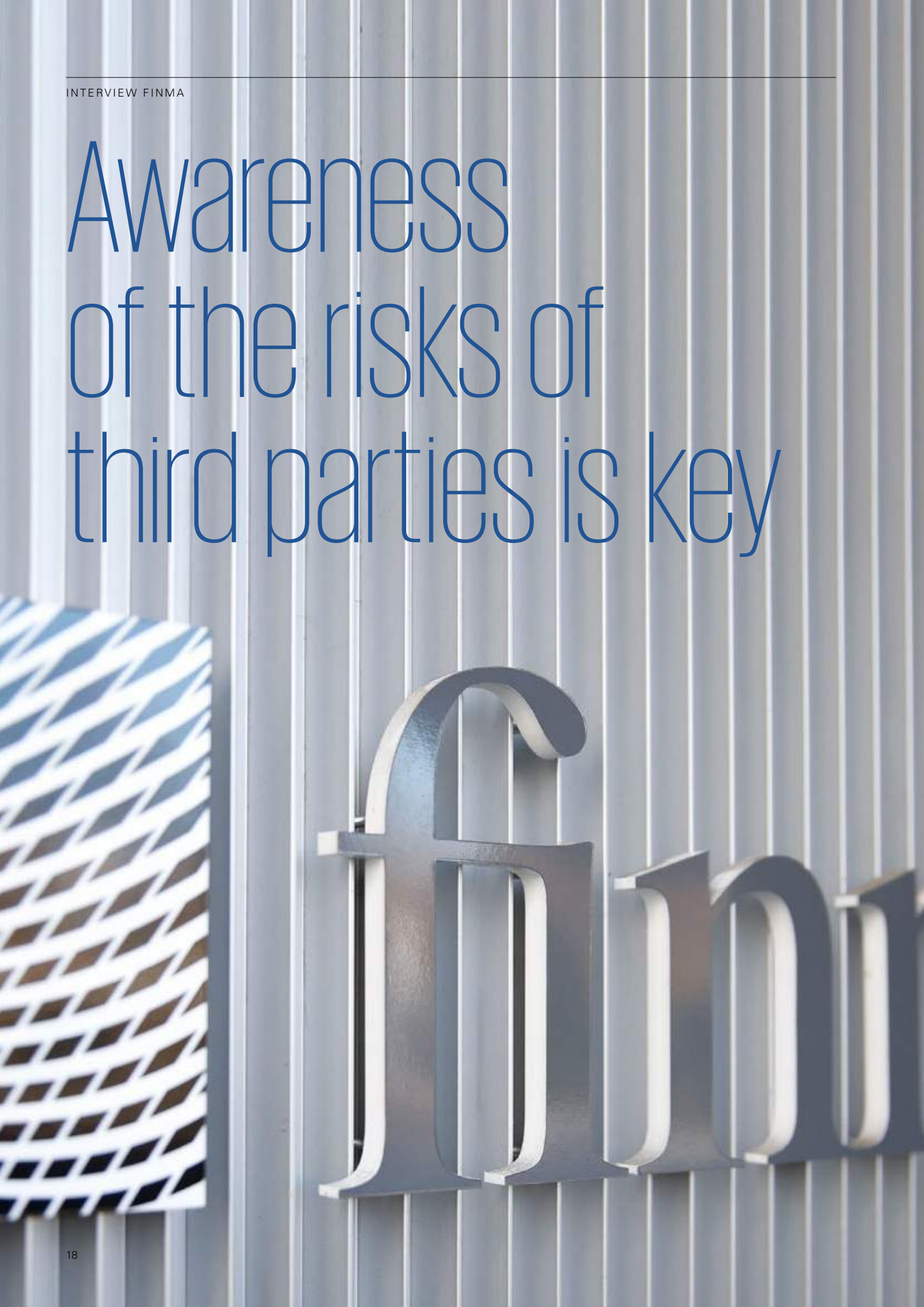
This technical, incident-driven approach has been a problem for a number of years now. How optimistic are you about changing this?

The Cyber Security strategy in some companies is largely driven by compliance, while others are driven more by the value that's at stake. It's a heterogeneous landscape, but overall I really do see some good progress in the dialogs that we're having with the market. It's important that we work together with third parties such as KPMG to jointly communicate this message. Speaking more generally, I think that collaboration is key to dealing with this issue effectively. MELANI is doing a good job in bringing industries together, but I think we should do more to engage in dialog with the security providers and the consulting companies. It's all about trust, of course, and also about understanding each other's world.

What exactly do you mean by that?

I'll give you an example. When we work on a project for a customer, their investment often covers a timeframe of 20 years. This is quite a contrast with IT providers, who often have a horizon of just a couple of years. So if we're using IT in these projects, we must have a dialog upfront on how we ensure fully supported IT components during the whole lifetime. This is one important prerequisite for enabling 'security by design'. In this interconnected world, seamless cooperation with third parties is increasingly important. This goes beyond simply having clear agreements in contracts – partners also need trust in the relationship. That's why we engage in dialog with them – in a continuous dialog to make sure that we share the same goals, develop a good relationship and are ready to act swiftly when needed.

Awareness of the risks of third parties is key



Michael Schoch, Head Banks division and member of the Executive Board of the Swiss Financial Market Supervisory Authority FINMA. He shares his views on how Swiss financial institutions should prepare themselves in the cyber domain.

Swiss banks should take the necessary technological measures to ensure the security of their IT infrastructure and the integrity and confidentiality of their data.

KPMG *The theme of Cyber Security has been around for a while. What do you consider to be important new trends?*
Michael Schoch The trend towards digitization of business processes continues in the Swiss banking sector and the innovation power of the fintech sector further contributes to this. One example is the domain of asset management, where Robo Advisors play an increasing role in investment processes. In addition, digital identification or "block chain" technology offer banks new opportunities to adapt their value chain. Furthermore, as a regulatory body, we have a keen interest in the outsourcing of key business processes such as payment and securities settlement to third parties or the use of external data centers. Cloud solutions also bring new challenges for Swiss banks. One of the important requirements is that banks should meet the regulatory requirements for data protection. The combination of these trends leads to additional cyber risks that need to be mitigated.

Which domains of Cyber Security should get more attention?
Banks must be able to effectively ward off cyber attacks. The revised guidelines for operational risk (FINMA circular 2008/21 "Operational risks at banks – partial revision") contain new principles for Swiss banks on how to deal with IT and cyber risks. In general, dealing with cyber risks requires systematic measures and calls for enhanced cooperation by banks, beyond the borders of their own banking institution. This takes place with federal agencies such as MELANI and also with companies that specialize in cyber defense. In addition, it is necessary to perform regular tests on the resilience of their institute against cyber attacks, by hiring external specialists who can analyze the vulnerability based on "penetration testing". In general, banks must prepare for increasingly complex cyber attacks, attacks that may extend over several weeks or months.

Would you agree that Cyber Security is still mainly driven by a technical approach and that we need to change that?
Basically, we see two things. On the one hand, banks indeed take technological measures to mitigate the threat from cyber attacks. On the other hand, they also take measures to increase awareness. Most banks in Switzerland actively communicate with their employees and customers on cyber risks. In our view, this should be done particularly when there is a risk of social engineering. This technique uses sophisticated methods that not only focus on the bank customers, but also on the bank employees. The perception of these employees is often that they operate in a very secure infrastructure. Furthermore, we also believe that awareness of the cyber risks associated with external service providers is key. These providers increasingly serve as an entry point for attacks on the ultimate goal, the banking institution.

Do you agree that your organization is more driven by compliance than security?
Indeed, FINMA in its supervisory activities focuses on compliance with the regulatory requirements. These are principle-based requirements for dealing with cyber risks. Keywords in this regard are governance, risk identification, system protection, detection and response to cyber attacks and recovery measures. On this basis, Swiss banks should take the necessary technological measures to ensure the security of their IT infrastructure and the integrity and confidentiality of their data. The implementation of the concrete measures is a responsibility of each banking institution. The measures taken should be tailor made to the institution, so may differ from case to case. The review of the effectiveness of the technological solutions is a responsibility of the banks and a supervisory authority may verify this via "penetration testing".

Extortion is the name of the current game in cybercrime

MELANI, the Reporting and Analysis Centre for Information Assurance, contributes to the protection of critical national infrastructure by collecting and sharing insights on the evolving nature of cyber attacks.
The interview with representative **Max Klaus** took place one day after Switzerland was surprised by a DDos attack that simultaneously took down nine reputed webshops. At that moment, the motives and background of the attackers were unclear.

If you have enough money to rent large botnets, you can take any website down.

KPMG *You have been engaged with MELANI for eight years now. With that background, what relevant trends do you see in cybercrime?*
Max Klaus The nature of the attacks is continuously evolving. One overarching trend is that the level of professionalism on the attacker's side is increasing. The recent DDos attacks on Swiss webshops are just one example of that. The attackers have been able to deploy enough botnet power to take down websites of both small and large organizations. Mostly, it's just a matter of money. If you have enough money to rent large botnets, you can take any website down.

Having said that, this case also proves that the level of predictability is practically zero in the domain of Cyber Security. Usually, the people behind a DDos attack demand that a certain amount of Bitcoin be paid into their account. But we haven't seen that kind of extortion so far. In another recent case, it was just the other way around. Banks were asked by Armada Collective to pay money and if they didn't, the criminals would start an attack. However, the attack never took place. All this demonstrates that the behavior of the criminals – a very varied group, ranging from script kiddies to organised groups – is very hard to predict.

The attacks surely were a wake-up call for Switzerland, as it has never before happened on this scale. What is your advice?
As to extortion, we are always very clear in our advice. Don't pay. The argument behind this is obvious: giving in to extortion will ignite more cases of extortion as criminals will spread the word that crime pays. Apart from that, we have a range of advice on how organizations can best prepare for cyber attacks and twice a year we give insights in how the landscape of cyber threats evolves. However, I keep stressing the fact that a decent Cyber Security strategy is not only about an assessment of criminals' methods. It starts with an awareness of what's at stake in your organization.

What exactly do you mean by that?
Many companies are focused on implementing tools and techniques, but that is just one aspect of a Cyber Security strategy. You have to know what assets are of key importance for the continuity of your daily processes. Once you know that, you can get more focus on what to do to effectively deal with the threats. I'm afraid that many organizations in fact lack that insight. One example of that is that Switzerland has many smaller businesses that develop new innovative products and services. Often, they don't fully realize that their intellectual property is at stake. The larger companies are more aware of that.

Your organization operates in the heart of this domain. What can you contribute to an effective defense?
We believe that sharing insights is vital for Cyber Security. Apart from our publicly available reports on the attacks, we also see much value in bringing organizations together to share insights that are not meant to go public. With our partners in the financial industry, this has proven to be very useful. There is a great level of trust to communicate on issues such as new strategies for phishing, which continues to be an important topic. In other sectors, there is definitely room for improvement. We need to nurture trust to stimulate an open culture, which I believe will contribute to better security.

start

With the why

Florian Widmer is Head of Information Risk and Project Risk at Zurich Insurance. In this interview, he shares his views on the importance of business adoption, the dilemmas in collaboration and the inevitable shift towards the fourth industrial revolution.

The starting point should be to get a clear view on what's at risk in your organisation and to develop an understanding of who might attack what for what reasons and how sophisticated their capabilities are. In other words: it all starts with the why.

KPMG *From an overall perspective, which main trends do you distinguish in Cyber Security?*

Florian Widmer There are a wide variety of important trends to consider. These include digital transformation and the introduction and implementation of multi-sourcing strategies, which are amplifying cyber threats by increasing connectivity and creating new vectors of attack. The overarching trend is that attack methods are becoming increasingly sophisticated. This is of course nothing new, it has been going on for years. In fact, cyber attacks have become the norm. Organizations must assume that they are under constant threat of attack.

What is your view on how to deal with Cyber Security in a proper way?

Again, there are some basic assumptions that have been valid for many years. One of them is that we need a balanced approach with regard to protection, detection and response capabilities. That's merely the basics. In my view, it is essential to look beyond technology. The major Cyber Security challenge for most organization lies in the way in which technology is adopted into business processes and changing human behaviours. This is reflected in numerous studies into the root causes of cyber incidents, which show that the vast majority of incidents are not caused by technology failings but rather by poor processes and human error. The starting point should be to get a clear view on what's at risk in your organisation and to develop an understanding of who might attack what for what reasons and how sophisticated their capabilities are. In other words: it all starts with the why. Factoring this in, you then need to develop a cyber-risk strategy based on the dynamics of your business and operating model, your business strategy, and your risk appetite.

Another related key point is that the IT department should not be the sole owner and driver of Cyber Security. It is the responsibility of the whole organisation. Of course you need specialised officers with state-of-the-art knowledge of technology and risk, but you also need professionals that know how to communicate with the business and who at least have a good understanding of what's going on in operations. That is a prerequisite for business adoption of Cyber Security.

One of the outcomes of our survey is that collaboration has increased. Do you recognise that trend?

There is no doubt that collaboration between organizations and institutions is important. Sharing insights across industries can only help businesses prepare for attacks and improve the collective threat intelligence, which is an important aspect of cyber resilience. Having said that, I feel that there's definitely room for improvement when it comes to sharing insights. Solutions based on trust among peers are good, but not sufficient as these are not scalable. We need anonymized "loss" databases to get a comprehensive understanding of risk.

More specifically the insurance sector is piloting initiatives to exchange data on claims resulting from cyber attacks, including data on the root causes and the financial consequences. The use of a central clearing house ensures that data remains anonymous and contributes to better insights into this relatively new area. Right now, there is a lack of sufficient data and a lack of appropriate risk models, which are critical requirements for developing insurance products in this area. The better the industry can assess risks, the better it can service customers with insurance products and also with advice on how to avoid or respond to incidents.

To conclude. The World Economic Forum recently pointed out the consequences of the so called Fourth Industrial Revolution, which is being fuelled by factors such as the Internet of Things and the rise of artificial intelligence. How does this affect Cyber Security?

That's a big question. Looking at it from a distance, we can distinguish two major trends. One is that business processes are becoming more tightly coupled, primarily due to robotic process automation. The other is that we are moving from linear to complex, interconnected interactions. For example, it is estimated that a considerable volume of transactions and content authoring will be conducted by autonomous software robots within a couple of years. That means that in terms of Cyber Security we will have a reduced tolerance for system failure and processing errors. The effect of an incident is simply bigger. As a consequence, Cyber Security will be imperative to success in the fourth industrial revolution.

CHAPTER 1

Basic principles

What is so special about Cyber Security? Nothing, in fact. Cyber Security was once an exotic topic when the internet landscape was still its infancy stage. Cyber attacks have become commonplace. And now as the connected world matures, the topic of securing digital assets and infrastructure has become not only essential for success, but should have turned into a routine process. Cyber Security should now be business as usual. But it isn't.

More than ever, Cyber Security is a prerequisite for business success

No one can ignore Cyber Security

The results of this year's survey on the state of Cyber Security in Switzerland is proof that this is indeed the case. One of the interviewees put it very clearly: "Everyone is under attack, or will be soon." Approximately half of the respondents say that their organization has experienced a cyber attack in the past 12 months. In almost half of these cases, organizations suffered from a business disruption after these attacks, and one quarter feel that the events caused reputational damage. Taking these figures into account, there can be no doubt about it: business leaders must ensure that their organization has a flawless Cyber Security programme in place. This is of course nothing new and has been the case for many years now. Having said that, it is also clear that this applies only to a limited number of companies who have been working on Cyber Security for many years already and who have truly embedded the theme in their business decisions. Nevertheless, mature organizations struggle with the rapidly evolving threat landscape. Less mature organizations risk being left behind as business and operating models evolve.

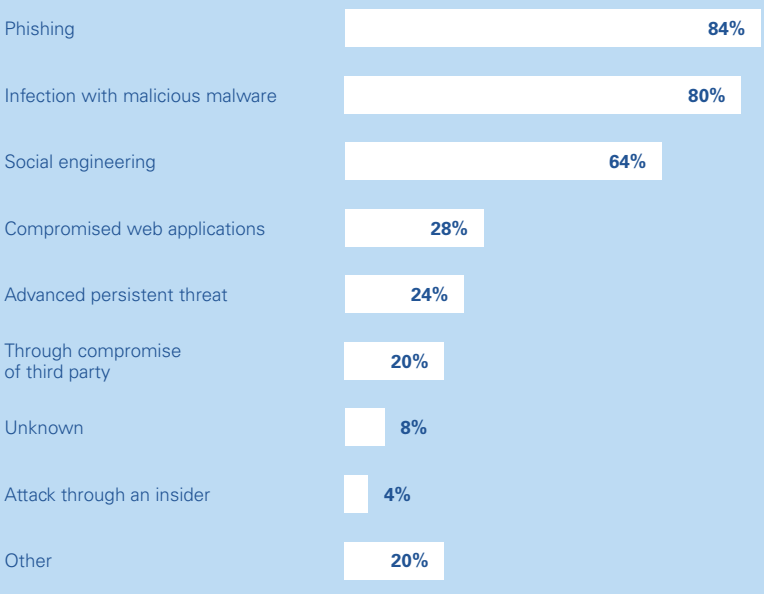
Swiss organizations step up efforts and start to see the bigger picture

Now that the topic has matured, we also see that some organizations have stepped up their efforts and become more professional in their Cyber Security programmes. One of the basic assumptions of Cyber Security is that organizations shouldn't base their efforts on fear of incidents and/or media reports, although this may be tempting in times of turbulence. Rather, they should focus on reaching their own strategic goals and subsequently manage the risks based on three pillars: to protect, to detect and to respond. Again, the survey indicates that Swiss organizations are doing quite well in this respect. Some companies are left behind, while others struggle to keep up with the evolving landscape. Overall, the sense of urgency has further increased and it is promising to note that 75% agree that the Executive Board perceives Cyber Security as an operational risk, although we are just as surprised by the fact that the remaining 25% obviously don't.

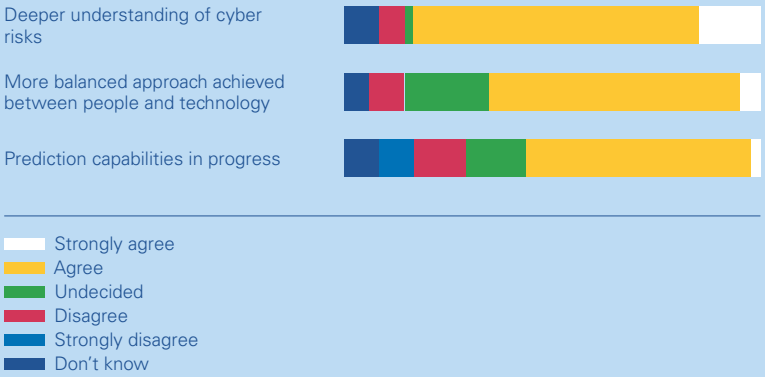
Interestingly, our correlation analysis shows that companies who consider Cyber Security as an operational risk tend to increase the budgets. One-third increased by more than 20% compared with the previous year.

The implication for Security Officers is clear: if they succeed in communicating the cyber risksproperly, they will obtain more resources.

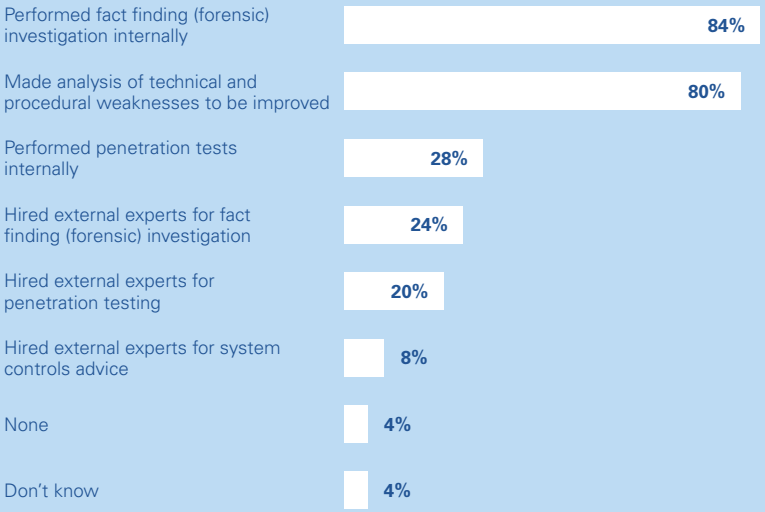
What was the nature of attack(s) that your organization experienced?



Can you confirm improvement from a Cyber Security point of view within the last 12 months on the following topics?



Which measures have you taken directly following the cyber attack(s)?



This recognition paves the way for the proper approach to include cyber risk in the overall risk management processes. More companies have a response plan in place. In 2015, 45% didn't have one; in 2016 this figure has dropped to 36%. Also, a vast majority (84%) indicates that their organization has reached a deeper understanding of cyber risks in the past 12 months. A remarkable development in this area is that response statistics from the financial services sector indicate a robust improvement, while others have remained on the same level.

Overall it is fair to say that at least some Swiss companies seem to be more aware of the bigger picture. Quoting the American author James Thurber: "Let us not look back in anger, or forward in fear, but around in awareness".

54%
have experienced a cyber attack in the past 12 months

75%
agree that the Executive Board perceives Cyber Security as an operational risk

36%
do not have a response plan in place

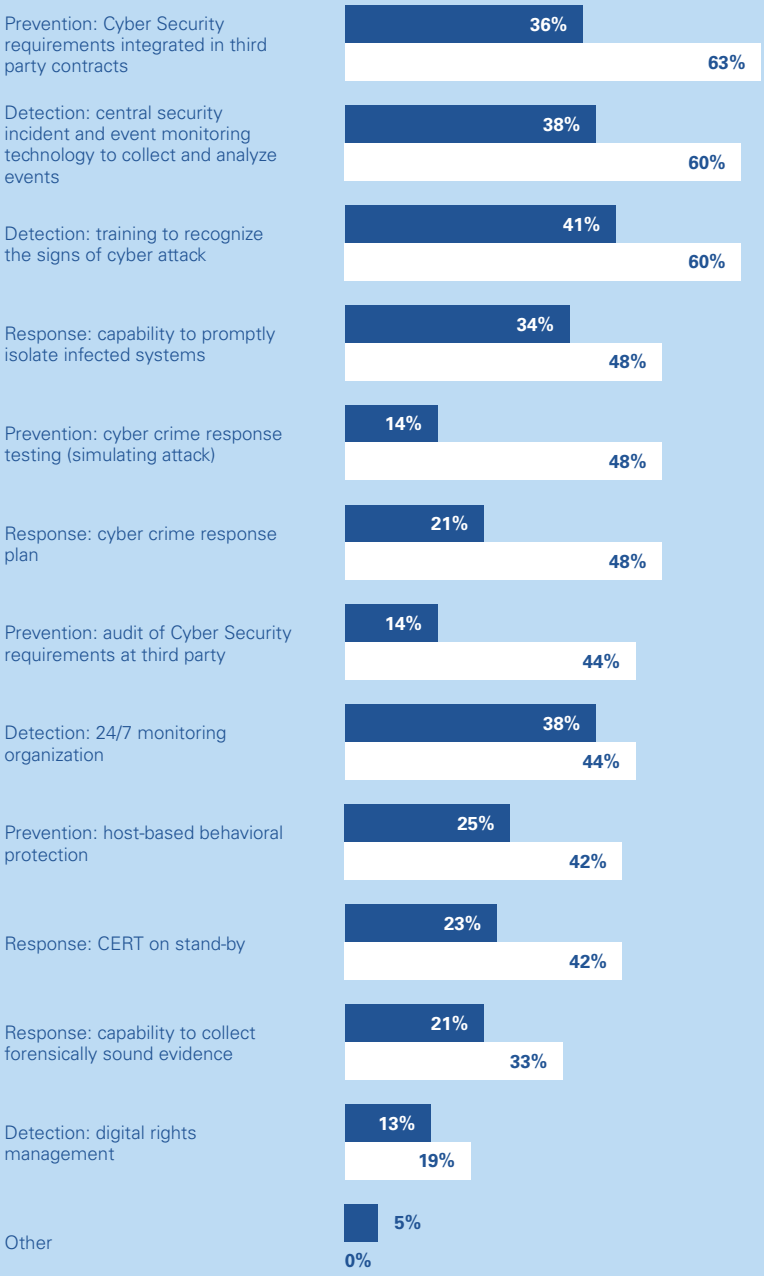
84%
indicate that their organization has reached a deeper understanding in the past 12 months

64%
agree that their organization has adopted a more balanced approach between people and technology in the past 12 months

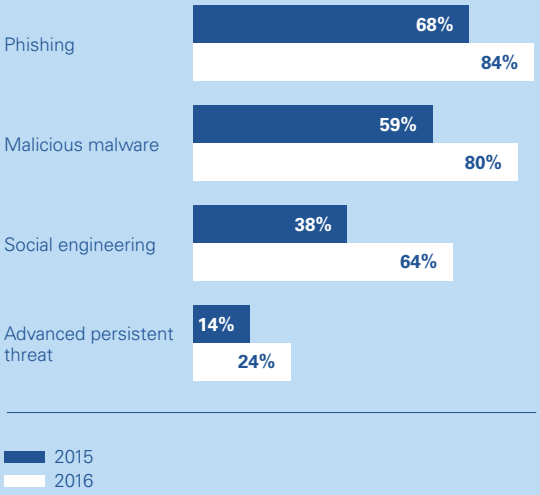
64%
of the respondents were targets of social engineering attacks

48%
consider Cyber Security mainly as a technical issue

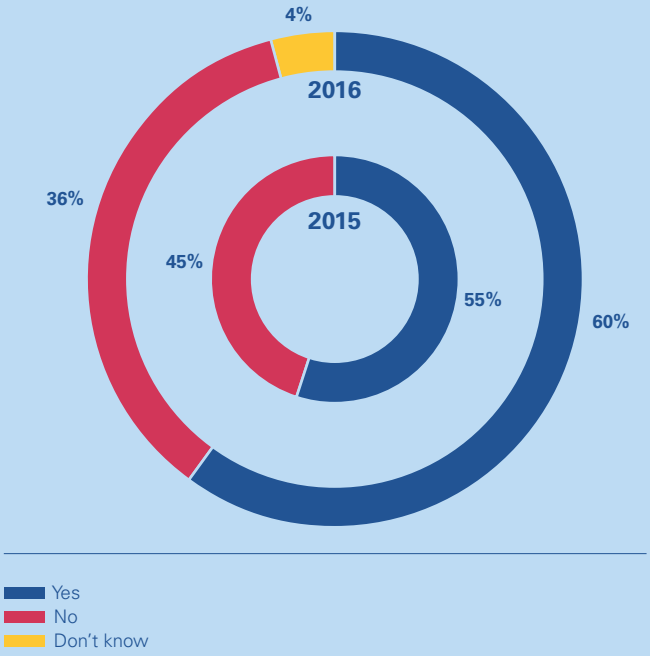
Which controls have you implemented in order to prevent, detect and respond to cyber attacks?



What was the nature of attacks that your organization experienced?



Does your organization have a cyber response plan?



Swiss organizations say they don't put all their bets on technology

Another almost classic problem in Cyber Security is that the technological perspective often dominates Cyber Security efforts. Although technological tools and solutions surely should play an important role in Cyber Security, these solutions will have the desired effect only when properly embedded in the organization. In our view, successful Cyber Security calls for a balanced approach between technology, people and processes. An indicator of this is the fact that the survey learns that two thirds of the respondents were attacked with social engineering (last year: 38%), which a reliance on technology only may not be a very wise strategy. On the one hand, there is a clear message from the respondents that organizations are moving towards a more balanced approach: two third of the respondents agree that in the last 12 months, their organization has adopted a more balanced approach between people, process and technology.

In particular, the importance of a coordinated approach between people, process and technology for dealing with the challenge of managing cyber threats by insiders was clearly highlighted by the majority of the respondents.

At the same time, they have stepped up efforts in areas such as:

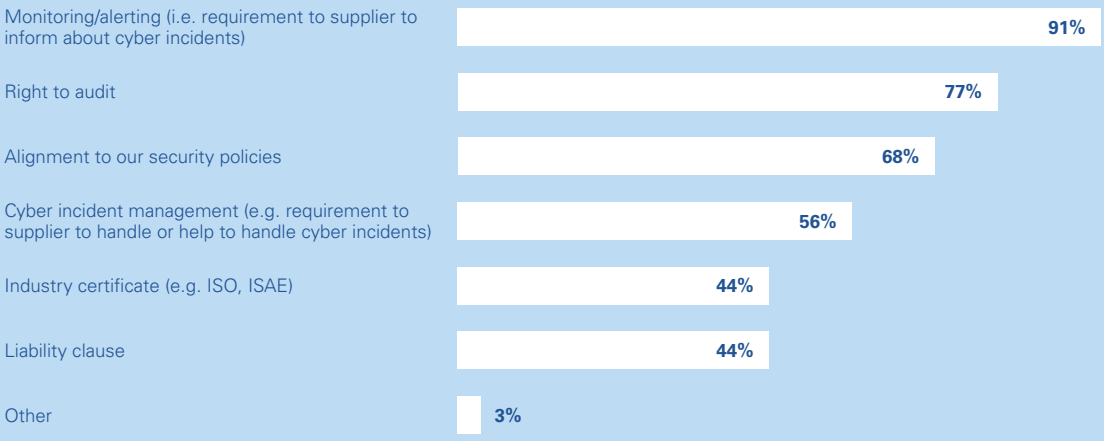
- Sharing lessons learned from attacks, sharing preventive measures, and sharing response experience in collaborations
- Implementing a central security incident event monitoring to collect and analyse events.
- Implementing training to recognize the sign of cyber attack.

However, to be honest, there may be some wishful thinking in this area. Our experience shows that Cyber Security is still mainly considered a technical issue. Changing this remains one of the major challenges. As one of the interviewees stated: "The phase of full user adoption is in fact the hardest part." To conclude, an interesting correlation in the survey results tells us that companies that put too much focus on technology in their Cyber Security efforts also have trouble in finding a language that the business understands. Moreover, companies that find a better balance between people, process and technology enable advances in prediction and a deeper understanding of cyber risks, as proved by our survey.

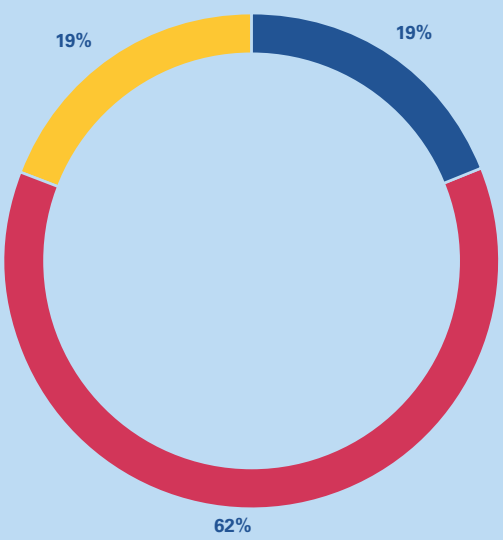
Swiss organizations deal with third-party risk
In today's economy, third parties provide more and more critical services to companies and other institutions, especially within the financial services industry. Outsourcing and interconnection with all sorts of business partners due to the break-up of value chains and the building of ecosystems in many industries has reached levels where companies rely on their partners for provision of their services. It goes without saying that this has significant consequences in the domain of Cyber Security: organizations remain responsible for the security of their outsourced processes and should invest in specific measures. Our survey shows that 72% of the respondents now indeed require specific security measures in third-party contracts. Respondents seemed to have stepped up efforts in this area, in the field of compliance (claimed by 47%), prevention (23%) and detection (23%). Another remarkable development is the fact that in last year's survey, 15% of NON-FS institutions said that outsourcing decreased their understanding, visibility and control of Cyber Security. This year, this figure has improved to 8%. However, responses from the financial services sector indicate the opposite direction, with this figure moving from 25% to 33%. This indicates that financial institutions feel less confident about their understanding of cyber risk in the context of outsourcing compared to last year. This might be due to the increase in questions from the regulators.

In conclusion, we refer to the use of cloud technology as a form of outsourcing. Not only is it clear that Swiss companies seem to be conservative in embracing cloud technology in comparison with their international counterparts, they also seem to think that on-site technology is safer, which may often be a misjudgment. Only 19% believe that leveraging cloud technology can reduce security efforts in terms of infrastructure protection.

What Cyber Security measures do you require in third-party contracts?

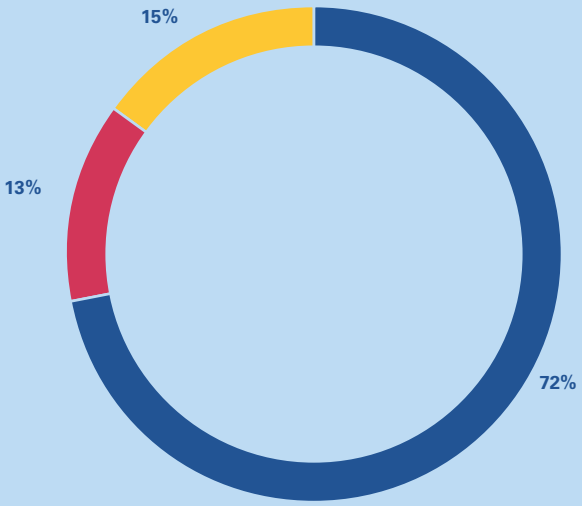


Do you believe that leveraging cloud technology can reduce your security effort in terms of infrastructure protection?



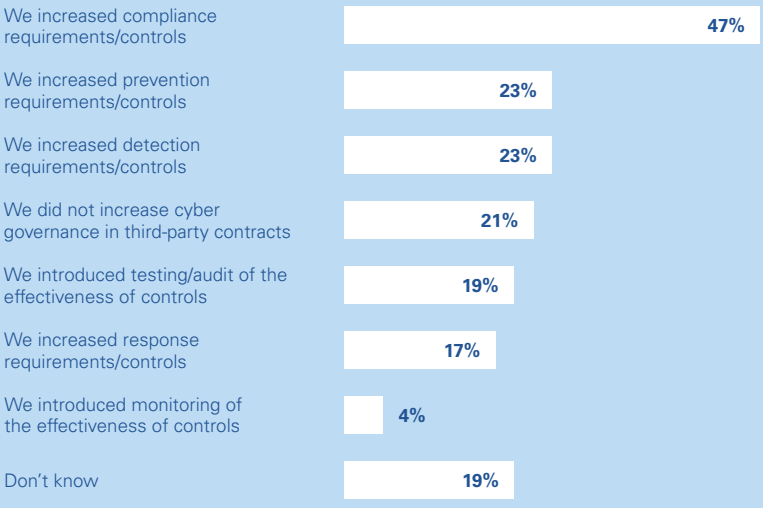
Yes
No
Don't know

Do you require specific Cyber Security measures in third-party contracts?



Yes
No
Don't know

How have you increased cyber governance in third-party contracts over the past 12 months?

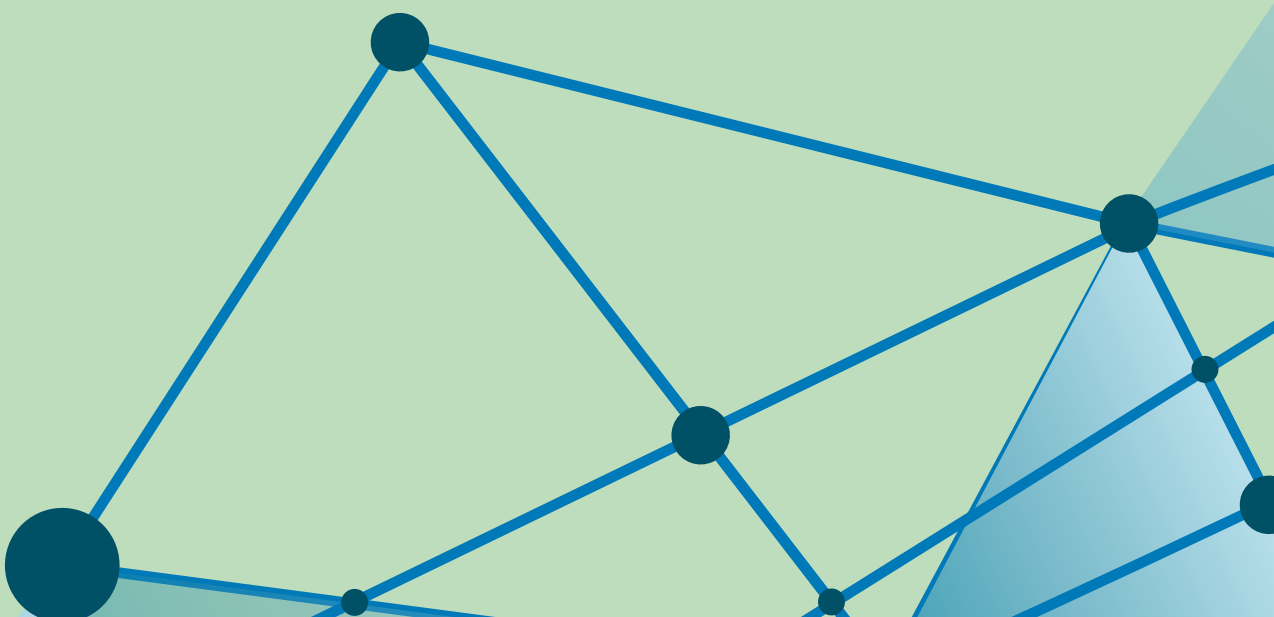


72%
require specific security measures in third-party contracts

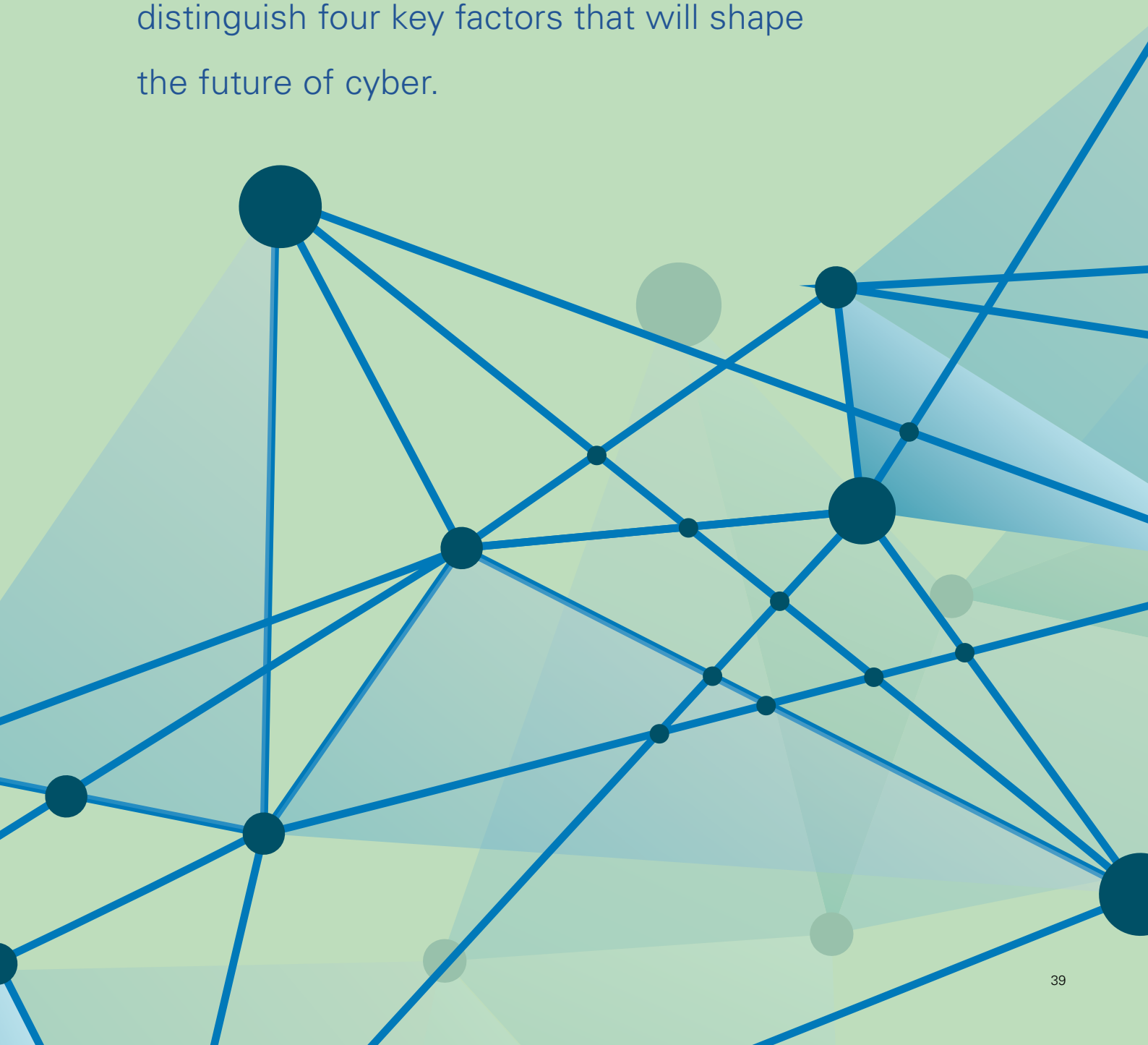
19%
believe employees are suffciently aware of the cyber risk

CHAPTER 2

The next wave of challenges in Cyber Security



Change is a constant factor in today's world. That may be a cliché, but it is also the challenging truth when it comes to Cyber Security. Based on our survey, interviews with opinion leaders in this area and our own experiences, we distinguish four key factors that will shape the future of cyber.

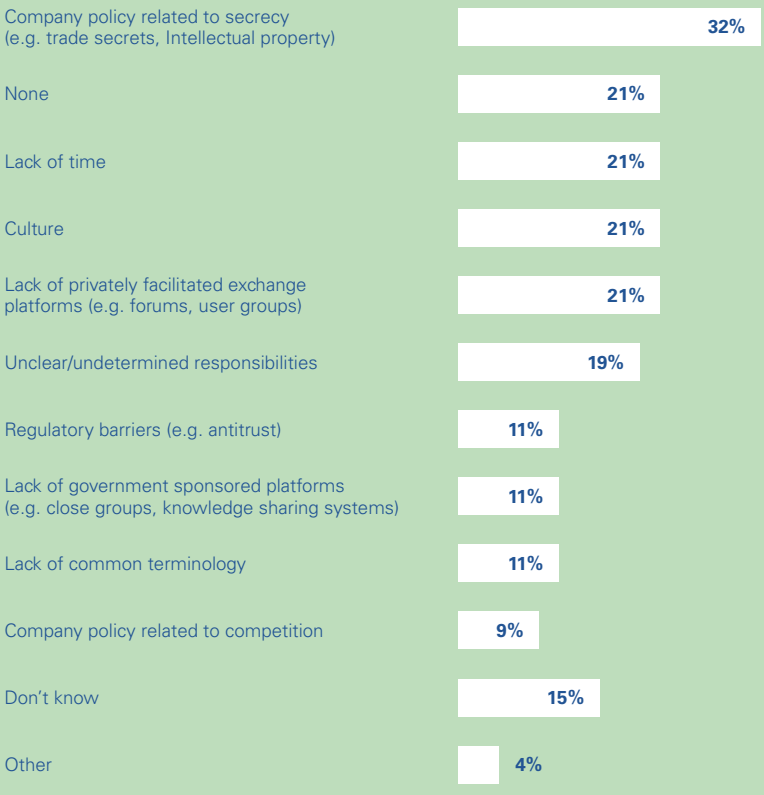


More collaboration is essential

It takes a network to defeat a network

In last year's survey, 95% of the respondents indicated the wish to have better collaboration in place. Their wishes have at least partially been fulfilled: 66% of the respondents state that the level of collaboration has increased in the past 12 months. The main arguments in favour of doing so are to share threat intelligence (named by 88%) and to share lessons learned from attacks (83%). Organizations also seem to be quite satisfied with these collaborations. Many companies find it hard to start open collaborations. Important barriers are company policies related to secrecy (named by 32%) and the organizational culture (21%).

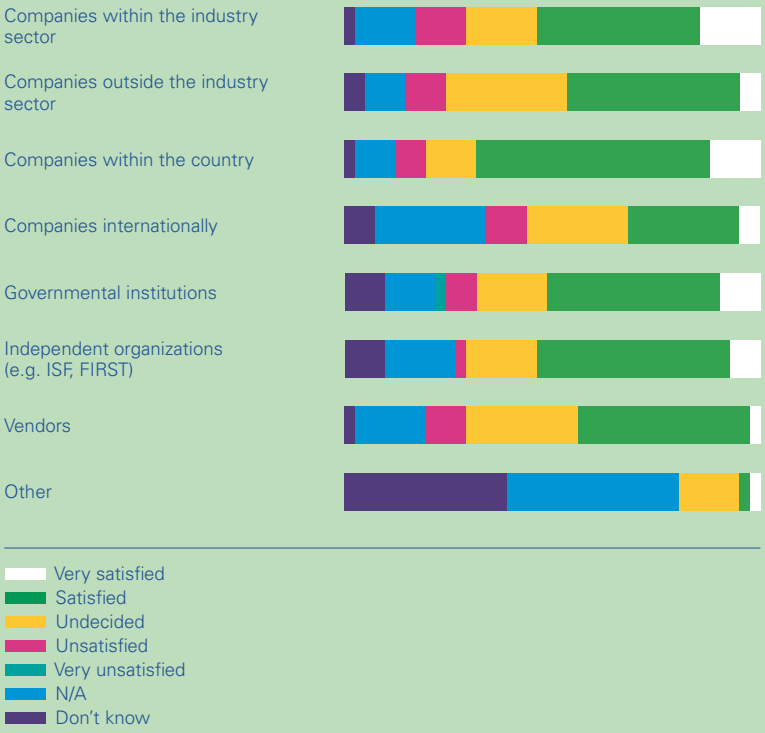
What are your constraints on open collaboration?



Looking at it from a distance, there does not seem to be an alternative to moving towards more collaboration. Cyber criminals operate in rapidly changing networks and share knowledge. To be well prepared for this reality, organizations should not isolate themselves but rather opt for building up intelligence networks as well. Seamless collaboration is essential. An analogy can be made with how General McChrystal learned lessons when he was responsible for the American military forces facing Al Qaeda and later the Taliban. At first, the American forces were struggling to successfully deal with these terrorist networks. The road to success started when McChrystal realized that terrorists were self-organizing and unstructured networks with ever changing tactics, which sounds quite familiar with how cyber criminals work. Traditional indicators, predictive of enemy action, were too numerous and non-linear to serve as a base for informed decision making. And intelligence sharing tended to stovepipe along organizational and cultural lines. The general managed to break down the silo walls of American military bureaucracy and started to reorganize the forces into networks with liaison officers. The forces in fact started to operate like a street gang and to swarm like soccer teams.

The challenge that McChrystal faced shows a similarity with the challenge that is at stake in defending against cyber attackers. They too operate in dynamic networks and a strictly linear defense will not be effective. At this moment, we're not yet able to operate in seamlessly communicating networks on the defense side. But the survey shows that there's a strong urgency towards better collaboration.

With which companies or organizations do you collaborate and what is your level of satisfaction?

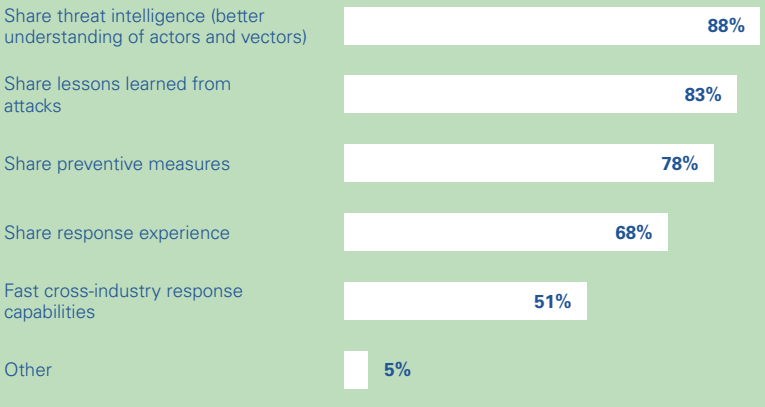


66%
have increased collaboration in the past 12 months

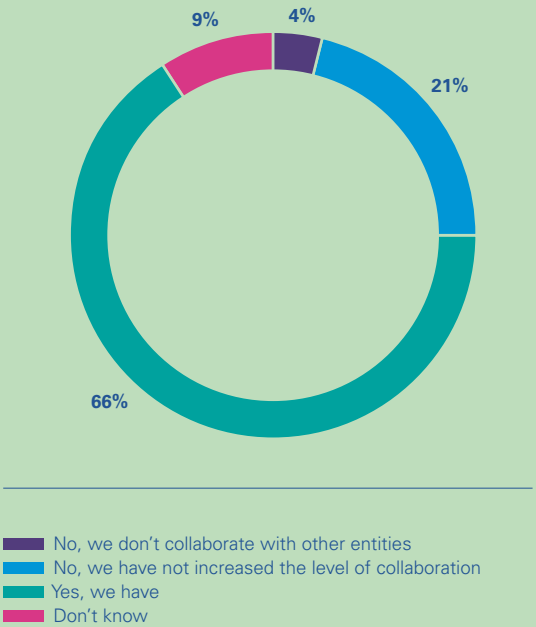
32%
are constrained from open collaboration by company policies

21%
are constrained from open collaboration by organizational culture

What would you like to achieve through collaboration?



Considering the past 12 month, have you increased your level of collaboration with other entities?



Never a dull moment

No room for complacency

It's commonly known that every closed system evolves toward a state of maximum entropy. It's a natural evolution and when it comes to the information society, we see this effect in many aspects of it. The French writer Robert Branche made an interesting point about entropy in his book "Les Radeux de Feu". He noted that entropy is in fact not so much about increasing disorder, but also about increasing unpredictability. His thesis is that all of nature's invention – life, first cells, then plants, then animals and ultimately humans – contributes to unpredictability. With each invention, the number of possible future states increases dramatically. Now that humans are transforming the world with their innovations, the unpredictability will grow at an exponential pace, and in particular the innovations that shape the fourth revolution – with many interconnections – will further accelerate this. If this is true, it doesn't make sense to think that we will soon enter a more stable environment. We may think we're in the eye of the storm and that it will calm down once new technologies have settled. But in fact, it will not. Resilience is critical in such an environment.

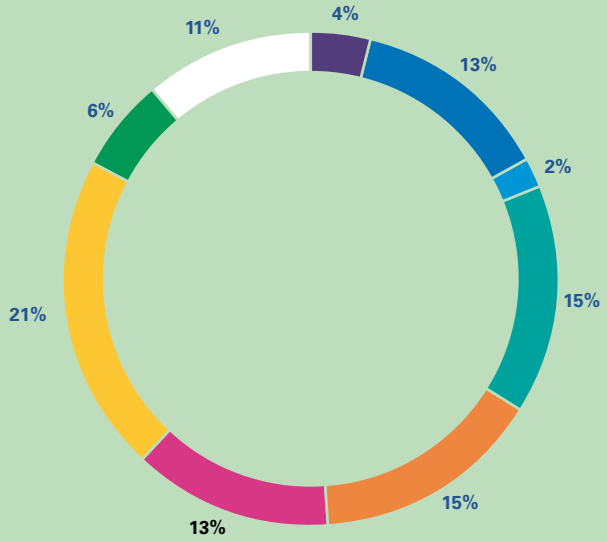
This also teaches us a lesson when it comes to Cyber Security. It raises the question of whether we can actually be fully in control of the risks in this ever increasing level of uncertainty. The recent DDoS attacks, which affected a number of Swiss organizations, were anecdotal evidence that cyber attacks often don't follow patterns that we expect them to do, based on historic data. Experts expect the attackers to extort the victims, but they didn't. This may or may not be a case where criminals deploy the art of deception. This case is typical of today's uncertainty and unexpected developments. The fact is that organizations cannot afford to be complacent, even with a state-of-the-art Cyber Security program in place.

Looking at it from a distance, we distinguish two leagues in the Swiss business landscape. On the one hand, the companies that still have some work to do on the hygiene of Cyber Security. They're not in control and they know they aren't. Typically, there are many small companies but also a surprising number of global corporates in this league. Their perception is that they're not attractive to attackers, when in reality they are. One of the reasons is that these companies have ties with larger organizations (for instance as a supplier) and attackers may focus on them as they look for the weakest link to gain access to larger organizations. In addition, it takes less effort for an attacker to steal CHF 1 million from 100 companies than CHF 100 million from one company.

On the other hand there is the proverbial Champions League of Cyber Security, mainly occupied by larger organizations and those from the financial sector that have long been working on Cyber Security. The latter category shows a lot of professionalism but risks complacency. They think they're in control when in fact that is impossible due to the increasing speed of Cyber Security dynamics and the complexity of their organization.

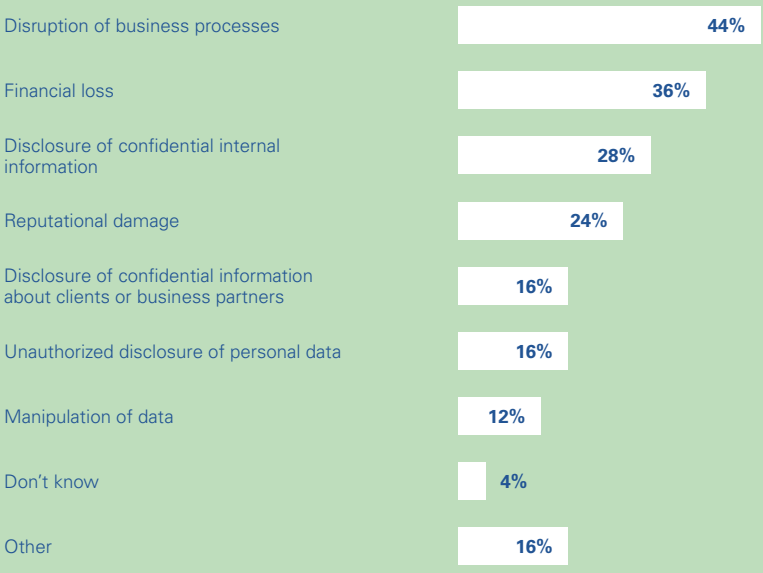
The lesson is to be prepared for anything. Keep challenging your efforts in the domain of Cyber Security. Be agile in understanding the business and the threat landscape and structure your cyber governance accordingly. Keep learning. And thereby be prepared for a world in which surprises have become the standard.

What are the main reasons for a lack of threat intelligence in your company?



- We don't know what threat intelligence should cover
- We don't know how to best structure threat intelligence organizationally
- We do not think it is necessary for us
- We do not have the capability (knowledge and resources) to develop threat intelligence
- We do not have the expertise
- Our executive don't see the need for threat intelligence (lack of funds)
- We think we have adequate threat intelligence in place
- Don't know
- Other

What were the consequences of the cyber attack(s) for your business?



54%

of respondents from FS institutions simulate cyber attacks, but only 27% of NON-FS institutions do it as well

30%

of NON-FS institutions respondents claim that lack of time is a constraint on open collaboration, yet only 4% of FS institutions considers this as an issue

43%

of NON-FS institutions consider that lack of compliance monitoring is the main issue related to third-party risks, while the corresponding number for FS institutions is 18%

New challenges in the fourth Industrial Revolution

Being secure becomes a license to do business

The modern history of the world in a nutshell: the first industrial revolution was all about mechanizing production using water and steam. The second was about mass production. The third was about deploying electronics and information technology to automate production. And now we are in the midst of the fourth revolution characterized by a fusion of technologies that is blurring the lines between physical, digital, and biological spheres.

This creates massive strategic challenges and opportunities for many companies. And it also changes the dynamics of Cyber Security as the interconnectedness of the world accelerates. Many objects ranging from cars to buildings and from watches to pacemakers are now connected 24/7. In this shift towards complete connectivity it is evident that part of our longstanding technology can no longer keep up. We've already witnessed media reports that show how new (and sometimes unexpected) vulnerabilities emerge. Power plants have been under attack; hackers managed to cause a blast furnace at a German steel mill by attacking the network, thereby causing massive damage and forcing a shutdown of a furnace. Another example was the hack of the Ukraine power grid last year, where several substations were put offline and more than 230,000 residents left in the dark.

These examples draw a lot of public attention as their character is media-savvy. However the biggest risk is probably in other area; for instance, how hackers may exploit devices to gain entry to corporate and government networks and databases. This may result in obtaining control over industrial systems that control power plants, the energy grid, water supply, and damming traffic infrastructure. The changing dynamics has two perspectives.

On the one hand the variety and number of devices is exploding, which brings new challenges to manage the multitude of devices and systems; on the other hand the level of interaction between all these devices also increases, which allows a domino effect and thus multiplies the impact of a possible disturbance.

There are no easy answers in this domain. But it is clear that this trend leads us to a new reality in Cyber Security. A reality in which Cyber Security is no longer confined to cyber space but also comprises our physical world.

> **Many companies should take into account that the security, safety and reliability of their physical products will depend on managing Cyber Security properly.**

Thus, Cyber Security is in fact a license to operate. It will become a prerequisite for success and a differentiator in the market space.

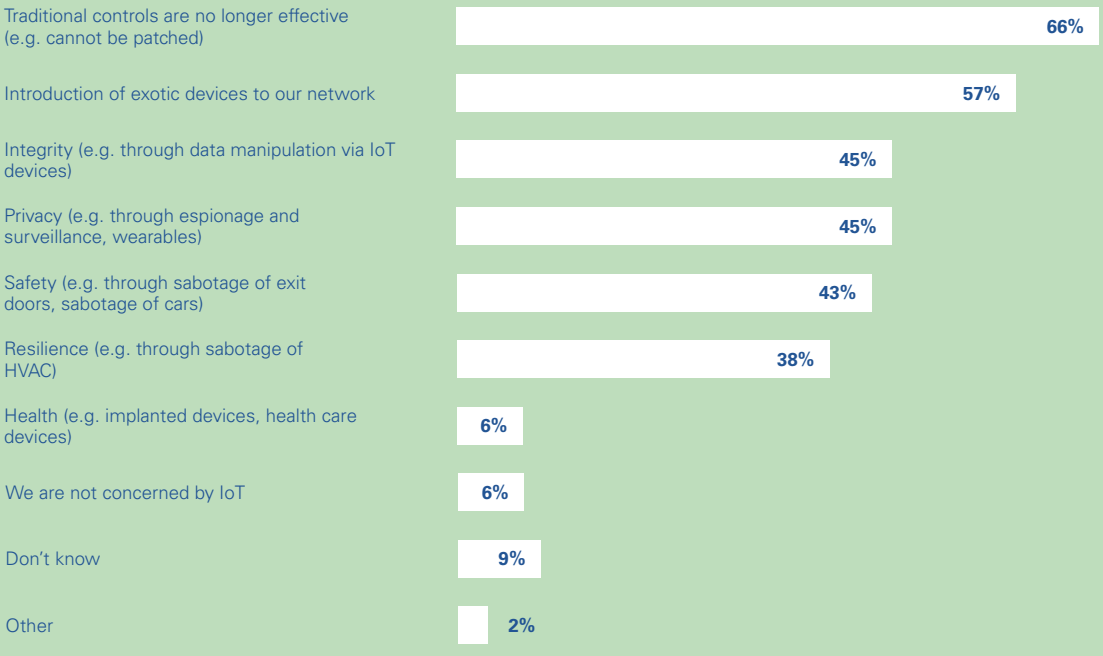
How do Swiss organizations deal with this topic? Based on our survey, the preparation is still in its infancy stage. A majority of respondents (53%) do not even try to get an overview of their relevant Internet of Things devices. Having said that, there seems to be awareness that this topic deserves attention. The biggest concerns are the fact that some traditional security strategies and controls are no longer effective (e.g. cannot be patched) (named by 66%), the introduction of exotic devices to the network (57%) and privacy (e.g. through espionage and surveillance) (45%).

53%
do not try to get an overview of their Internet of Things devices

66%
are concerned that the Internet of Things implies that traditional controls are no longer effective

In conclusion, we must be aware that future security will partially be managed automatically by system components instead of users. This calls for the design of secure technology and will require a new approach and mindset. In this respect, 25% of respondents say that they do not leverage security by design, although they consider Internet of Things a topic for their organization. That should be food for thought.

What are your biggest concerns relating to the Internet of Things?



Internet of Things

Smart meters

2015
313 m

2020
> 1 bn

Home and city

- Smart meters – efficient use of energy
- Home automation
- Smart management of city infrastructure
- Surveillance
- Water supply
- Sewage disposal

Transportation

- Connected vehicles
- Self-driving cars
- Smart infrastructure
- Public transportation
- Aviation
- Sea faring

Manufacturing and operations (Industry 4.0, IoT)

- Industrial controls
- Health and safety management
- Supply chain optimization (RFID)

Consumer and retail businesses

Improved customer experience

In-store localization

Connected devices

2015
13.2 bn

2020
> 25 bn

Since 2008, the number of things connected to the internet has exceeded the number of people on earth.

Health

Expanded access to healthcare

Well-being – the quantified self

Emergency calls

Connected vehicles

2015
373 m

2020
> 3.5 bn

Sustainability

Feed the planet – improved crop yield

Sustainable environment – reduced water consumption

Source of figures: Gartner, Cisco

Know thy enemy

Less is more in threat intelligence

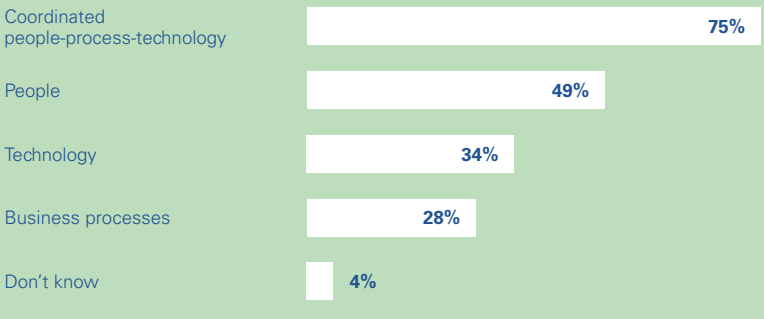
"I made this so long only because I didn't have the time to make it shorter." This quote is attributed to Pascal Blaise, and stresses the fact that getting to the core of the message takes time and effort and is in fact harder than producing a report with all the necessary information. This message is also valid when it comes to the use of threat intelligence in Cyber Security.

Know thy enemy. Knowing your adversary can drastically reduce the chances of successful threats. The key is to have good cyber threat intelligence in place as a basis for prioritizing threats, assessing the risk exposure and being able to respond swiftly and appropriately. Threat intelligence can help organizations anticipate threats by distilling the relevant intelligence from the myriad information feeds available in and outside their organization. Mastering threat intelligence is key to an agile and adaptive cyber governance.To live up to this promise, threat intelligence should be more than raw information. The intelligence has to be both consumable and actionable. If not, even start-of-the-art information is only interesting at best. "There is plenty of intelligence available," says one of the interview partners. "But show me a vendor who offers me tailor made streams of intelligence relevant to my company."

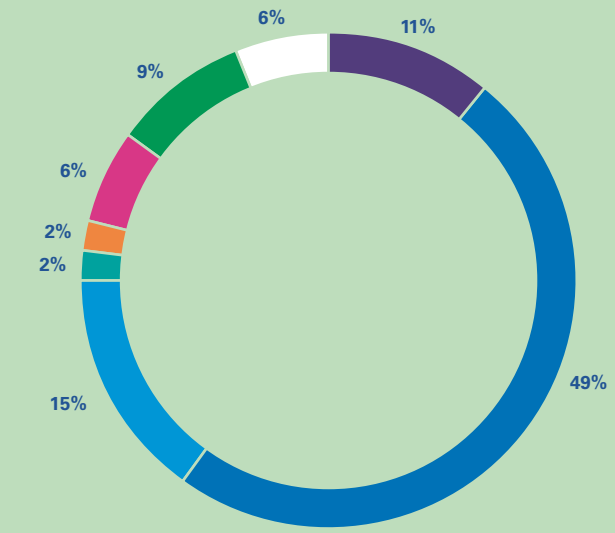
He's definitely right. The challenge is to have bespoke actionable intelligence instead of heaps of data. This knowledge should extend beyond the technical nature of the tools and tactics of attackers. Combining technical and non-technical information (patterns) can merge into actionable knowledge. It contributes to all aspects of Cyber Security: prevention, detection and response.

The survey shows some interesting statistics. Almost one third of the respondents do not have subscriptions to threat intelligence. More than half of them have threat intelligence in place. This half can be divided into two categories: 36% says that this intelligence improves their Cyber Security position, while the other 15% says it doesn't.

In your opinion, what are the main focus areas in order to successfully manage the cyber insider threat?



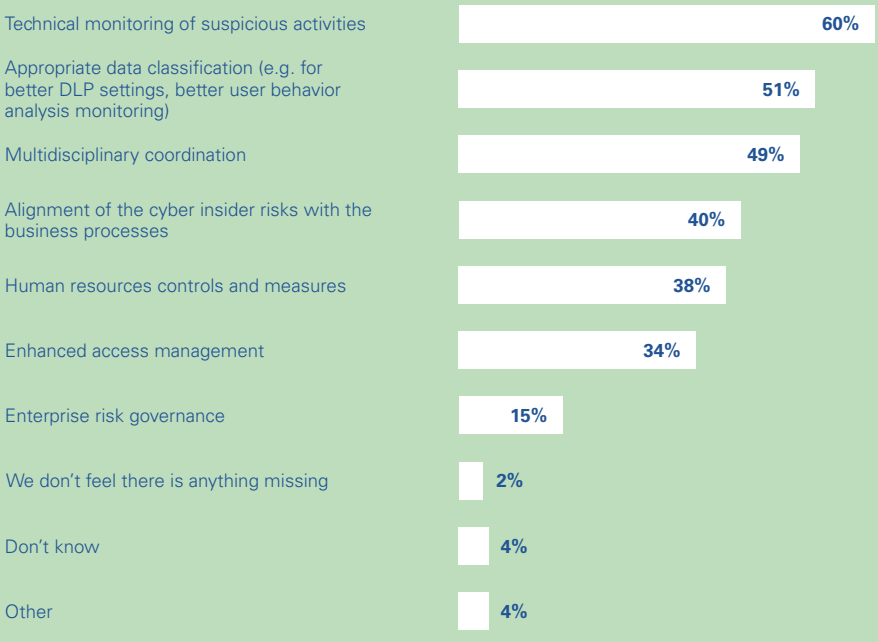
Who currently manages Cyber insider Threat?



- Head of IT
- CISO
- CSO
- Legal
- General management
- We don't have an insider threat management program
- Don't know
- Other

32%
of the respondents do not have subscriptions to threat intelligence

What is missing in order to mitigate the cyber insider threat?



Distribution of survey participants by sector

48.3%
Financial services

15.5%
Consumer/ Industrial

6.9%
Government

5.2%
Professional services

5.2%
Infrastructure

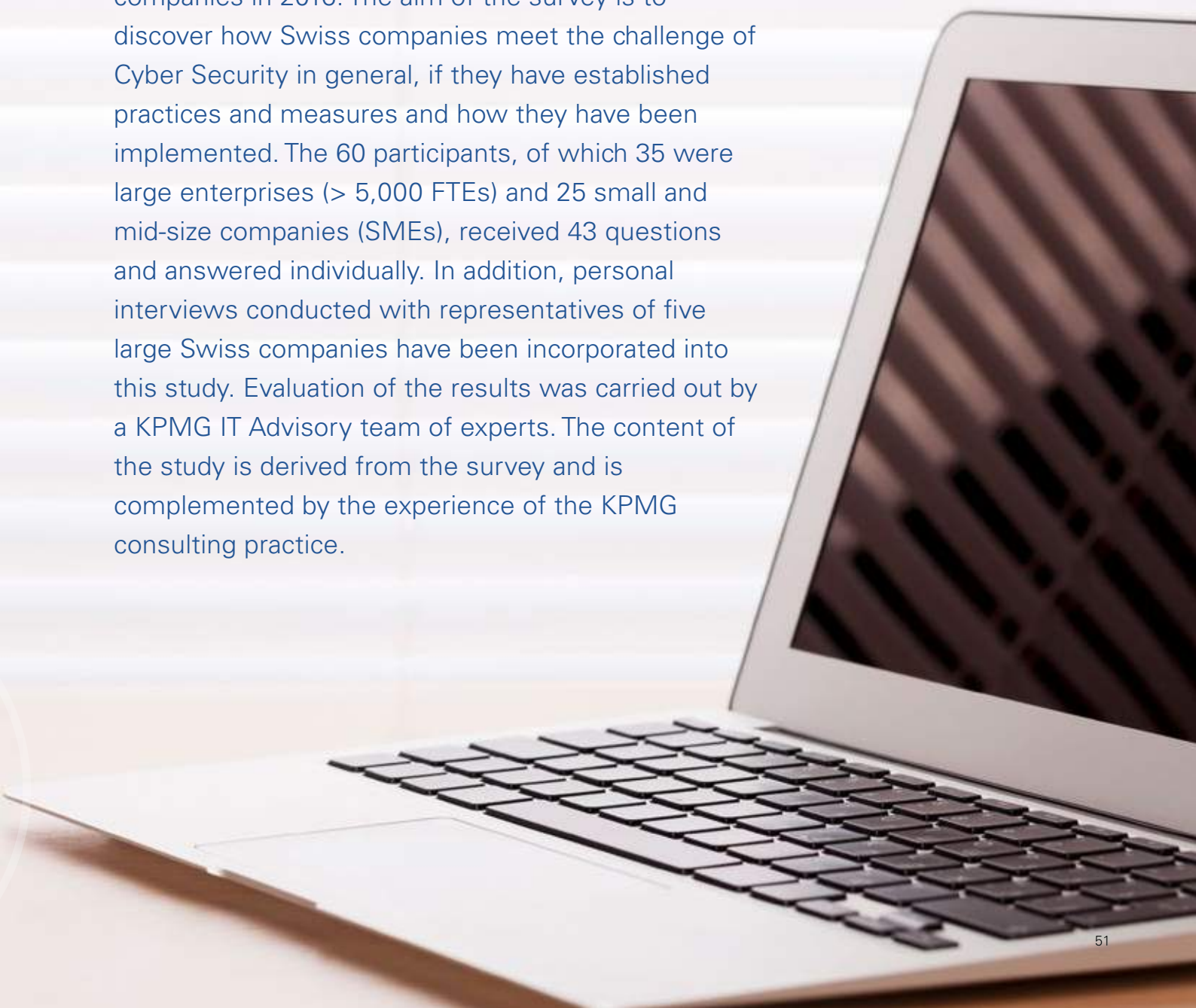
5.2%
Pharmaceutical

1.7%
Energy and natural resources

12.1%
Other

Survey Methodology

KPMG conducted this Cyber Security survey of Swiss companies in 2016. The aim of the survey is to discover how Swiss companies meet the challenge of Cyber Security in general, if they have established practices and measures and how they have been implemented. The 60 participants, of which 35 were large enterprises (> 5,000 FTEs) and 25 small and mid-size companies (SMEs), received 43 questions and answered individually. In addition, personal interviews conducted with representatives of five large Swiss companies have been incorporated into this study. Evaluation of the results was carried out by a KPMG IT Advisory team of experts. The content of the study is derived from the survey and is complemented by the experience of the KPMG consulting practice.



Principles
of our approach to Cyber Security

Razor-sharp insights

In a fast-moving digital world of constantly evolving threats and opportunities, you need both agility and assurance. Our people are experts in both Cyber Security and your market, which means we give you leading edge insights, ideas and proven solutions so that you can act with confidence.

Secure the future of your business

KPMG can help you transform your approach to Cyber Security, providing the expertise, support and challenge to help you cut through the complexities of Cyber Security. We have drawn on our experience across many sectors and clients to develop a straightforward, but effective layered approach to achieving Cyber Security.

Shoulder to shoulder

We work with you as long-term partners, giving you the advice and challenge you need to make decisions with confidence. We understand that this area is often clouded by feelings of doubt and vulnerability, so we work hand-in-hand with you to turn that into a real sense of security and opportunity.

Driven by business aspirations

We work with you to move your business forward. A positive management of cyber risk not only helps you take control of uncertainty across your business, you can turn it into a genuine strategic advantage.

We are ...

Collaborative

We facilitate and work with collaborative forums to bring together the best minds in the industry to collectively solve shared challenges. KPMG's I-4 forum brings together more than 50 of the world's biggest organizations to discuss emerging issues and solutions.

Global, Local

We have more than 2,000 security practitioners working in KPMG's network of firms, giving us the ability to orchestrate and deliver to consistently high standards globally. KPMG member firms can service your local needs from information security strategy and change programs, to technical assessments, forensic investigations, incident response, training, and even ISO 27001 certification.

Trusted

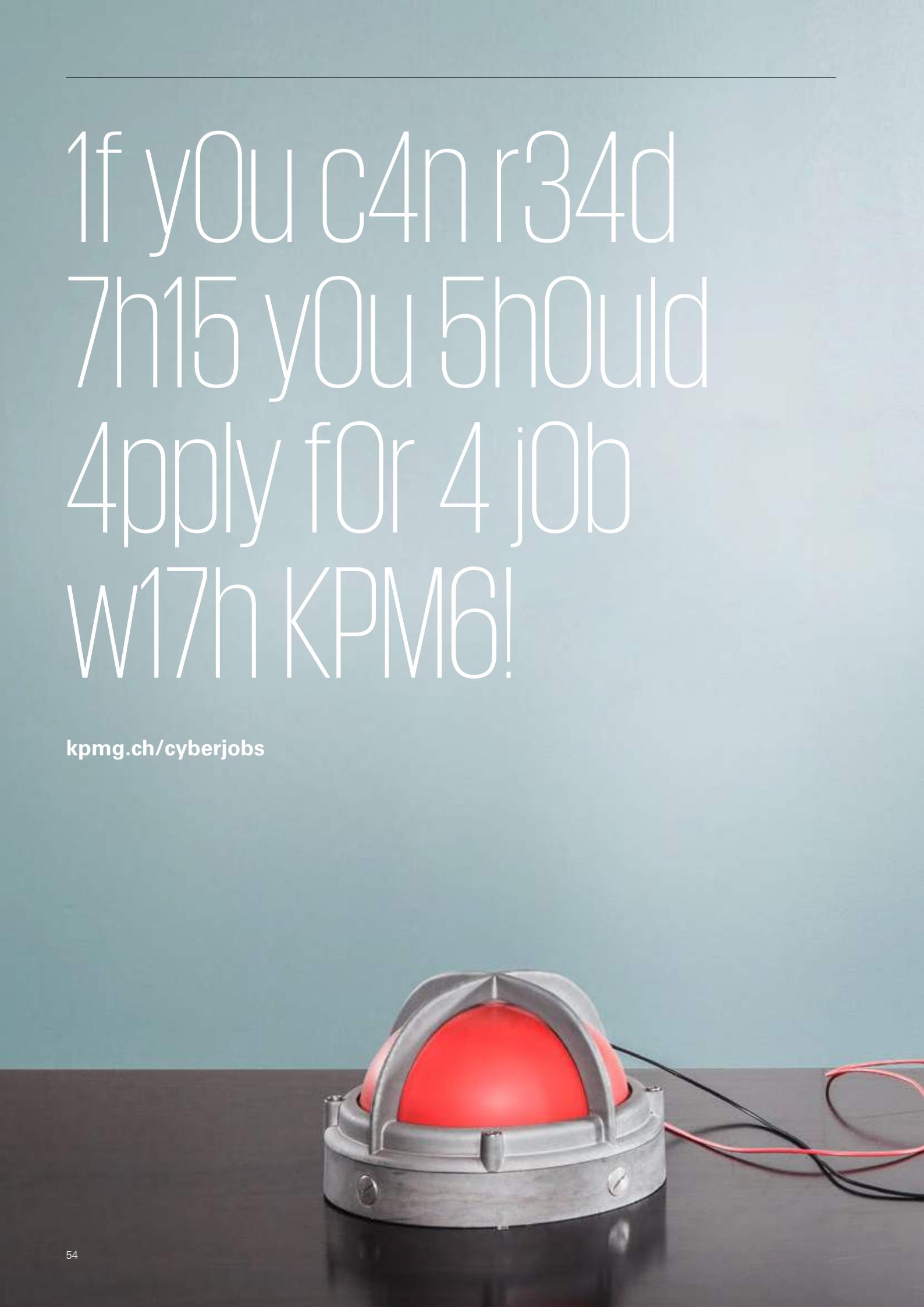
We have a long list of certifications and accreditations to work on engagements for the world's leading organizations.

Issues-led

We are constantly enhancing our capabilities to meet heightened client demand for robust information protection and business resilience services.

1f y0u c4n r34d 7h15 y0u 5h0uld 4pply f0r 4 j0b w17h KPM6!

kpmg.ch/cyberjobs



“Clarity on” publications

The “Clarity on” series from KPMG Switzerland offers a wide range of studies, analysis and technical articles. All publications are available in print and online. Additional information can be found at **kpmgpublications@kpmg.com**

Latest issues

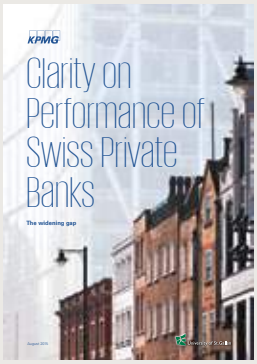
Clarity on
Commodities Trading

Clarity on
Mergers & Acquisitions

Clarity on
Data & Analytics

Clarity on
Entrepreneurs

Clarity on
Tax Function Transformation



Clarity on
Performance of Swiss Private Banks

Clarity on
Compliance

Clarity on
Swiss Taxes

Clarity on
kpmg.ch/clarity-on

KPMG Knowledge App

Get instant access to the expertise of KPMG’s specialists with the “Knowledge app” for iPad – now even more compact and customizable to your specific requirements.

Download on the App Store

Google play

KPMG Apps
kpmg.ch/apps

IMPRINT AND CONTACTS

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

Gerben Schreurs
Partner, Cyber Security
+41 58 249 48 29
gschreurs1@kpmg.com

Marc Bieri
Director, Cyber Security
+41 58 249 64 05
marcbieri@kpmg.com

Roman Haltinner
Senior Manager, Cyber Security
+41 58 249 42 56
rhaltinner@kpmg.com

Anne van Heerden
Partner, Head of Advisory
+41 58 249 28 61
annevanheerden@kpmg.com

Ulrich Amberg
Partner, Head of Consulting
+41 58 249 62 62
uamberg@kpmg.com

Publisher
KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich
+41 58 249 31 31
+41 58 249 44 06 (Fax)
kpmgpublications@kpmg.ch

Editorial Team KPMG
Matthias Bossardt
Gerben Schreurs
Roman Haltinner
Rikard Sandström
Konrad Schwenke

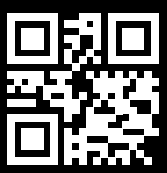
Concept and design
KPMG, Stephan Erdmann
Konkret, Andi Portmann

Print
GfK PrintCenter, Hergiswil

Pictures
Shutterstock
Getty Images

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

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



Clarity on Cyber Security
kpmg.ch/cyber