



Clarity on Cyber Security

**Towards understanding
the cyber risk**

May 2015

4

What's at stake in Switzerland?

An attractive target for cyber attacks.
Are Swiss companies prepared to
defend themselves?

12

Key findings

A better understanding of the
cyber risk is the first step towards
a predictive cyber defense.

14

Survey results and interviews

A call for action based on a survey
among 64 cyber crime professionals
and five interviews with Swiss
companies.



A close-up of an owl's face. The owl has brown and white feathers. Overlaid on the right side of its face and neck is a glowing blue energy field consisting of many thin, radiating lines.

**RAZOR SHARP
INSIGHTS**

A close-up of a peacock's head and neck. The peacock has vibrant blue, green, and gold feathers. Overlaid on the right side of its neck and tail is a glowing blue energy field consisting of many thin, radiating lines.

**DRIVEN BY
BUSINESS
ASPIRATIONS**

A close-up of a lion's face. The lion has a thick, golden-brown mane. Overlaid on the right side of its face and neck is a glowing blue energy field consisting of many thin, radiating lines.

**SECURE THE
FUTURE
OF YOUR
BUSINESS**

A close-up of a lioness's face. The lioness has a golden-brown coat. Overlaid on the right side of its face and neck is a glowing blue energy field consisting of many thin, radiating lines.

**SHOULDER
TO SHOULDER**

Clarity on

Cyber Security

	EDITORIAL
3	From reactive to predictive

	CHAPTER I
4	What's at stake in Switzerland?

	CHAPTER II
12	Key findings

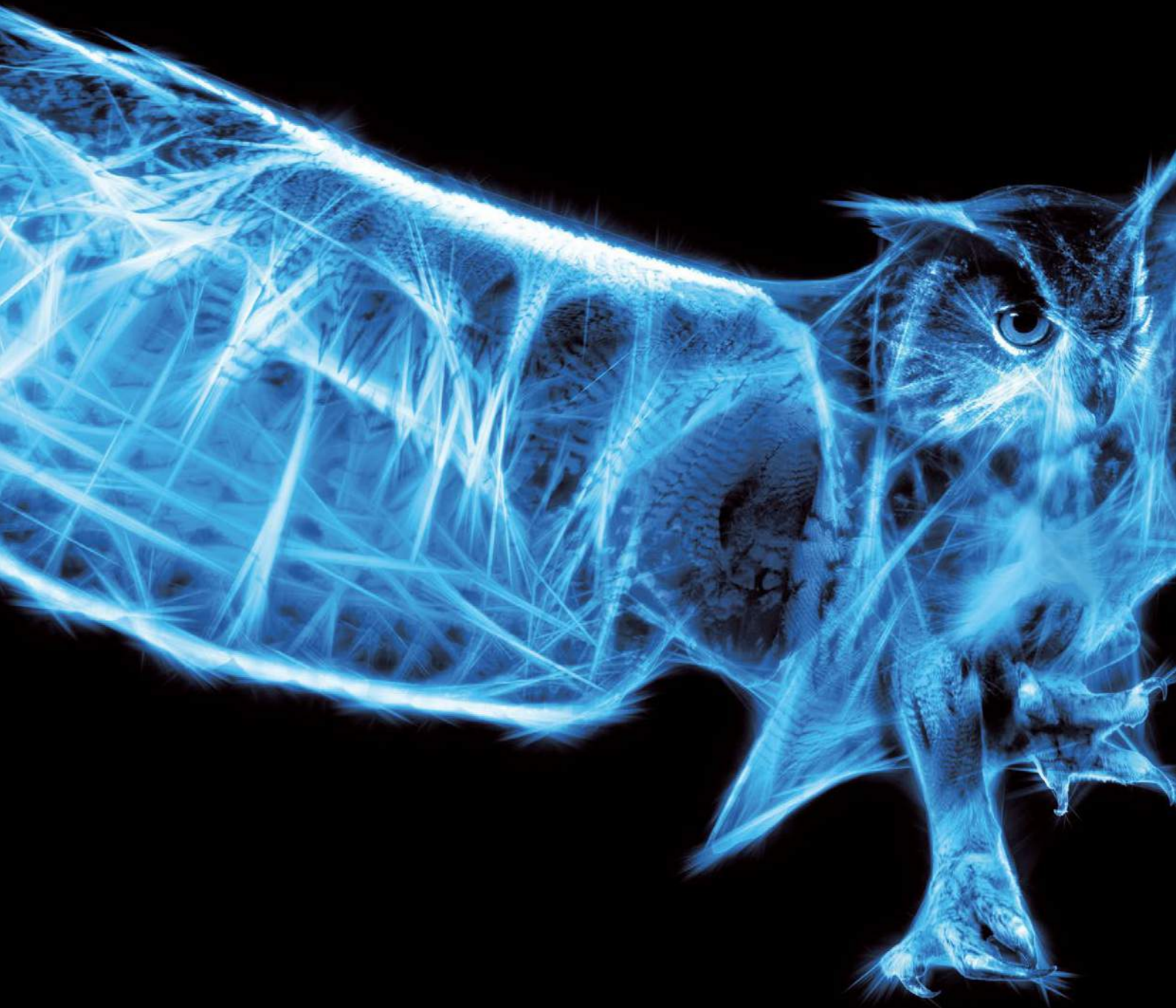
	CHAPTER III
14	Survey results and interviews

14	Tackling cyber threats: Three key priorities
16	Interview Swisscom, Roger Halbheer
18	A lack of insight into the issue of Cyber Security
20	Interview Helsana Group, Stefan Burau
22	We need to shift from a technological approach to a more balanced approach focused on people, technology and processes
24	Interview Alpiq, Werner Meier and Urs Köhler
26	From reactive to predictive organizations must develop their cyber capabilities
28	Interview Melani, Max Klaus
30	Interview Baloise, Olaf Romer
33	Survey Methodology

	CHAPTER IV
34	About KPMG

34	Principles of our approach to Cyber Security
38	Pinboard

39	IMPRINT AND CONTACTS
----	----------------------



**ACTING OUT OF FEAR FOR THE
CONSEQUENCES OF A
CYBER INCIDENT MAY NOT LEAD
TO THE BEST RESULT. A CYBER
STRATEGY FOR PREVENTION AND
RESPONSE IS REQUIRED.**



Matthias Bossardt
Partner, Cyber Security



Gerben Schreurs
Partner, Cyber Security

Towards understanding the cyber risk

Media reports on cyber incidents are everywhere these days. It seems as if all organizations – both public and private – are extremely fragile compared to the invincible strength of their attackers – varying from script kiddies to organized crime. Recent incidents once again signaled that reputations are at stake when private data comes out into the public arena. It goes without saying that organizations must protect their digital assets properly and that failing to do so may result in serious problems. Cyber Security clearly deserves a prominent place on the management agenda.

However, acting out of fear of the consequences of an incident may not be the best reaction in this domain. A better approach is to build an effective strategy for prevention and response. This brings us to the question: what is the best strategy to cope with the threats of cybercrime in a time of constant change, like digitalization, globalization, etc.? And how do Swiss organizations cope with this challenge?

Against this background, KPMG conducted an online survey of 64 Cyber Security professionals in Switzerland from all sectors and combined these insights with five interviews. This survey concludes that many organizations need a better balanced perspective to effectively cope with the challenges of cybercrime. Starting with being better informed about (patterns) of threats and having a deep understanding of what's at stake. This paper aims to provide an overview of how the issue is – and should be – dealt with in corporate Switzerland.

We hope you will enjoy reading this publication, and we look forward to discussing your questions and issues.

Matthias Bossardt

Gerben Schreurs

WHAT'S AT STAKE IN SWITZERLAND?

“

The Swiss tend to think:
it won't happen to us.

”

Peaceful, prosperous and modern. These three words characterize Switzerland and its highly competitive economy. For many years, the modern market economy has shown excellent performance in terms of low unemployment, a highly skilled labor force, and a high GDP per capita. Switzerland's economy largely thrives on a modern service sector, led by financial services, and an innovative manufacturing industry that specializes in high-technology, knowledge-based production. The economic and political stability – and the neutrality – further contribute to the Swiss reputation of trustworthiness. Recent incidents are a threat to this reputation. Fortunately, trust is still one of Switzerland's key assets.

In terms of Cyber Security, however, trust may also be a disadvantage. We Swiss have long nurtured a strong culture of quality and trust – “we do what we say”. This also relates to the fact that Switzerland is still neutral and considered a safe haven in the financial landscape. The implicit thought about serious cyber crime is that “this won't happen”. Awareness of the matter may be there, but in practice it turns out to be difficult to translate this awareness into robust action.

The reality is that the stakes are very high for the Swiss where it comes to Cyber Security. The exposure of the banking industry is high as this is an attractive target group for direct financial gain. The same is true for the Swiss

industry, with its intellectual property and high standards in terms of innovation. The essential trademarks of Swiss success are the quality of its products – “Swiss made” – and deeply rooted values in terms of discretion and secrecy. These trademarks may be under pressure in a hyper-connected world. The secrets of successful innovation may be stolen and the secrecy of doing business may be compromised.

The openness of the economy may further raise the bar. Swiss organizations have a history of being very connected with organizations internationally. These connections bring exposure when it comes to outsourcing activities and third-party relationships, etc. Furthermore, two “leagues” can be clearly distinguished in the Swiss business landscape: domestically orientated companies tend to rank cyber threats low, while international companies are more conscious of the risks. Many small and medium-sized companies may not be aware of the serious risks they face.

In short, Switzerland has many attractive assets and is strongly networked with other countries. Some sectors are poorly prepared for the issue of Cyber Security. This combination should be a wake-up call to executives.

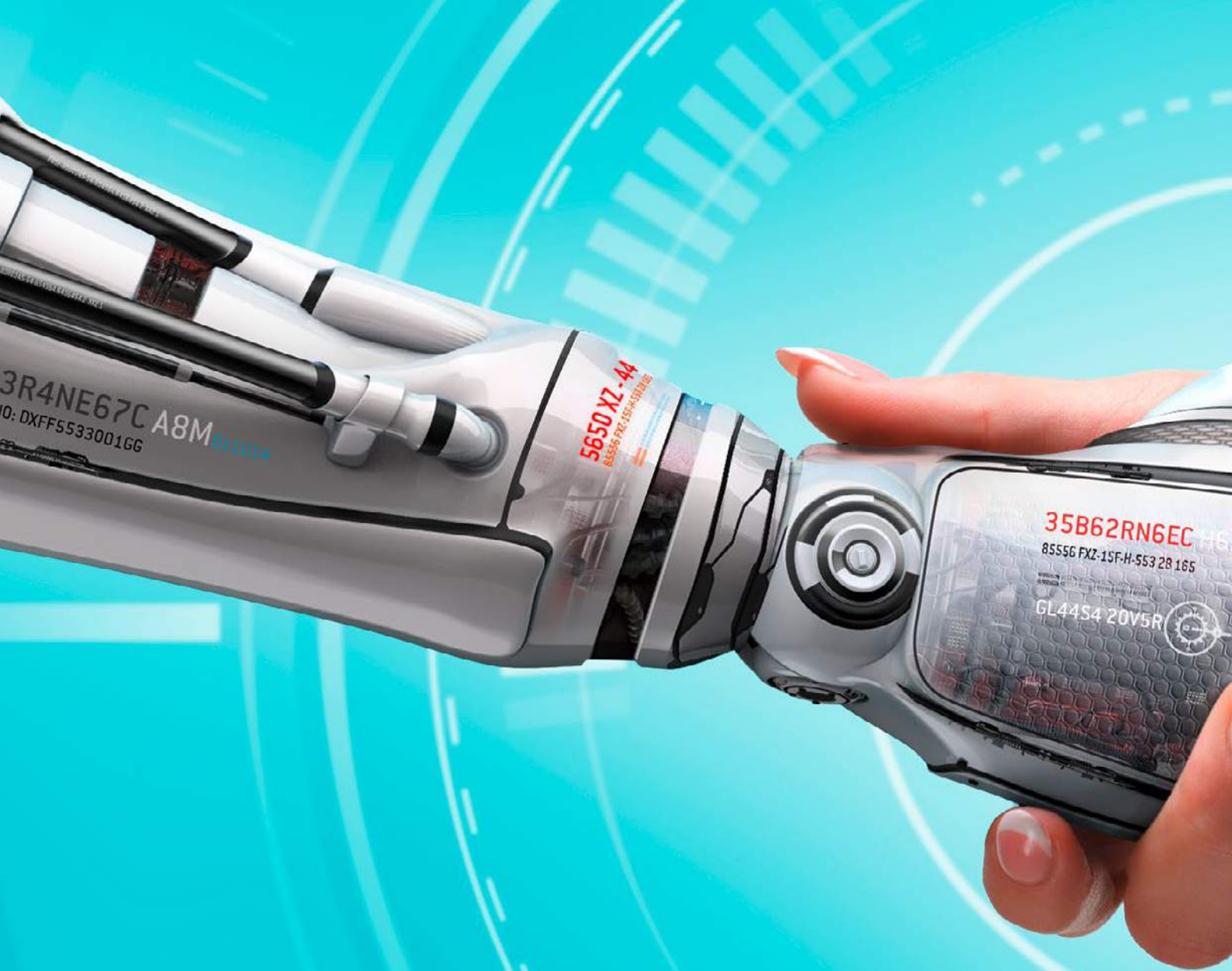




UNDERSTAND THE CYBER RISK

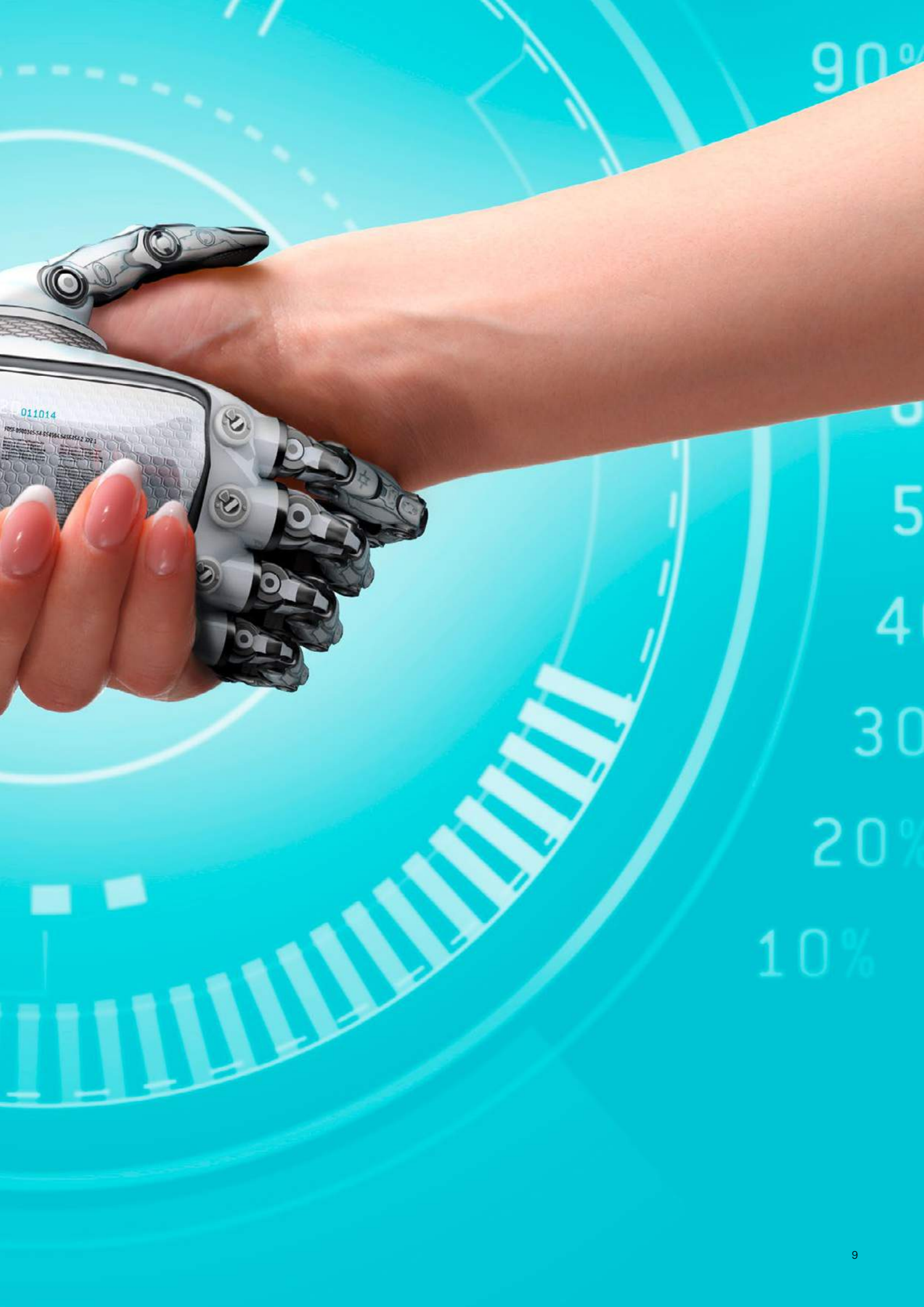
Whilst Cyber Security is on top of many board agendas, companies struggle to properly assess, measure and communicate to what extent their business is resilient against cyber attacks. This understanding is paramount in order to tackle cyber risk effectively.

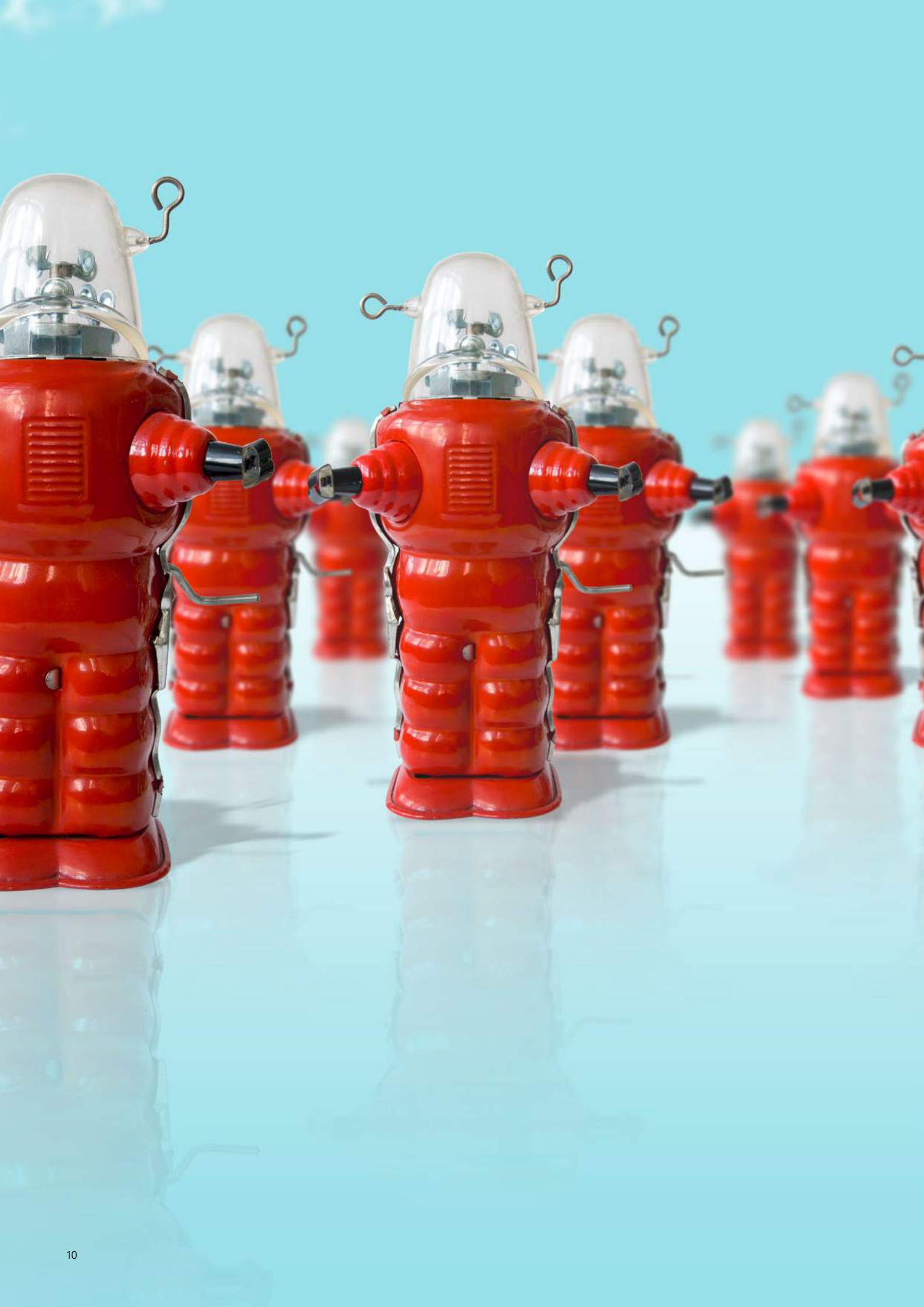




BALANCE PEOPLE, PROCESSES AND TECHNOLOGY TO MITIGATE THE RISK

Whereas cyber crime has a strong connotation with “technology”, fighting it effectively requires an integrated and balanced approach involving both people and processes as well as technologies.







FROM REACTIVE TO PREDICTIVE

Given the strategic relevance of Cyber Security, a reactive approach to managing the cyber risk is no longer sustainable.

The attention of the board presents an ideal momentum to develop an insight based, risk focused, and predictive management of cyber risk.

KEY FINDINGS

NEED TO BALANCE PEOPLE, PROCESS, AND TECHNOLOGY

53%

STATE THAT THE EXECUTIVE BOARD CONSIDERS CYBER SECURITY A TECHNICAL ISSUE

53%

BELIEVE THEIR ORGANIZATION IS ABLE TO DETECT ONGOING CYBER ATTACKS

59%

ARE NOT CONVINCED OR DO NOT KNOW WHETHER THEIR SERVICE PROVIDERS UNDERSTAND HOW TO DEFEND AGAINST CYBER ATTACKS

14%

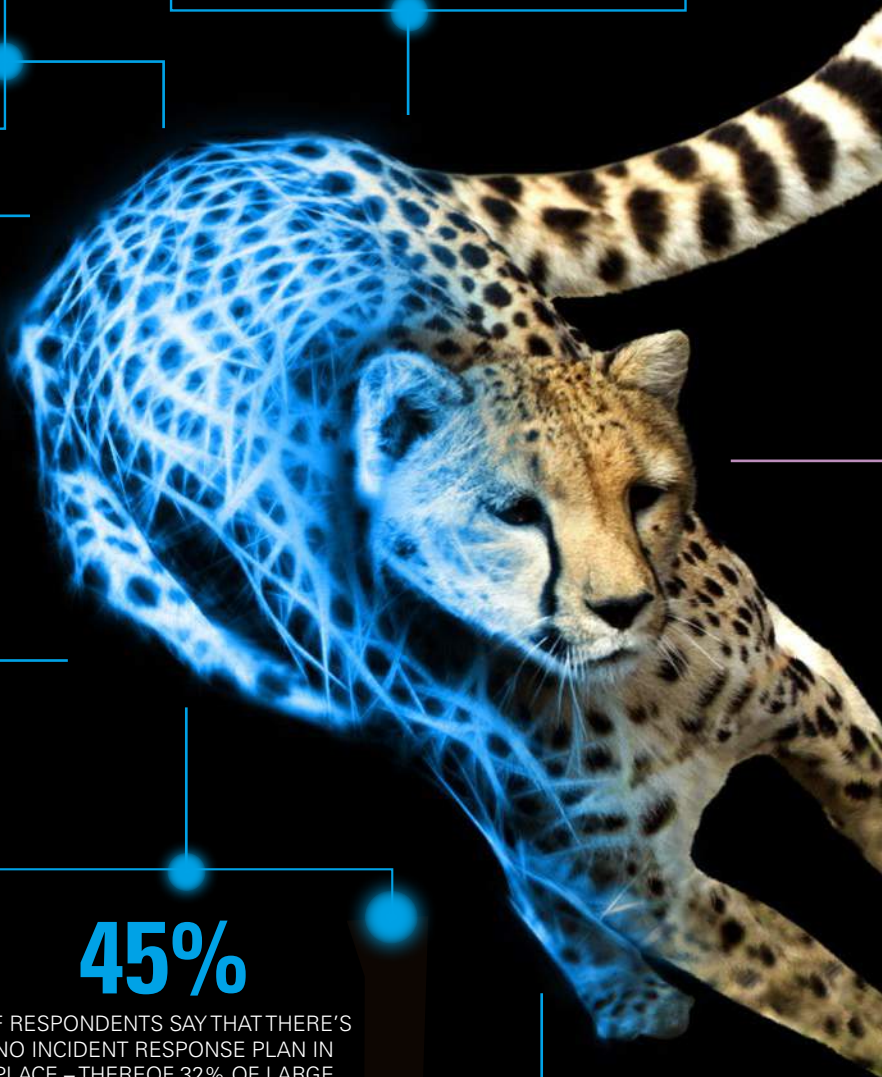
TEST THEIR CYBER INCIDENT RESPONSE PLANS

45%

OF RESPONDENTS SAY THAT THERE'S NO INCIDENT RESPONSE PLAN IN PLACE – THEREOF 32% OF LARGE COMPANIES, 52% OF FINANCIAL INSTITUTIONS AND 53% OF SME (SMALL AND MEDIUM ENTERPRISES)

36%

BELIEVE EMPLOYEES ARE SUFFICIENTLY AWARE OF THE CYBER RISK



LACK OF INSIGHT

44%

OF RESPONDENTS STATE THAT THE EXECUTIVE BOARD DOES NOT HAVE ANY METHOD TO MEASURE THE CYBER RISK TO THE BUSINESS

15%

OF NON-FS INSTITUTIONS AND 25% OF FS INSTITUTIONS FEEL THAT OUTSOURCING HAS DECREASED THEIR UNDERSTANDING, VISIBILITY AND CONTROL OF CYBER SECURITY

50%

OF THE LARGE COMPANIES HAVE NO INSIGHTS IN CYBER THREAT DAMAGES

TACKLING CYBER THREATS

63%

CONSIDER THEMSELVES AN ATTRACTIVE CYBER THREAT TARGET

76%

BELIEVE THAT CYBER SECURITY IS NOT A HYPE THAT WILL SUBSIDE

FROM REACTIVE TO PREDICTIVE

51%

BELIEVE THAT CYBER ATTACKS CANNOT BE FULLY PREVENTED

75%

OF RESPONDENTS AGREE THAT A MAIN DRIVER FOR INTENSIFYING CONTROLS IS THE OCCURRENCE OF AN INCIDENT

95%

SAY THERE SHOULD BE MORE COLLABORATION BEYOND ONE'S OWN COMPANY TO SUCCESSFULLY FIGHT CYBER CRIME

TACKLING CYBER THREATS

THREE KEY PRIORITIES

It has often been stated that in a world where everything is interconnected, data is the new oil. The pace of technological progress is astounding and the world has become a village when it comes to communication and interaction. The classic boundaries of organizations – and their information systems – are blurred, while in all markets they can pursue success only through working in agile coalitions with partners. In the light of these developments, one fact is very clear: control of your data and systems is essential to achieve strategic goals.



You can't manage what you don't know.



The challenge is that risks are growing in this domain. It is easier than ever before to buy do-it-yourself malicious software; the strong mutual dependencies in a network-based society bring along new vulnerabilities. Cyber crime shifts from amateurs to resourceful organized crime groups, which perform focused attacks for espionage or massive disruptions of systems. And hacktivists have discovered cyber crime is an effective means to make their views heard by bringing sensitive information into the public domain. In short, cyber crime is growing in scale and sophistication. And the stakes are high.

① The issue of Cyber Security suffers from a lack of insight

The survey shows that many organizations lack proper insights, both in terms of the outside threats and in terms of what's at stake for their organizations. This is a serious impediment to proper management of the risks, as managing starts with taking informed decisions. The mantra "what gets measured gets managed" deserves more attention.

② We need to shift from a technological approach to a more balanced approach focused on people, technology and processes

The survey – combined with the interviews – clearly indicates the pitfalls of treating Cyber Security as a purely technological challenge. To effectively deal with the issue of cyber crime, we must place more focus on the human perspective, thereby implementing a more balanced and holistic approach. Technical vendors should not dominate the field of Cyber Security.

③ Organizations should aim to develop their cyber capabilities from reactive to predictive

The field of cyber crime continues to evolve at high speed. Sophisticated approaches may help high profile organizations to minimize risk by building capabilities for predictive analysis of threats. Sharing information between organizations will be very helpful in taking this step.

You will find a more detailed analysis of these key points on the following pages.

63%

consider themselves
an attractive
cyber threats target

95%

state they cannot defend themselves in isolation

31%

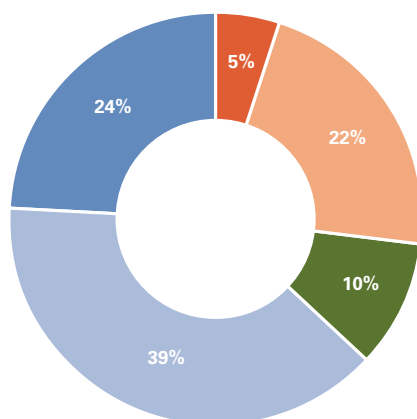
struggle to understand how
their data could be accessed
by hackers

36%

believe employees are
sufficiently aware of the
cyber risk

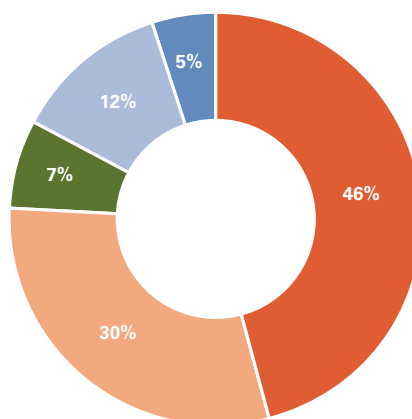
OUR ORGANIZATION IS AN ATTRACTIVE TARGET FOR ATTACKERS

All companies surveyed



CYBER CRIME IS A HYPE THAT WILL SUBSIDE

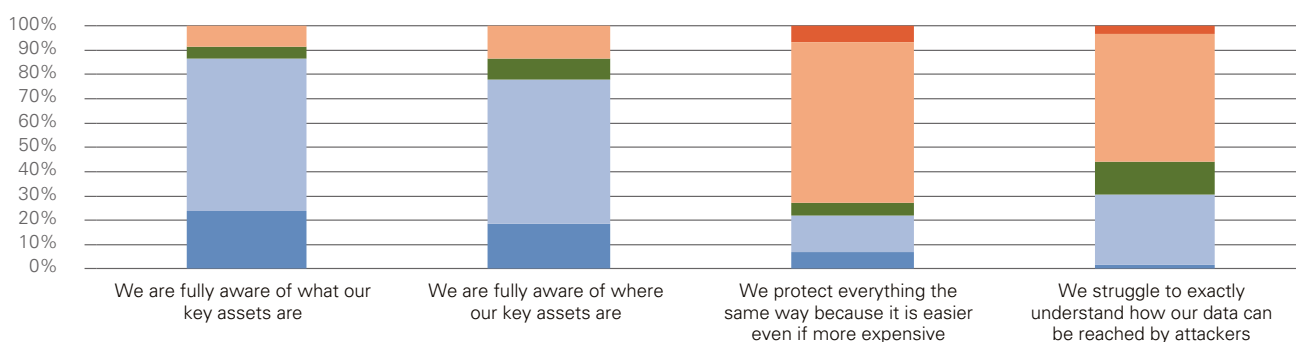
All companies surveyed



Strongly disagree
Disagree
Undecided
Agree
Strongly agree

OPINION ON EACH STATEMENT

All companies surveyed



INTERVIEW SWISSCOM

MORE FOCUS ON EASE OF USE

What would you consider the biggest challenges in Cyber Security at this moment?

First of all, the challenge is far from new. It has been around for many years and the struggle has always been to put the bits and pieces together in an effective way. For us, one of the challenges right now is to bring the physical world together with the cyber world. To do so, we need seamless cooperation between Cyber Security experts on the one hand and the engineers that are responsible for buildings and installations on the other hand.

What do you expect from the future? Do you see any specific areas where the threat landscape will evolve?

Typically, there are five types of attackers: the vandal, the criminal, the hacker, the terrorist and the hostile nation. We could divide these types into opportunists and more targeted attackers. I expect that the opportunistic attacks will continue to occur as they have done in recent years. I feel that we should worry more about targeted attacks that are becoming sophisticated. Attackers start combining different techniques and thereby innovate their strategies. Moreover, there is an important difference between espionage and sabotage. Where it comes to espionage, we can see patterns and we can at least monitor what attackers are trying to do. However, where it comes to sabotage, the intruder may already have obtained strategic places in your network and is just waiting for the right moment to push the kill switch. The answer to this threat is not an easy one. We should at least realize that we are probably being compromised right now. The question is not if we are

compromised. The question is how do we deal with it and how do we minimize consequences.

What key messages would you have for companies setting up effective Cyber Security programs? And do you see any aspects of Cyber Security that deserve more attention?

Let me give you three domains to focus on. First of all, we should focus on getting the basics of Cyber Security right. Second, and this is a lot more challenging, we should put more focus on ease of use for the user where it comes to protection measures. We must look at these measures from the perspective of the user, not from the perspective of technology. If it's too much work or if it feels like a hassle, users simply won't adapt to secure routines. I see a lot of potential for using the smart phone as a security token, for face recognition and other easy to use approaches. And thirdly, we must improve our detection techniques.

Stop the technological monoculture when it comes to Cyber Security. Start building up multi-disciplined intelligence on the issue. And focus on the user.

These are some of the key messages of Roger Halbheer, who is responsible for the Cyber Security domain at Swisscom.

Do you agree that there is too much emphasis on technology and too little on processes and people?

Some security companies tend to sell features instead of solutions. As a consequence, many Cyber Security programs concentrate on implementing tools, while forgetting about what is necessary to turn these tools into solutions. Another persistent problem is that the fear strategy is still dominant in this domain. It's very hard to get rid of this: we have even become accustomed to the fact that we use the terminology of fighting a war. It would be

“

It would be better if we started seeing Cyber Security more as a fact of life. As a natural given fact.

”

better if we started seeing Cyber Security more as a fact of life. As a natural given fact. As a flu that inevitably comes up now and then and needs attention. Not as a war.

What's your take on the compliance frameworks with regard to Cyber Security?

Many compliance procedures are focused on how we deal with the incidents and attacks we see. However, these are not my main concern. I am more worried about the threats that are not yet on our radar. Compliance may however force us to focus on following the right procedures and checking the proper boxes for the incidents we see. That can be an extremely counterproductive reflex while we need to focus on the real danger. We really need to focus on better threat intelligence, not on stricter compliance.

Do you see opportunities for better threat intelligence?

Absolutely. First of all in terms of better cooperation between organizations who share similar challenges. A near miss database would be fantastic, but this will probably be hard to realize as there are obstacles in sharing sensitive information. Apart from that, there are other options. We can enrich our insights by combining data from different sources and by combining data with issues from the past. It is important to avoid a specialist blindness, which is why I am looking for sociologists and statisticians in my team. They can bring new perspectives. Which is exactly what we need in the Cyber Security domain.

Roger Halbheer



A LACK OF INSIGHT INTO THE ISSUE OF CYBER SECURITY

At first glance, the results of our survey seem to be comforting. A vast majority, 86%, of respondents state that they are fully aware of what assets they need to protect and 78% state that they also are fully aware of where these assets are.

This contradicts our own experience and also some of the interviews we conducted: in reality, most companies struggle to grasp what cyber crime really means for their organization. This constitutes a gap between an intuitive and operational knowledge of the assets.

Moreover, the information processes about threats, risks and solutions tend to be dominated by technological buzz words. This further contributes to the sense of mystery that surrounds Cyber Security for management and it blurs their perception of the subject. Many executives struggle to grasp what is really going on and debunking the lingo of the security industry is essential in making them understand what is and what can be at stake.

This is also reflected in the fact that almost half of the respondents (44%) state that the Executive Board does not have any method to measure the cyber risk to the business. Slightly more than half (53%) state that the risk appetite related to cyber crime is discussed at Executive Board level. This is an issue in terms of proper risk management and defining the risk appetite.

Furthermore, companies seem to grope in the dark when it comes to measuring the return on security investments: 39% of respondents do not monitor the aggregate damage (i.e. direct and indirect) of a cyber attack. This lack of information would not be acceptable in many other investment

categories, where return on investment is a key metric for decision makers. Among large enterprises, this figure is even higher with 50% of respondents having no insights into the damage. A possible explanation is that measurement of the impact is more complex in larger organizations.

All in all, it seems fair to say that many organizations lack the necessary insights to be able to take informed decisions when it comes to Cyber Security. This is a serious issue and IT leadership should simply not accept this. They need to be able to make well-informed investment decisions that address Cyber Security risks. By doing so, they can engage business sponsors and build understanding, confidence and credibility. In practice, this is largely done in a rather reactive way.

This is in stark contrast to other management areas – such as commercial information – where relevant insights are often just a few clicks away to justify strategic decisions, such as acquisitions or an entry into new market segments. There's no reason why insights into Cyber Security should not be available at a comparable level. Moreover, such insights are highly significant: a lack of effective Cyber Security may have serious consequences and may even hamper organizations in reaching their strategic goals.

A professionalization of insights is the foundation for applying a risk management approach to dealing with Cyber Security. In essence, Cyber Security means performing a risk assessment from the perspective of the organization as well as the attacker (prevention), identifying and analyzing critical assets (detection), and implementing a standby incident response organization (response). The success of such an approach, however, is dependent on solid insights.

58%

of respondents say that IT security does not report directly to the Executive Board

44%

of Executive Boards are not sufficiently aware of the risks of Cyber Crime

51%

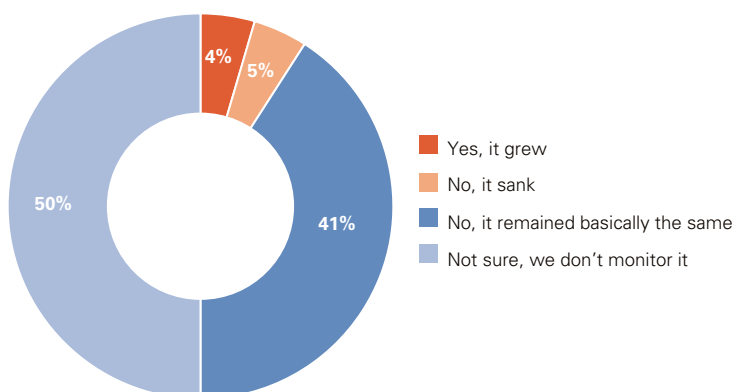
cannot detect ongoing attacks

59%

are not convinced their service providers know how to defend against cyber attacks

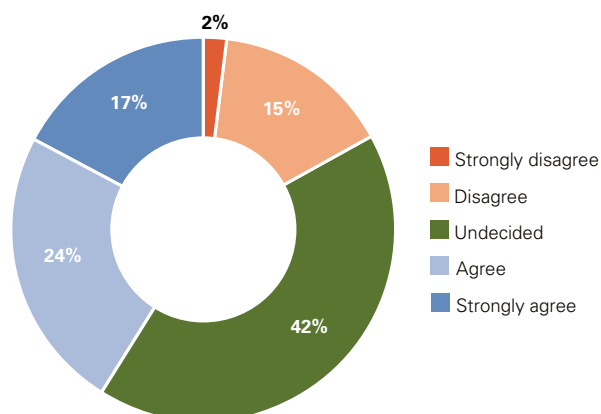
DID THE AGGREGATE DAMAGE (DIRECT AND INDIRECT) GROW COMPARED TO THE PREVIOUS TWELVE MONTHS?

Companies > 5,000 FTE's



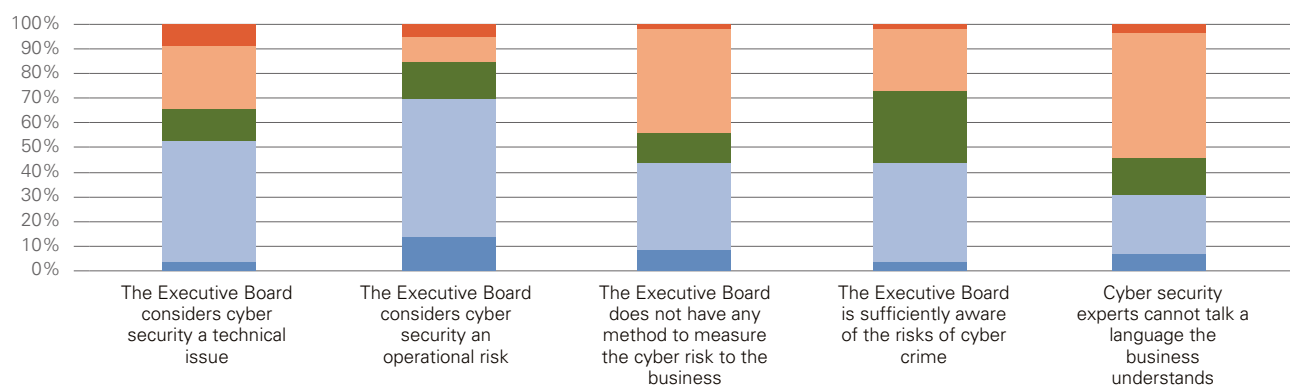
OUR PROVIDERS UNDERSTAND HOW TO DEFEND AGAINST CYBER ATTACKS

All companies surveyed



OPINION ON EACH STATEMENT

All companies surveyed



INTERVIEW HELSANA GROUP

THE HEALTH INSURANCE SECTOR IS A STABLE INDUSTRY

Is the health insurance sector an attractive target for hackers?

In my experience not really. Our industry is quite stable and calm because financial interests are not paramount as, for example, in the banking sector. Address information and physical health details of the customer, which are subject to the data protection law and professional secrecy, might be of interest since they can be turned into money. Furthermore such incidents would damage our reputation. Industrial espionage is rather irrelevant for our sector, as new insurance products are developed over years and are therefore not of interest.

What are the challenges in regards to Cyber Security?

The resilience of the security processes and the organization and availability of the security operations center (SOC) are our biggest concerns. We want to implement proactive solutions in the area of IS governance and the SOC, and will establish reporting lines to the responsible authorities.

Many companies only begin to invest in IT after an incident occurs. Do you agree?

Absolutely. Usually the executive management does not know what happens in the cyber area. The security specialists are being called to report on the situation only after an incident occurred. On the other hand, we are in

regular contact with the CIO and several members of the executive board.

How important is the exchange with other companies?

Very important. An exchange among insurance companies is being organized up to four times a year, where we openly talk about information security topics,

as for example incidents and potential risks. In my opinion it is necessary that such meetings are being organized and moderated by an external person.

Can companies be considered secure when outsourcing their IT-departments?

There is always a risk. Today the dependency on outsourcing and cloud services increases. Everything is specified in the

The health insurance sector is at present not an attractive target for hackers. The exchange among companies of the industry is important. Outsourcing and cloud services pose a risk. The third-party providers have good security measures nowadays.

These are the key statements from Stefan Burau, who is responsible for information security at Helsana Group.

contract with the third-party provider. It is important in this context that the outsourcing or cloud provider has implemented a mature and well documented IT and IS governance control framework. Additionally it has to be tested whether service providers have established adequate security controls, which are reported regularly according to the scope of the services provided.

Do you agree that your organization is driven more by compliance than security?

On one hand I agree mostly in regards of data protection and the compliance to the Swiss data protection act, but on the other hand I am witnessing that the issue of security and governance have become more important than in the past.

“

It has to be tested whether service providers have established adequate security controls.

”

Stefan Bureau



WE NEED TO SHIFT FROM A TECHNOLOGICAL APPROACH TO A MORE BALANCED APPROACH FOCUSED ON PEOPLE, TECHNOLOGY AND PROCESSES

Half of the respondents state that their Executive Board considers Cyber Security a technical issue, whereas two thirds of respondents recognize that Cyber Security focuses too much on technology. This clearly implies a lack of attention to the other two pillars of a complete and balanced strategy: people and processes.

This finding is closely interlinked with the fact that Cyber Security is a relatively young issue. In a short period of time, the industry has evolved and introduced a series of concepts, tools and techniques. It may be tempting for executives to embrace these solutions in order to feel comfortable about the security of their organization and its digital assets. Everyone can buy security tools, while it is much more challenging to build up a holistic approach.

The reality is that technology is just one part of the equation in the domain of Cyber Security and an isolated technological approach will lead to a false sense of security. In other words, a fool with a tool is still a fool.

Organizations should adopt a more balanced approach. A Cyber Security strategy should be a cost-effective control of the cyber environment, addressing the coherent domains of people, processes and technology. The best way to do so is to put the user experience – not the technology – at the center of the Cyber Security approach. Cyber Security is not about tools and technologies; it is about people using those tools and technologies in a user-friendly, natural way. Professionals working in the security domain have a responsibility here:

they should not focus solely on the technology. They also need the skills to communicate about the issue in a broader sense in terms of people, processes and technology.



Put the user experience – not the technology – at the center of the Cyber Security approach.



Related to this is the fact that Cyber Security cannot be delegated to specialist departments. Cyber criminals may use advanced technologies to penetrate an organization, but may also try social engineering or benefit from careless employees. The level of security depends on the weakest link in the organization. Therefore, Cyber Security concerns all employees in an organization and should not be delegated to a group of specialists. Cyber Security is an attitude, not a department. To create awareness, the right tone at the top is an effective driver to get more focus on this issue. Executives that “walk the talk” – for instance, by demanding that their mobiles and tablets are secure – have a stronger impact on the rest of the organization. Executives that do not lead by example may run the risk that the rest of the organization lowers its security standards.

48%

say that employees are not sufficiently aware of cyber risk

61%

state Cyber Security is too much focused on technology

53%

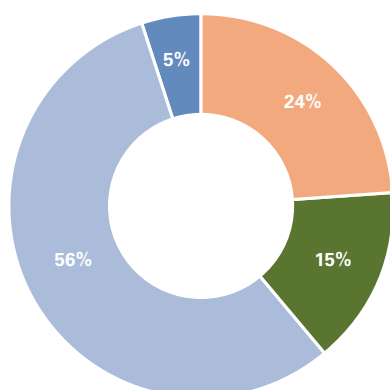
say their Executive Board considers Cyber Security a technical issue

31%

agree that Cyber Security experts cannot talk a language the business understands

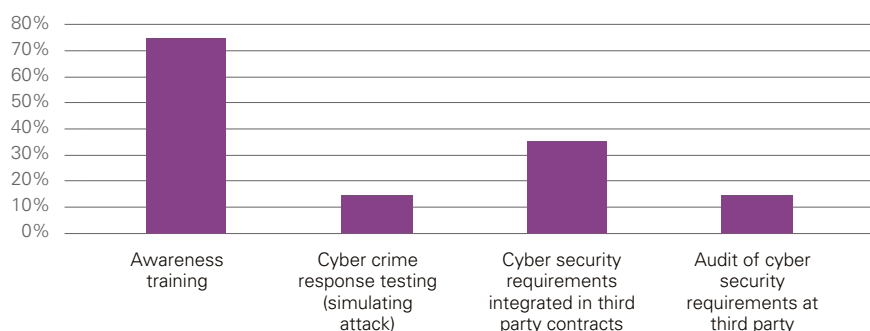
CYBER SECURITY IS TOO MUCH FOCUSED ON TECHNOLOGY

All companies surveyed



WHICH CONTROLS HAVE YOU IMPLEMENTED IN ORDER TO PREVENT CYBER ATTACKS

All companies surveyed



OPINION ON EACH STATEMENT

All companies surveyed



INTERVIEW ALPIQ

TREAT SECURITY AS A STRATEGIC ISSUE

In general, what's your view on the trends in the area of Cyber Security?

Köhler: Cyber Security has progressively become a dominant topic and both threat scenarios and attack vectors have become increasingly complex. In the past, it was possible to physically isolate sensitive data and systems. Nowadays, neither physical nor electronic isolation is a viable option. This high degree of complexity leads to a greater exposure to being attacked. That implies a big challenge for firms today: how are they going to tackle the complexity of these systems?

Meier: Nowadays, many processes are being managed via the cloud, and in many cases we do not know which kind of data is being viewed or accessed by whom persons. This is one of the reasons we shouldn't consider Cyber Security on a mere technical level. The human factor represents an essential and immense weakness when it comes to security. I observe a general lack of awareness on how to deal with information. People thoughtlessly give away information to the public, which leads to the opportunity to observe and spy. It is crucial that society becomes more aware of this threat.

Do you feel that companies tend to overemphasize the technical aspects of Cyber Security?

Köhler: Security will always depend on a combination of both the human factor (their behavior) and the situation. People should be monitored and checks conducted not only regarding data leak prevention but also in terms of Identity

Access Management. Firms become vulnerable when employees are frustrated or have left the company being dissatisfied. This represents a real risk in the broader sense, potentially leading to sabotage or data theft.

Meier: In our organization, we highlight the importance of the human dimension by putting an emphasis on culture. We generate more awareness under the motto "lived by all". Security has to be in people's minds. The security team has to develop the mantra so that each and every one believes in it and can and will incorporate this value.

Although awareness on Cyber Security has risen considerably in the past years, this may not have kept up with the fast changing reality. One of the challenges in building a cyber resilient organization: to treat Cyber Security as a strategic topic, instead of opting for panic driven actions following incidents.

These are the key statements from Werner Meier
Head Group Security and Urs Köhler
Information Security Officer of Alpiq AG.

What's the best strategy to involve board members in this domain?

Meier: Cyber Security is linked to bringing up bad news, which no one wants to hear and no one wants to pay for. That's a classic dilemma for security officers and there is no easy remedy. Security has to be a strategic topic and needs to be addressed in "management language," which is fairly difficult. Cyber Security is often

merely being viewed as a sub topic. But in case of something happening, everybody suddenly states "Why didn't you do anything against it? How could that happen?" Then, all of a sudden, it becomes a key topic again. The problem here is the risk of potential panic reactions followed by a weakening movement when the bad news fades. Treating security as a strategic topic is the answer to that dilemma.

Köhler: Internal Audit plays an important role as the interface that communicates to the board. Paired with integrated safety, this helps us having proper access to the board. The

Urs Köhler



Werner Meier



audit and risk committee pays the attention it needs to that particular topic.

How do you perceive the risk of attacks via suppliers?

Köhler: We put a lot of effort in choosing our partners. We want to know how the processes work at the providers and also assess these. If you manage to define specific parameters, you will enjoy great quality paired with security. It is not only a matter of purchasing at low cost, you also have to assess these parameters. It is likely that we do not possess all the necessary qualitative instruments yet to conduct these checks. However, there are opportunities. In SLA's, it will be decided whether and to what extent the services have been delivered. We can monitor this process, which is subject to constant improvement. A process is of no use if you cannot check it.

“

The human factor represents an essential and immense weakness.

”

FROM REACTIVE TO PREDICTIVE

ORGANIZATIONS MUST DEVELOP THEIR CYBER CAPABILITIES



Incidents are still the main driver for investments in Cyber Security.



Our survey shows that the main driver (75% of respondents agree) of intensification of controls is the occurrence of an incident. This reflex may not be very surprising and is understandable. However, it is also a clear sign that many cyber strategies are largely reactive. This immaturity may also mean that organizations focus on the wrong areas: they probably miss upcoming issues and will almost inevitably be overwhelmed by a continuously changing technological landscape.

Closely related to this is our finding that compliance seems to be a dominant factor when it comes to investing in Cyber Security. Just over half of the respondents feel that their organization is driven more by compliance than security. At the same time, most of them leverage compliance to achieve security targets. In practice, the differences between various organizations and sectors are huge in this respect. Some organizations are driven solely by a response

to incidents. Their reactive investments in the Cyber Security domain are driven by fear. On the other side of the spectrum are organizations that have a lot more self-confidence. By continuously scanning threats and analyzing data patterns, they have developed capabilities to predict the character and nature of future events.

The maturity level of organizations can roughly be divided into four stages of cyber strategies, ranging from reactive, structured, and integrated to predictive.

To achieve the highest level of maturity – which is key for high-profile organizations where the stakes are high – organizations must find new ways. They should of course focus on being well informed of possible threats and invest in a proper defense. However, they should not do this in an isolated way, but rather use the knowledge and experience of peers, both in the public and private sector. A joint effort is essential to the maintenance of a high level of intelligence. This is underscored by the results of our survey: nearly all respondents are convinced that they cannot defend themselves in isolation and that there should be more collaboration.

Another important aspect is better knowledge management. Insights can be enriched by smart combinations of data from different sources and by combining data with issues from the past. A multidisciplinary approach helps to avoid specialist blindness and brings in the necessary new perspectives to improve predictions of risk areas.

37%

say that an attack on a competitor
or third party provider is a reason for
intensifying controls

51%

of respondents say that a
main reason for intensifying
controls is an increased awareness
of the senior management

75%

of respondents agree that a
main driver for intensifying
controls is the occurrence of
an incident

55%

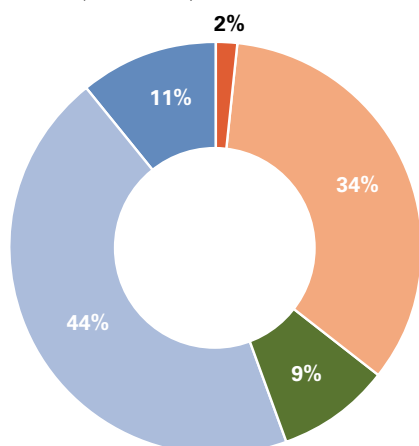
say their organization is
compliance rather than
security-driven

51%

believe that cyber attacks
cannot be prevented

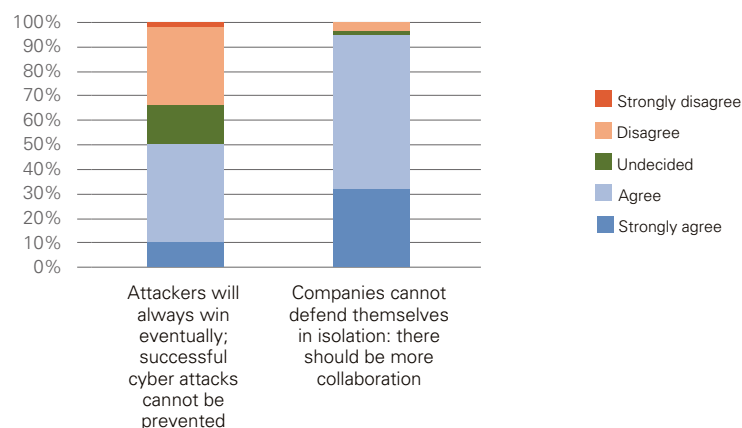
OUR ORGANIZATION IS MORE DRIVEN BY COMPLIANCE THAN SECURITY

All companies surveyed



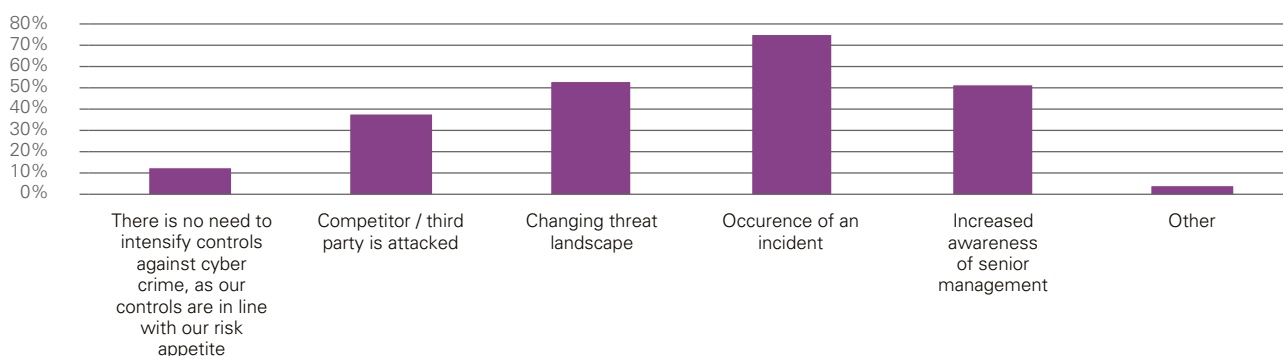
OPINION ON EACH STATEMENT

All companies surveyed



IN YOUR ORGANIZATION, WHAT ARE THE EXECUTIVE BOARD DRIVERS FOR INTENSIFYING CONTROLS AGAINST CYBER CRIME?

All companies surveyed



INTERVIEW MELANI

FURTHER INTERCHANGE AND COMPETENCE DEVELOPMENTS ARE VITAL

What are the biggest challenges and areas of concern regarding Cyber Security?

We note an increasing number of targeted and professionally executed attacks. According to a study it is SME's with 10-100 employees who are more and more becoming the focus of attacks. Most attackers want to obtain financial resources e.g. by stealing credit card data, launching attacks on e-banking customers or by means of economic espionage (spear phishing). Attacks on critical infrastructure like power plants can have severe consequences. The awareness of many companies is insufficient to some extent, for example if internal information is sent unprotected by email. We are constantly in close contact with over 100 companies to give advice on how to protect oneself best nowadays. MELANI is in the fortunate position to be able to pass on information to its customers that is not accessible to the public.

Another challenge is the identification and arrest of the perpetrators (hackers). Not all countries provide legal assistance to Switzerland. Moreover, it is extremely difficult to locate these perpetrators.

What are the key measures to limit the (impact of the) attacks?

The interchange between companies and the government is important. Without the collaboration with other

companies or government authorities, it will be extremely difficult to protect oneself against the newest attacks. We organize workshops with the biggest Swiss companies once or twice a year. Mainly with companies from the finance, telecommunications and energy sectors. In the past, many did not dare to talk openly about attacks. Today entrepreneurs become more open and even interchange with direct competitors, which I see as a very positive development.

A further measure is the establishment of expertise. Ever so often the companies lack the necessary technical specialists and/or the financial resources.

We use a protected portal for the exchange of information within our

customer base. We irregularly inform SME's and the public in a newsletter about incidents that, according to our assessment, pose a risk to a majority of the population.

Targeted attacks are increasing and are being executed more professionally. As a consequence, companies are more dependent on interchanging knowledge among each other. The cyber subject is often still being underestimated on management level.

These are Max Klaus' key statements, deputy head of MELANI, the Reporting and Analysis Centre for Information Assurance in Switzerland.

Many companies do not start to invest in their IT until they are attacked. What is your experience?

Often management underestimates the cyber topic as long as no incidents occur. In addition, plans, for example with regard to continuity management, are often insufficiently established. There is no time to prepare when an attack takes place. The crisis and communication plans and the corresponding processes have to be implemented in advance.

“

Without collaboration it will be extremely difficult to protect oneself.

”

Are the companies safe when outsourcing their IT department?

Outsourcing/cloud can lead to problems, as the data is entrusted to a third-party provider. One has to trust that the host of the cloud handles data reliably, performs backups regularly, does not pass on data to third parties, protects the server farms adequately and so forth. Outsourcing and cloud services are suitable for non-sensitive data. However, sensitive data (results of research, construction plans, etc.) should, if possible, remain under the control of the company.

How does Switzerland compare to other countries with regard to Cyber Security?

In essence, Switzerland is exposed to the same threats as every other country. Switzerland has a national cyber strategy („National strategy for Switzerland’s protection against cyber risks”) which states the main risks, recommends actions and takes the development of competencies into consideration. In comparison to similar strategies abroad, the Swiss strategy provides specific measures and a plan for the implementation of the measures. During ten years of operation, MELANI established an international network to similar organizations and specialists all over the globe, as well as to important manufacturers (e.g. Microsoft, Google, developers of anti-virus software). These contacts can be the key to success when handling time sensitive incidents.

Max Klaus



INTERVIEW BALOISE MANAGEMENT'S AWARENESS IS CRUCIAL

What does information security mean for Baloise insurance?

„Making you safer“ is an essential element of the culture and purpose of Baloise Insurance. Needless to say, this applies to us in IT as well. Hence, a systematic approach for the management of information and IT security has been established on group level for years. Advancement of digitization has led to increasing risks related to the protection of sensitive data within the company as well as the vulnerabilities of IT systems.

What are the key drivers for these risks?

Key drivers are increased interconnectedness and the company's interactions with stakeholders and clients across digital channels, the use of mobile devices with access to the company's IT system and data, as well as the global professionalization of cybercrime. Baloise Insurance is continuously adjusting the established protective measures to these new threats and risk

scenarios. The topic of "Cyber Security" has, especially by means of high presence in the media, led to the advancement of information security management in regards of prevention, detection and handling of respective incidents.

How important is the human factor?

An integral part of effective measures consists of building employee's awareness and staff training, since many attacks target deficiencies in this area. Here we rely on playful awareness campaigns (gamification). The established measures have thus far proved to be an effective protection

The topic of "Cyber Security" has led to the advancement of information security management in regards to prevention, detection and handling of respective incidents.

This is one of the key statements of Olaf Romer, Head of Corporate IT, Group CIO of Baloise Insurance.

against notable incidents or loss of data, however, one hundred percent security can never be guaranteed. The extent of future investment in Cyber Security is heavily dependent on top management's awareness in regard to the company's vulnerability.

“

Key drivers are increased interconnectedness and the company's interactions with stakeholders and clients across digital channels, the use of mobile devices with access to the company's IT system and data, as well as the global professionalization of cybercrime.

”

Olaf Romer



DISTRIBUTION OF SURVEY PARTICIPANTS BY SECTOR



40.6%
FINANCIAL SERVICES



3.1%
PHARMACEUTICAL



4.7%
INFRASTRUCTURE



7.8%
ENERGY AND NATURAL
RESOURCES



4.7%
COMMUNICATION/
ENTERTAINMENT



9.4%
GOVERNMENT



9.4%
PROFESSIONAL SERVICES



3.1%
HEALTHCARE



12.5%
CONSUMER/
INDUSTRIAL



4.7%
OTHER



SURVEY METHODOLOGY

KPMG conducted this Cyber Security survey of Swiss companies in 2015. 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 if they have established practices and measures and how they have been implemented. The 64 participants, of which 27 were large enterprises (> 5,000 FTEs) and 37 small and mid-size companies (SMEs), received 30 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.

KPMG

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.



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.



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.



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.

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.

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.

WE ARE ...


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.



A person wearing a blue patterned shirt is resting their head on a wooden bar counter. The background is a blurred bar area with various bottles on shelves. The text is overlaid in a white, handwritten style.

If you can
read this you
should apply
for a job
with KPMG!

kpmg.ch/cyberjobs

Clarity on

Online publications

KPMG Switzerland's Clarity on series provides a wide range of studies, analyses and insights. You can find more information at kpmg.ch/clarity-on.

Latest issues



Clarity on **Investment in Switzerland**



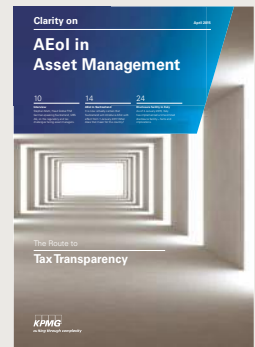
Clarity on **Performance of Swiss Private Banks**



Clarity on **Digital Transformation**



Clarity on **Swiss Taxes**



Clarity on **AEol in Asset Management**



Clarity on **Mergers & Acquisitions**



Clarity on **Life Insurance matters**



Clarity on **Healthcare**



Clarity on **Commodities Trading**



Clarity on **The Future of Swiss Private Banking**

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.



kpmg.ch/knowledge

IMPRINT AND CONTACTS

For further information on
Clarity on Cyber Security
please contact:

Matthias Bossardt

Partner, Cyber Security
+41 58 249 36 98
mbossardt@kpmg.com

Jean-Paul Ballerini

Senior Manager, Cyber Security
+41 58 249 55 64
jballerini@kpmg.com

Gerben Schreurs

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

Roman Haltinner

Senior Manager, Cyber Security
+41 58 249 42 56
rhaltinner@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
Jean-Paul Ballerini
Roman Haltinner
Rikard Sandström
Konrad Schwenke

Anne van Heerden

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

Ulrich Amberg

Partner, Head of IT Advisory
+41 58 249 62 62
uamberg@kpmg.com

Concept and design

KPMG, Stephan Erdmann
KPMG, Irene Hug
Konkret, Andi Portmann

Print

GfK PrintCenter, Hergiswil

Pictures

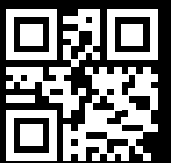
Shutterstock



Articles may only be republished by written permission of the publisher and 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.

© 2015 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss legal entity. All rights reserved.



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