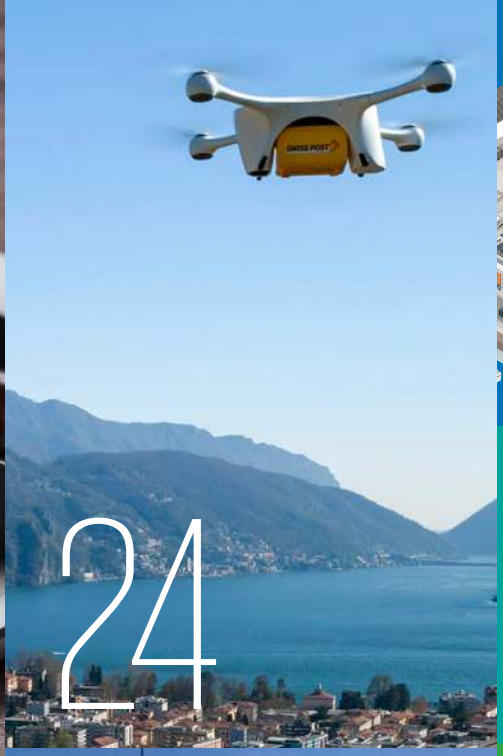
Clarity on Cyber Security

Ahead of the next curve

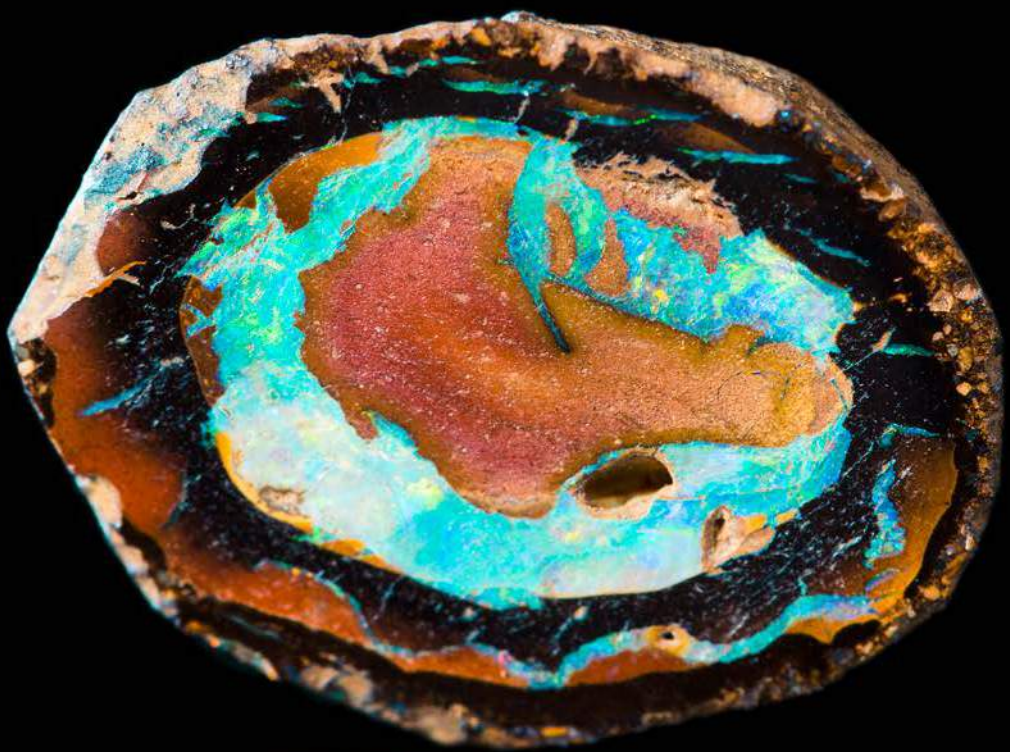
May 2017



CONTENT

Clarity on Cyber Security

Organizations must have insight into what's at stake - mapping the crown jewels is key to building a successful cyber strategy.



EDITORIAL

Ahead of the next curve

Matthias Bossardt
Partner, Head of Cyber Security

Never a dull moment. This was the title of last year's Clarity on Cyber Security. The challenges in previous years prove that this couldn't be more true. Following several incidents, the topic of cyber security has earned a prominent place at the table of the world's political leaders as it influences society, state sovereignty and economy; the Fourth Industrial Revolution leads us into a world where everything is interconnected at dazzling speed; and attackers deploy even more advanced and professional strategies than before.

It may be difficult to cope with the speed of change. However, this is what makes cyber security so interesting. This year's survey highlights current challenges as well as looking beyond the next curve in the evolving cyber security journey. We analyze how Swiss organizations build cyber resilience. We also delve into new domains that are not yet mature but that nonetheless deserve our attention now. Domains such as the use of Artificial Intelligence in business processes in cyber measures.

In all this turbulence and complexity, one certainty stands out. A good cyber security approach takes the business – not technological vulnerabilities – as a starting point. A business-centered approach, rather than a technology driven approach, is needed. This means that organizations must have insight into what's at stake – mapping their crown jewels – and build a cyber strategy based on these insights rather than starting with working out their technological vulnerabilities.

This requires a major rethink in many organizations as it is not yet common practice. Most executives think of two things when they hear the term 'cyber security'. One, it's nothing more than an IT challenge. And two, it's about compliance. In fact, it's way more than that. What's needed is a Risk Management approach based on business objectives. The first step is to identify the crown jewels. This is the basis for classifying data and systems. So that the focus of security measures and policies is on the information assets that matter most. Part of this is to assess the risk profile in the value chain. Maintaining a dialogue with vendors and other partners on the risks in the value chain is essential.

Trendsetters have started to embrace this strategic focus. They prove that this not only leads to excellence in cyber security. But that cyber preparedness enhances the company's agility and better positions it for innovation and growth. In other words: excelling in cyber security is also an excellent business opportunity.

We hope that the content of this publication inspires you to stay ahead of the next curve by tackling cyber challenges so that your business achieves its strategic ambitions with agility and confidence in the digital age.

Matthias Bossardt

Cyber security moves beyond irritation

The human factor was, is, and will always be, the weakest link. Data breaches can often be traced to social engineering and human error. That's not just a matter of careless users. It's also a design problem. Security by design offers powerful potential to improve the user experience. To succeed, we must offer users a seamless experience instead of irritating time-consuming measures.

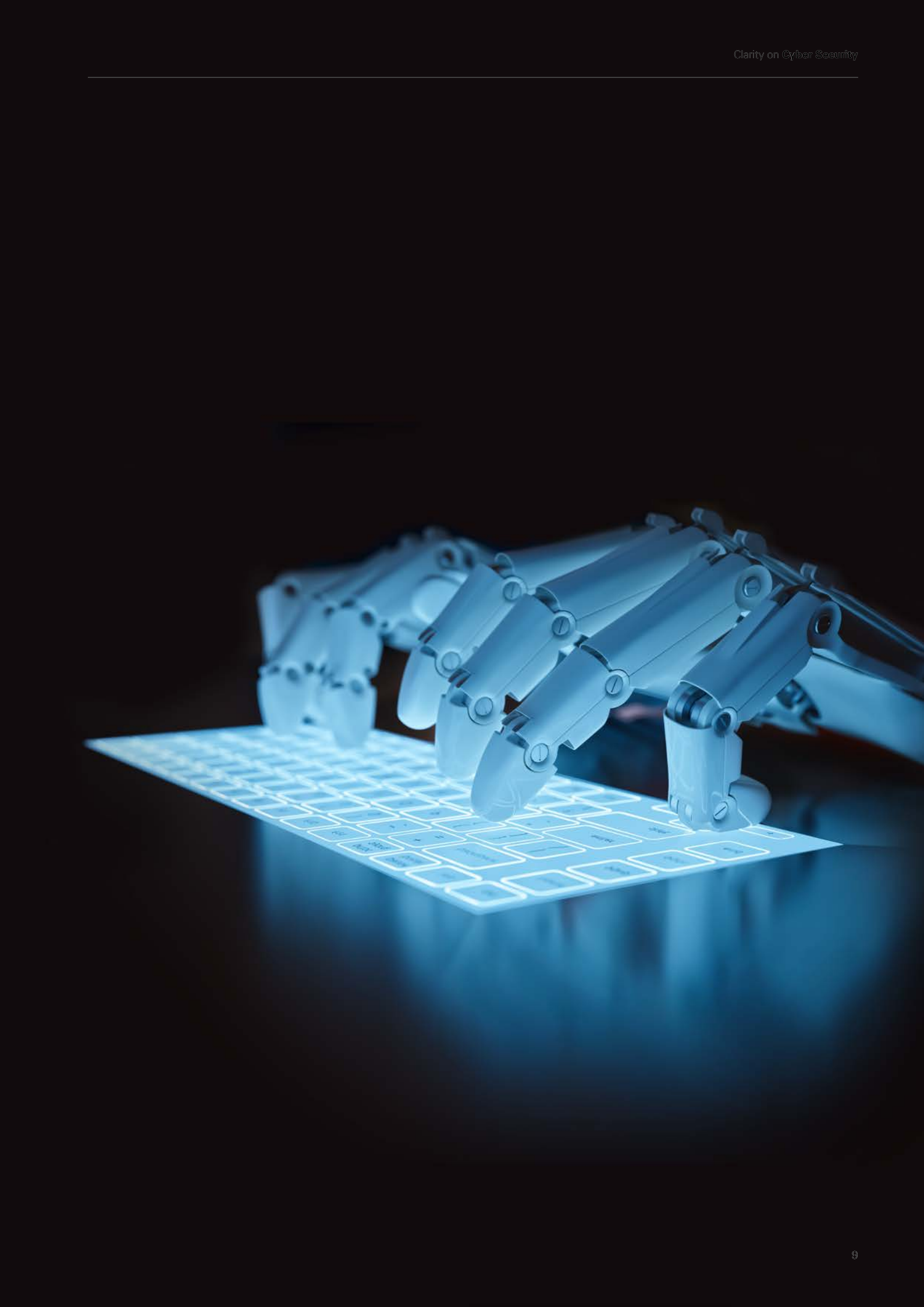
Cyber security moves beyond cyberspace

The Internet of Things is not just some fancy futuristic world. It's here today: a complex world full of connected things ranging from personal gadgets and household appliances to medical devices and critical infrastructures that are all networked. The physical world integrates with cyberspace. Cyber security strategies must anticipate that.


Things

Cyber security moves beyond human versus machine

Artificial Intelligence is essentially about smart machines that are able to automate complex and comprehensive processes and support humans in critical decision making. Attacks on such smart machines may have significant consequences for the resilience of our industries, economies and the systems that govern nation states. The concept of Artificial Intelligence also makes its entrance in attack and defense strategies. The idea of machine versus machine is no longer an idea for the future. Think about it before it pops up as a surprise.



Key findings

Cyber attacks are increasing

88% of respondents suffered a cyber-attack in the past 12 months (2016: 54%).

56% had to deal with a disruption of business processes (2016: 44%), 37% with reputational damage (2016: 24%), 36% with financial loss (2016: 36%) as a consequence of cyber attacks.

A deeper understanding of cyber risks is evolving

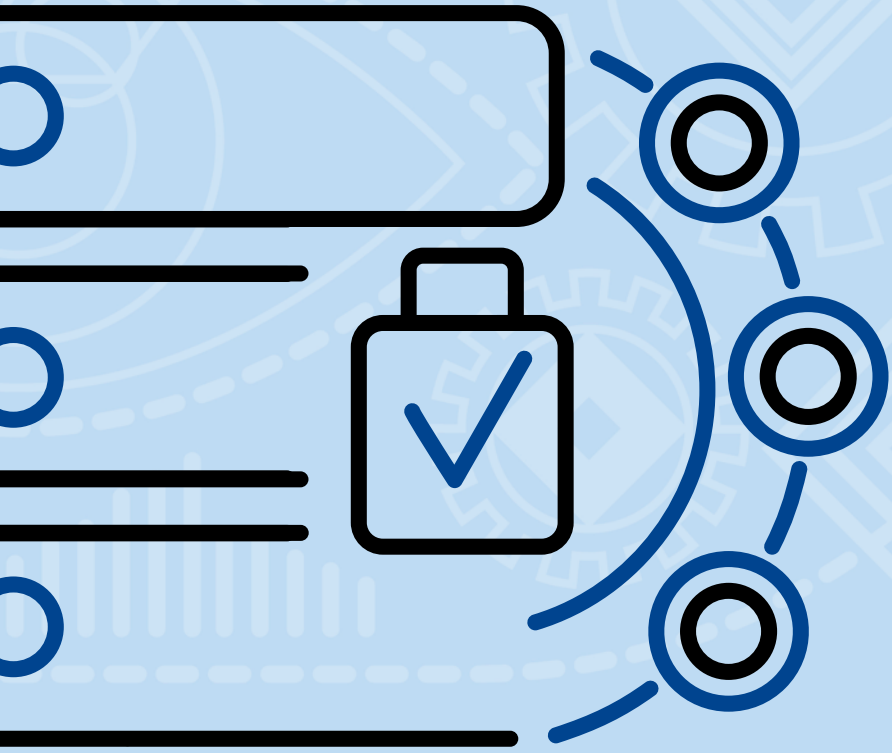
81% confirm that they have gained a deeper understanding of cyber risks in the past 12 months.

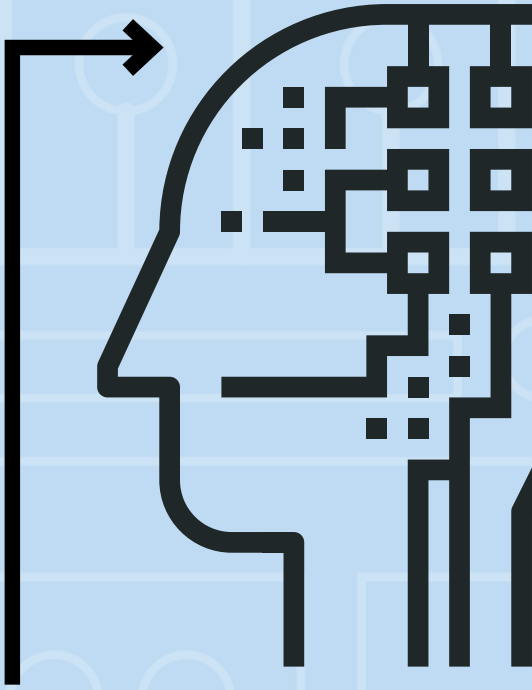
52% have gained better understanding of the attacker's motivation, strategy, and tools, 44% state that their prediction capabilities have improved.

The human factor in Cyber Security

65% confirm that their organization does not systematically work on cyber security measures that are user-friendly.

11% involve a UX specialist to achieve user-friendly security design.





Cyber Security and product/ service design

48% embed cyber security measures systematically in product/service design processes compared to 65% embedding data protection/privacy measures.

IoT concerns

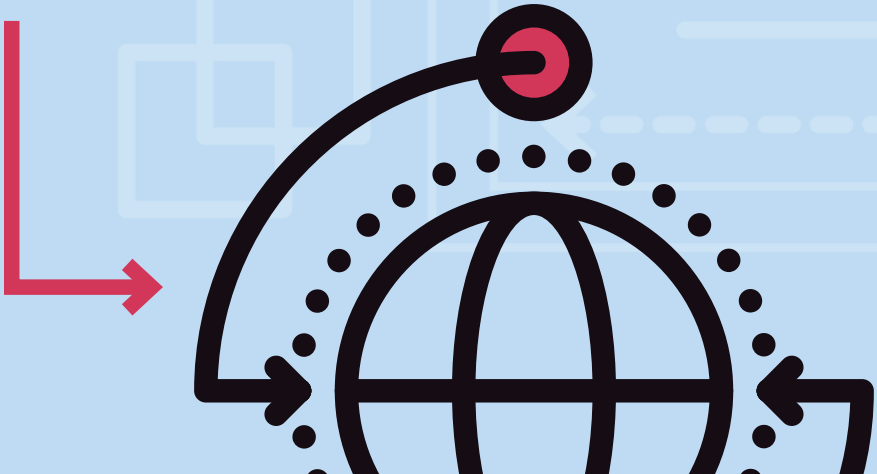
59% state that their main concerns regarding IoT-related risks are exotic devices that are introduced in the organization's network and the fact that traditional controls are no longer effective (also 59%).

Struggling with Internet of Things (IoT)

48% include IoT or operational technology (OT) assets in their cyber security strategy and policy.

33% report that they have gained better insights into the landscape of the relevant IoT devices in the past 12 months.

31% have an overview of IoT and operational technology (OT) devices deployed in their organization, 35% did not try to get an overview in the past 12 months (2016: 53%), 17% tried to get an overview, but did not succeed.



Slow anticipation of artificial intelligence

43% believe that the rise of AI will lead to new challenges in cyber security within 2–3 years, while only 26% think that the rise of AI leads to new challenges in cyber security now.

12% analyze the security impact of potential AI use cases systematically.

4% use AI to protect themselves from cyber threats, but 40% expect that AI is going to be used by attackers in the future.

Big Brother is already watching

Massive data collection is a fact of life for everyone. And algorithms gain massive influence on our daily lives. Dirk Helbing, Professor of Computational Social Science at ETH Zurich is convinced that we must learn to build information systems that operate with proper ethics. He points out that the current approach to fake news is ineffective or even countereffective and argues that we need a fundamentally new approach.

Picture: Davide Caenaro

Dirk Helbing, Professor of Computational Social Science at ETH Zurich

What developments will have the biggest impact on our lives over the next three to five years?

A lot of data is collected about us. This information can be used to manipulate people, and can also be used by hackers. This can influence not only our buying behavior, but also our political behavior and our opinions – people are being remotely controlled. This is also known as neuro-marketing. Such personalized marketing is more successful because it is tailored to the individual. We are not consciously aware of 95 percent of the information. The problem is that some of the people who use this method do not do so in a democratically legitimate way.

What are the ethical challenges of big data?

We are increasingly being controlled from the outside. We are losing individual control of our thoughts, feelings, actions and lives, and we are also facing the problem of hacker attacks on companies and critical infrastructures. These attacks are leading to an infiltration of society. It is becoming increasingly apparent that votes are being manipulated at the national level – and not only in and by Russia, as is often suggested.

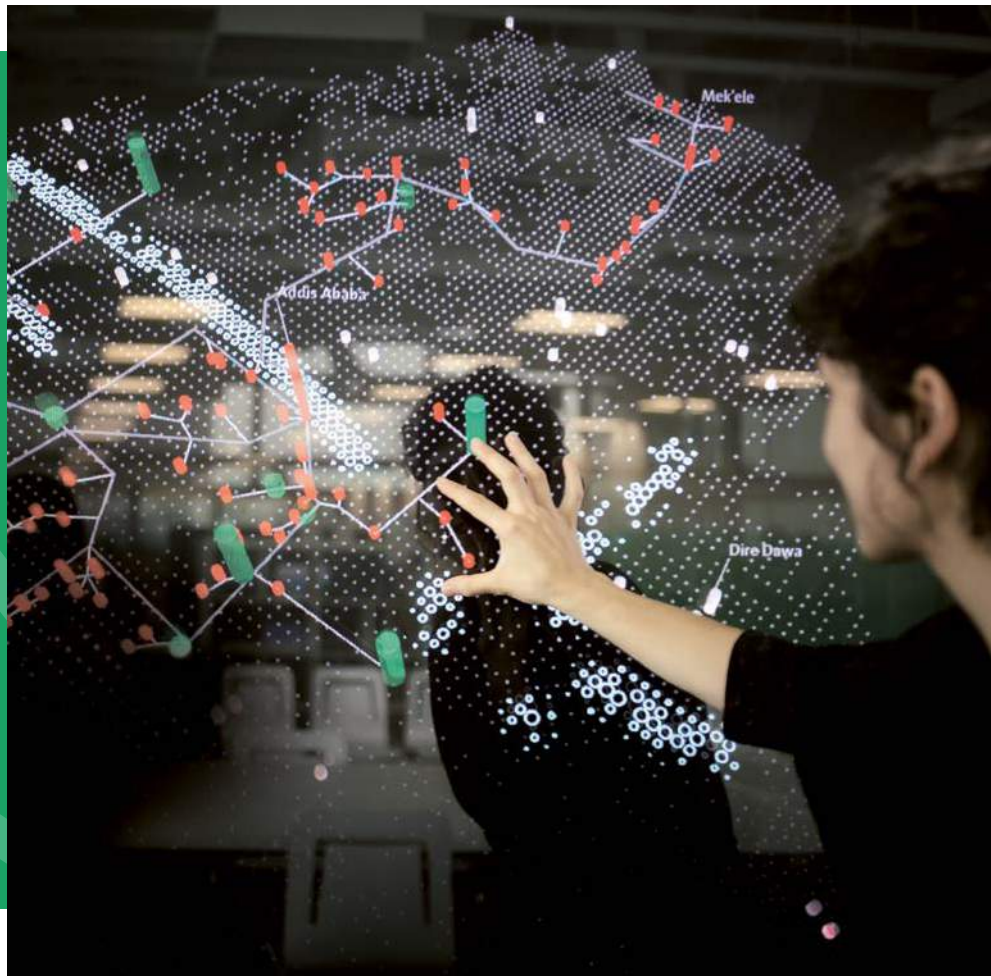
How should society respond to this?

There is a great deal of helplessness. Another problem is 'fake news', which is now being advanced as an argument for the introduction of censorship laws. But this is not compatible with democracy. There are also efforts to set up government agencies to provide information on what fake news is – 'ministries of truth', if you like. When you compare different national positions, though, such as in the US and Europe, you can see that it is simply a case of the elite retaining their status as opinion leaders – but citizens no longer trust them.

What do you make of the risks around data protection?

The risks are high, but at the moment you cannot effectively protect yourself. As soon as you use a browser, there are cookies that record what you click on, and this information is then resold. All these links contain a lot of information about us. Big Brother is already watching. We can't protect ourselves against it, because if we don't accept cookies then we can't use any services. It is untenable that we are so shamelessly researched. It makes us vulnerable. Apparently, someone can know us better from 300 Facebook clicks than our friends and partners do. I don't think it can continue like this. Society is being manipulated. People are increasingly living in filter bubbles and are losing the ability to understand people with a different attitude or from another culture.

"We need to integrate our society's values into technological systems."



What should be done?

We need a new approach, and this will hopefully come with the new data protection law. We need to integrate our society's values into technological systems. Today's information systems are incredibly powerful. Either they will destroy our society as we know it today, or the current technological approach must change. There is a great danger that human rights could be threatened; engineers have to learn to integrate and protect human values in their systems. This is why the Institute of Electrical and Electronics Engineers (IEEE) is currently developing a guide called *Ethically Aligned Design*.

Who determines these values?

There is currently a consultation process; people can get in contact and offer their views. Much of it is laid down in the constitution and there are various attributes that characterize democracy, such as the separation of powers, pluralism, the protection of minorities, participation and transparency. These characteristics must also be guaranteed in information systems; the question we must ask ourselves is how we can implement them. In terms of today's artificial intelligence systems, we are still very far away from such an implementation. They could do a lot of damage, for example with a Citizen Score.

What consequences does this have for society?

The digital revolution will fundamentally change our society. It is essential that we work actively to shape this transformation. This isn't easy, because it's not always clear exactly who is involved. There are also people who believe that from 2050, robots will take over our daily lives and people won't be required any more. This may be an extreme position, and one I don't share, but you can nevertheless see that we will be facing significant challenges.

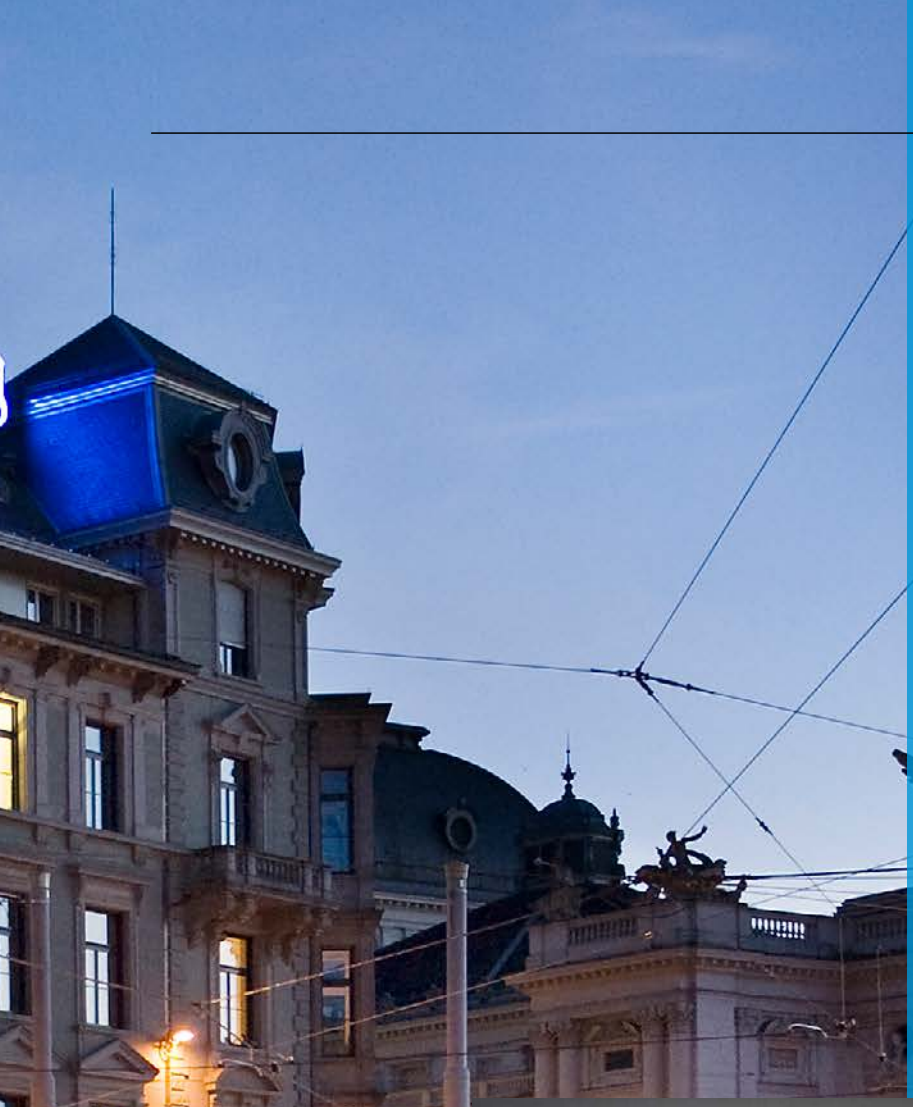
It also raises the question of what is classified as censorship, and how to deal with censorship requests from companies.

The fact that algorithms can be discriminatory has now been recognized. Some companies are already embracing the idea of democracy in the design of their information platforms.

It is also a question of ethics.

Many people see ethics as an obstacle, but it rather provides principles that help us to build a peaceful and sustainable society – principles of success!

Artificial intelligence cannot replace quality journalism and local focus



Veit Dengler is CEO of NZZ-Mediengruppe. He is fascinated by how technology impacts the world and points out that there are both risks and opportunities to the media business, e.g. the need to prepare against malafide attacks; and, opportunities like the automation of research and fact checking. A words of advice from him: "Make sure that you're agile and adaptive.

Veit Dengler, CEO of NZZ-Mediengruppe

What effect is digitalization having on the media sector and on the NZZ?

Our business model is changing. The easier part is that customers are migrating to digital products and paying for them as they used to pay for physical newspapers. I am positive that we will succeed in this task, as we started relatively early and demonstrate a high quality standard. We also have a cost advantage, as our printing costs are variable; if we print fewer copies due to the digital output, we pay less. The more challenging issue is the decline in advertising revenue and the question of how to compensate for it. We aim to achieve this by working with our readership, with business media and through events.

Do you also see a movement into other business areas?

It depends how you define the journalism business; for example, I see it as including the event business. So it becomes a question of diversification. We avoid anything that does not fit with our core business – all our activities are based on a journalistic business model.

Digitalization also creates new cyber-risks. What are the key scenarios in your opinion?

The rise of fake news means it has become even more important to be able to trace content and ascertain whether it comes from a trustworthy source or whether it has been intentionally manipulated. I can imagine a technology such as blockchain being used for this purpose. Similarly, the ability to semi-automate the fact-checking process is vital, as we need to examine large amounts of data. This process must be of high quality, as it's used to check content. However, digitalization not only brings risks – above all, it opens up new opportunities; for example, in research. A data search allows editors to gather information, so they do not have to write their articles completely from scratch – research becomes automated.

What consequences will this automated research have?

This concept will develop very quickly, but it will not replace journalists who are experts in their fields. Those writing agency reports for free newspapers, on the other hand, will have difficulty keeping their jobs.

"Fake news clearly represents a major opportunity for us. Organizations or media that can differentiate between true and false and offer readers orientation will become increasingly important in the future."

One of our strengths is our local focus. It's difficult to replace that via artificial intelligence. For us, automated research is primarily a means of increasing productivity – it helps us create more content for more channels using fewer resources. But employing fewer and fewer journalists to create more and more content, as some media companies are doing, will not work in the long term – it just leads to a downward spiral, where inevitably

the quality suffers and both readers and advertisers jump ship.

What cyber threats are you concerned about in terms of your company?

We need to protect our editorial system just as the banks do. We also need to protect our customer data.

Now, it seems as though all our online behavior is recorded.

I believe that this will produce a new industry branch – privacy tools that we can use to delete our digital trails.

Are there also dangers involved in the production process?

What concerns me is hacker communities. If they all attack together, there's nothing we can do. By definition, the internet is open – how do you protect something like that?

As a paying online customer, I expect everything to be up to date. How do you handle these cyber risks?

Unfortunately, there's little awareness of the risks of cyberspace. We need to weigh up the pros and cons; companies have to ask themselves how much they are prepared to invest in the unlikely event of an attack. This investment is expensive, but so is the damage caused by an attack. We need to see these threats – in particular from foreign states and terrorist organizations – as a management issue. And we need to talk about them more in public. We all grew up in an atmosphere of security and prosperity, which means we are unaware of the dangers and vulnerabilities. Yet when it comes to modern wars, the decisive factor is often how many billions are invested in cyber defense rather than how much is invested in fighter planes.

The Fourth Industrial Revolution is being driven by innovations such as the Internet of Things and Artificial Intelligence. How does your company position itself in relation to these developments?

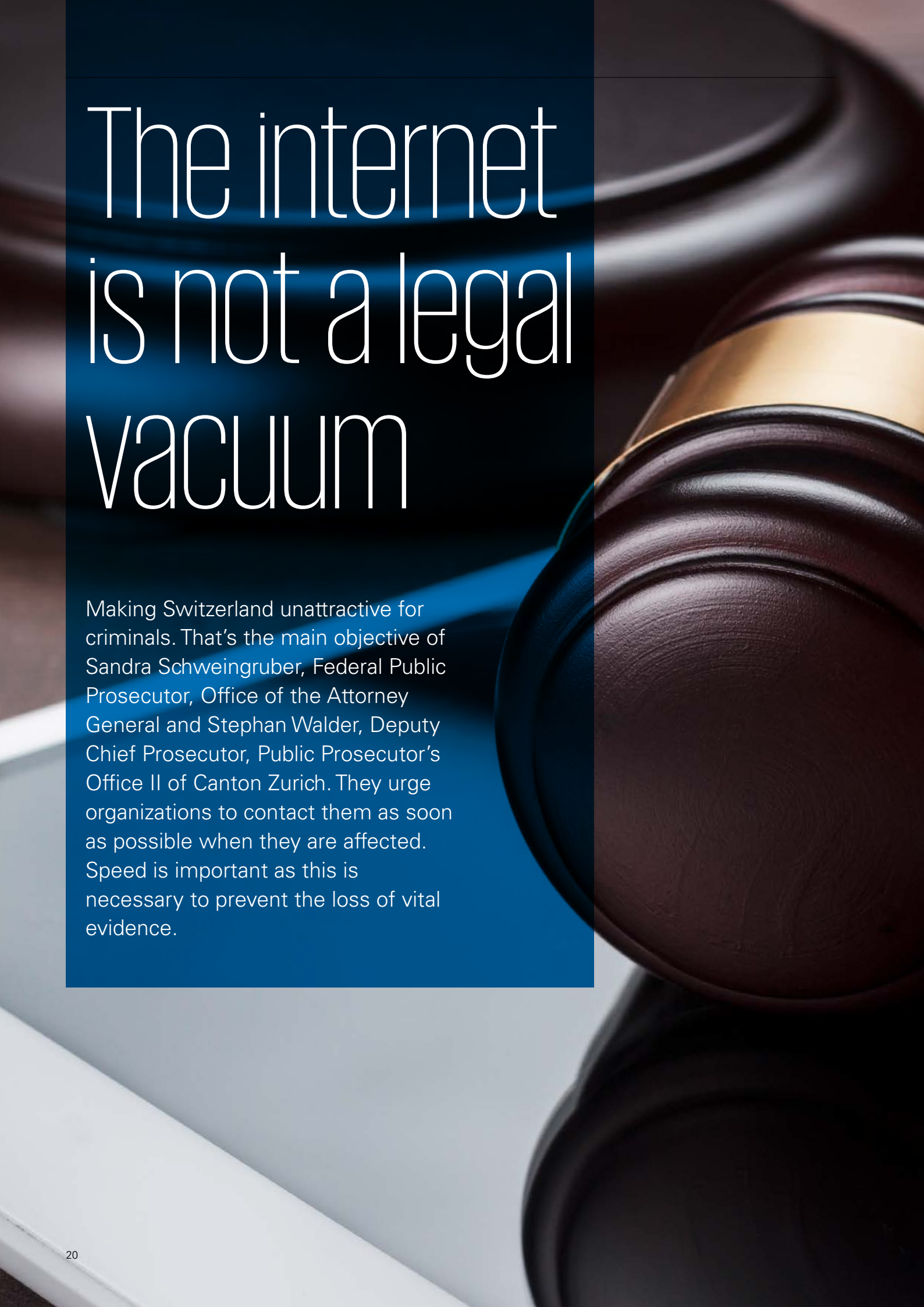
The situation is developing very rapidly. People are already organizing their lives using Amazon's Alexa (digital voice control), or getting it to read the newspaper to them. The two major trends – voice control with artificial intelligence and audio output – will significantly change our business once again. We're moving towards a model where, as a member of NZZ, you have access to all digital channels with individual subscriptions to the various formats and types of content. The Internet of Things will be relevant to us, as Alexa might be installed in my fridge or my car, allowing me to continue reading the news there. I find that really exciting.

Are there other opportunities in sight?

Fake news clearly represents a major opportunity for us. I think organizations or media that can differentiate between true and false and offer readers orientation will become increasingly important in the future. Many readers come to us because they are no longer able to cope with the rising flood of information. And digitalization has many other benefits. For example, we are able to process larger quantities of information more easily, communicate more quickly, even over long distances, make rapid decisions and adapt quickly to changing circumstances. Do you know Stanley A. McChrystal's book *Team of Teams*? It's about developing a system that can react to warnings of an armed attack as quickly as possible. But it is not only military organizations that have to develop this type of adaptive and agile system – companies must too.

The internet is not a legal vacuum

Making Switzerland unattractive for criminals. That's the main objective of Sandra Schweingruber, Federal Public Prosecutor, Office of the Attorney General and Stephan Walder, Deputy Chief Prosecutor, Public Prosecutor's Office II of Canton Zurich. They urge organizations to contact them as soon as possible when they are affected. Speed is important as this is necessary to prevent the loss of vital evidence.



Sandra Schweingruber
Federal Public Prosecutor,
Office of the Attorney General

Stephan Walder,
Deputy Chief Prosecutor,
Public Prosecutor's Office II
of Canton Zurich, Cybercrime
Competence Center

Are companies able to determine when and if the state prosecutor should be called in?

Walder: Those affected are often unsure about the aim and possibilities of prosecution. Our goal in the cybercrime division is to identify and localize perpetrators for the purposes of a criminal investigation. Speed is a central factor. In each case, our work begins with the securing and evaluation of all tracks with the aim of finding the perpetrators, and ends with the conclusion of preliminary proceedings, whether with a penalty order, a charge or a dismissal. Our objective is to make Switzerland unattractive to criminals from both general and specialist preventative viewpoints.

When should a company call in the public prosecutor's office?

Schweingruber: As soon as possible. The party concerned has an interest in the restoration of conditions as quickly as possible. This often leads to inadvertent destruction of evidence. It is important that companies consider early on whether or not to call in the public prosecution authorities. Once the decision is made, you can then jointly discuss what has to be secured as evidence for the investigation.
Walder: We also offer affected parties informal contact beyond the proceedings. This allows us to explain our fields of action and create a foundation of trust. In the event of an incident, we can offer emergency assistance. We meet the injured parties on site, with an investigator and technician on hand. Here we offer our expertise, since these incidents may be the first or only case for the party concerned, but for us it's part of our daily business.

Who should companies contact?

Schweingruber: Us; in other words, Mr. Walder or myself. We can then consider how best to approach the case and whether it falls under the jurisdiction of the cantonal or federal authorities.

What happens then?

Walder: We work on two levels. first, the technicians must be able to talk to their counterparts in the company.

Once the criminal investigation is launched, we need unhindered exchange of data. We have to create the foundation for this at a legal level, and the state prosecutor works closely with the legal department of the company. The goal is to find the perpetrators. We communicate each step with the company concerned, not least because we have to search for data on site.

Are companies right to be concerned that their operations will be interrupted by the investigation?

Walder: We operate on the living patient, as it were. An autopsy, by which I mean shutting down operations and carrying out a full evaluation, would probably offer greater precision. But in practice it's all but impossible without endangering the company's operations. The solution lies in finding a middle way. We secure the evidence while trying to keep interruption to the company's daily running to a minimum. This is a question of proportionality and a balance of the interests in question. No-one should fear that we will shut down the company for our investigations, or take away all its servers.

Schweingruber: For a successful investigation into cybercrime, we rely on the active cooperation of the company. Only together are we able to identify professional perpetrators and enforce penalties.

From the company's perspective, is there room for improvement in the procedures for current investigations?

Schweingruber: It used to be that the parties concerned were not involved, or only very marginally, in the investigation. We now try to involve the company, which acts as a private plaintiff, in the proceedings to a greater extent and to keep it informed. This creates transparency. From my point of view, cooperation with the private sector has improved. Now everyone is aware that cybercrime is a problem that affects every company.

What particular challenges does Switzerland face in the pursuit of cyber criminality?

Schweingruber: A big problem is the international dimension. Swiss authorities are often responsible for a criminal investigation simply because the company concerned has its headquarters in Switzerland. But the perpetrators and the evidence are in other countries. The principle of territoriality means that as prosecutors we cannot carry out investigations in a foreign state. So we rely on the cooperation of those authorities, which leads to a fairly cumbersome procedure. The willingness to participate in a Swiss prosecution varies from country to country.
Walder: The important point is that we do not have a view into the company concerned. Usually all we learn about an incident is what is reported. The exchange of information is therefore key. Maintenance of official secrecy guarantees absolute discretion at all times. We treat data entrusted to us with care.

What can you tell us about the clear-up rate? How would you describe cases that are particularly promising?

Schweingruber: For international cases, much depends on how well countries work together. Each country has its own interests, and they do not always overlap. As a small country, Switzerland is interested, wherever possible, in being part of international proceedings in which each country can make a contribution.

Walder: Our clear-up rate depends in all cases on the initial situation. The particularly demanding cases involve perpetrators from countries with poor legal assistance, and which are very well organized and can apply outstanding technical knowledge to carry out numerous offenses involving relatively small sums. Things are easier with "motive offenses", where it is not just monetary interests that play a part, but rather the perpetrator has a certain proximity to the injured party, such as a former colleague or competitor, and hurt feelings or grievances are involved.

In recent years, there have been numerous ransomware cases. Are these cases unsolvable?

Walder: This phenomenon definitely falls under the category of international cases, practiced by very well-organized perpetrators. Clearance is certainly not impossible, but it involves major challenges in the area of legal assistance.

Does it make sense to report these cases?

Walder: It does make sense. They are reported statistically and they remain registered. We collect these cases and analyze them for correlations in order to identify patterns. We also determine whether other countries are affected. But if it's just about reporting, I would recommend the federal government's Reporting and Analysis Centre for Information Assurance (MELANI), as this office has a centralized view of the situation and also offers ad hoc advice.
Schweingruber: For assessment of the situation in cybercrime, for me this would involve closer cooperation between MELANI and the law enforcement authorities in the future. We have to remember that cybercrime is a highly dynamic field of crime. It is a major challenge for a federally structured administration to remain up to date in such a fast-moving area.

> "'Nothing has ever happened to us, so nothing ever will happen to us.' This is a dangerous attitude."

Do you see trends in attacks relative to company size?

Walder: Many charges are brought by small and medium-sized companies and a decreasing number by larger corporations. SMEs generally lack the same financial resources to protect themselves. Sometimes their risk management is really quite reckless: "nothing has ever happened to us, so nothing ever will happen to us". This is a dangerous attitude. So when it comes to an incident, there is often no data saved that we can retrieve and evaluate.

What about industrial espionage?

Schweingruber: Industrial espionage is often a very large problem for companies, since usually important and sensitive documents go missing. In these cases, companies tend to be reluctant to report them out of concern that these documents will be made public.
Walder: It is not always apparent at the beginning of an investigation whether espionage is involved. Mostly it's just about simple "data theft". If we are able to arrest perpetrators red-handed or before they pass on stolen data, it's often not clear what they were intending to do with the data.

Does data theft occur between competitors?

Schweingruber: In my experience, there are fewer charges in this area. This could also be due to the fact that companies do not wish to disclose which data has been stolen, as it often concerns sensitive information.
Walder: We have identified a number of data thieves and data vendors. But the destination for the data is difficult to establish.

Is it always worth bringing you in?

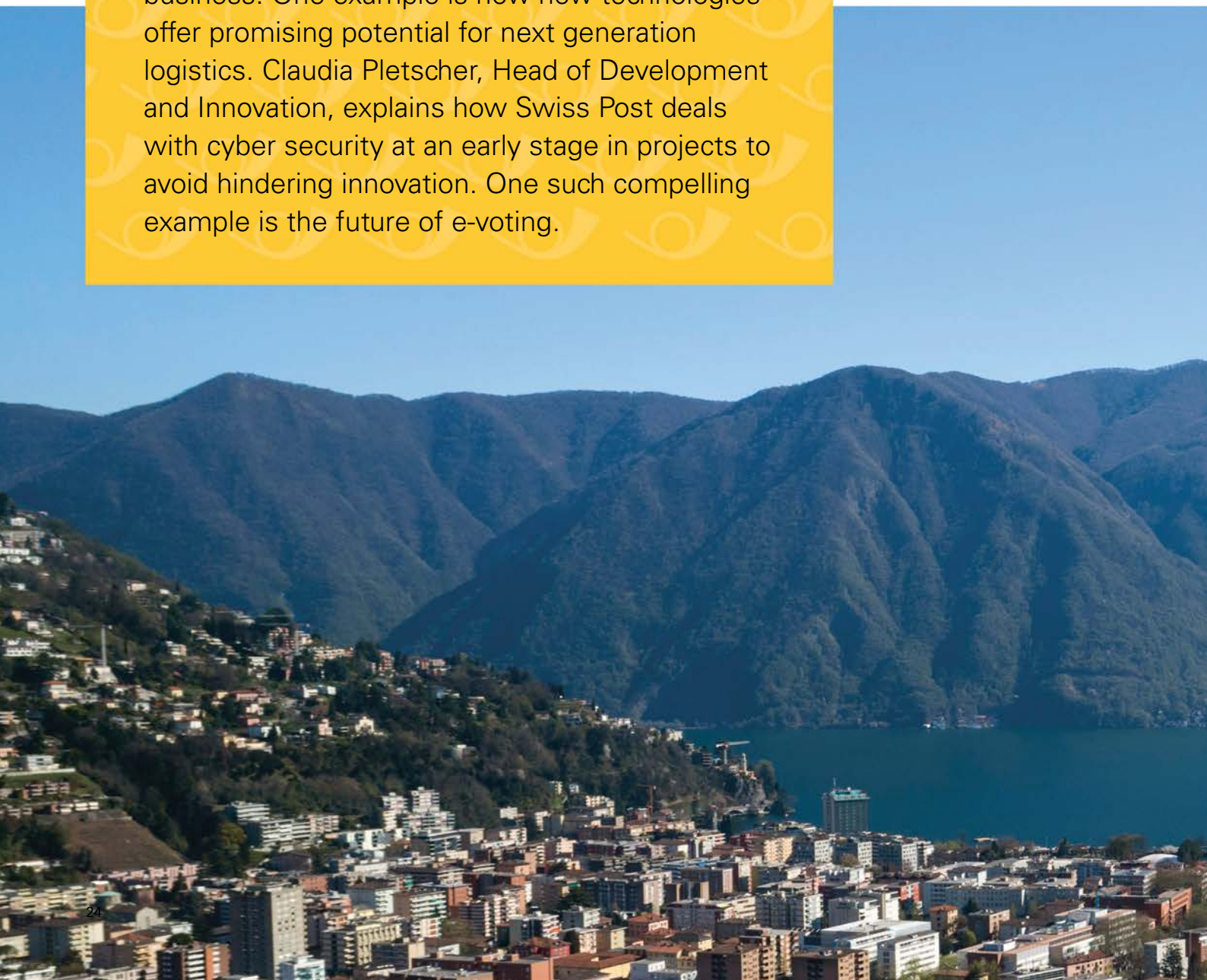
Walder: Generally, yes. But there have also been situations in which private interests such as reputational risk have outweighed the interests of a prosecution. But I believe companies need to say: the internet is not a legal vacuum; we will cooperate with law enforcement authorities. This cooperation is the most important thing for a successful investigation of a case.

Do you see a deterrent factor for perpetrators in Switzerland?

Walder: After a successful case, I read in a darknet forum that in Switzerland, 120 police officers were pursuing fraudsters on the darknet. That figure is not quite right, but it shows that word gets around about our actions and a post on the darknet is read just as often as a newspaper report. This deterrent factor is not to be dismissed.

Fostering trust is key

Digitalization has been the name of the game for Swiss Post in recent years in many parts of the business. One example is how new technologies offer promising potential for next generation logistics. Claudia Pletscher, Head of Development and Innovation, explains how Swiss Post deals with cyber security at an early stage in projects to avoid hindering innovation. One such compelling example is the future of e-voting.



What does digitalization mean for Swiss Post's current and future business?

Swiss Post will leverage its core strengths from the physical world in the digital sphere too. This means that we won't just fulfill our traditional role as the transmitter of confidential information in a physical sense, but in an electronic one too, and we will offer the people of Switzerland the corresponding digital infrastructure. Swiss Post is thus working on various digital solutions and is using cutting-edge technologies to develop new business areas; with eHealth and e-voting solutions, for example, or with the IncaMail encryption service. We are also launching a standard digital ID in partnership with the SBB and so, as a semi-public company, are helping promote simple and secure digital business in the economy and public sector. Swiss Post will also change with regards to logistics and mobility. Digitalization will allow us to supplement existing services with new ones. In Lugano, for example, we are trialling the use of drones to transport lab samples between two hospital sites. In Sion, we are testing self-driving shuttles, and in the Bern region, we have carried out tests using delivery robots for deliveries in the local area. One of Swiss Post's greatest assets is its nationwide presence: if we use the IoT to connect our physical infrastructure such as bus stops, post offices, mailboxes, buildings, ATMs and parcel terminals to the internet, we can optimize our operational processes and offer our customers new and more flexible services – such as individualized parcel delivery methods, for example.

Claudia Pletscher, Head of Development and Innovation at Swiss Post

"Digitalization will allow us to supplement existing services with new ones. In Lugano, for example, we are trialing the use of drones to transport lab samples between two hospital sites."

How do you think the cyber threat resulting from the digital transformation will change Swiss Post?

One direct effect of the digital transformation is that Swiss Post will be more vulnerable to cyber threats. The issue is thus becoming increasingly important for us. Swiss Post has already been active in digital business for a long time with services such as IncaMail. Relevant processes have been established and are being constantly adapted to new or updated conditions as part of an ongoing improvement process. For this, we are using an information security management system. We are also ISO 27001- and ISAE 3402-compliant, for example, so our processes are assessed periodically by the respective certification bodies.

What are the key elements of your security strategy to protect your digital products and services?

The key elements are forward-looking measures (Predict: e.g. security by design, certifications, security processes, etc.) combined with preventative measures (Prevent: e.g. ICT architecture, end-to-end encryption, four-eye principle, etc.). We have also implemented surveillance-related measures (Detect; e.g. logging, monitoring, etc.), which make it possible to identify deviations and irregularities. Specialized teams are trained to deal with any incidents as quickly and expertly as possible (Response: CERT team, communication, DSB processes), and to learn from them. In general, there are two critical aspects of our security strategy: firstly, constant compliance with our information security baseline – i.e. the implementation of best practices – and secondly, the specific focus on business risks, where additional security measures are required.

How do you ensure that cyber-security measures don't inhibit your ability to innovate?

That's a challenge, of course. We aim to develop services with architecture that already meets the relevant requirements (security by design), and to begin testing even during the development cycle. We also aim to treat innovation projects in a special way from an early stage and to integrate them gradually into higher requirements levels. This includes aspects such as: use of a protected development environment with secure APIs to our system landscape, performance of automated tests, agile development and gradual risk elevation, and transparent communication of risks to users.

The Internet of Things poses significant challenges to companies with regards to cyber security. How does Swiss Post address these challenges as an operator of autonomous PostBus and parcel drones?

In terms of ICT security, the Group's IT department is involved in our SmartShuttle project, as it is in all projects and we make it a priority to

evaluate all suppliers in an assessment. We also carry out penetration tests on solutions that contain user data or other sensitive information. There are additional technological hurdles that make it more difficult for a hacker to gain access to the vehicles. The vehicles from the manufacturer Navya cannot be remotely controlled directly over a web interface. The manual control takes place over a control panel, which is connected to a computer in the vehicle. Then, of course, there are other technical security measures that prevent, or at least impede, external access. But as we know, a cyber attack in the field of IT can never be 100% ruled out.

Can you use a specific postal service to demonstrate how the core elements of your cyber-security strategy have been implemented?

Our e-voting system is subject to the most stringent security requirements. Various inbuilt mechanisms and special security-related and cryptographic precautions guarantee security and data privacy. The data is end-to-end encrypted and no personal data is stored on Swiss Post servers. The votes can be individually verified, which means each voter can check whether their electronic vote has been saved in the same way it was sent. In the future, "universal verifiability" will also be possible. Cantons and the federal government can then carry out comprehensive checks when they open the ballot boxes to determine whether the electronic votes have been counted correctly and were not falsified. So we can't rule out attempts to attack the system but, thanks to mechanisms like these, we can guarantee complete transparency. This is extremely important in fostering trust in such solutions.

Between data and defense. How technology can help protect us.

Ann Johnson, Vice President of Worldwide Cyber Security at Microsoft, shares her insights into the future of machine learning, artificial intelligence and the reality of cyber threats.

Machine learning (ML) and artificial intelligence (AI) have become an integral part of our life. Which developments will impact us most over the next three to five years?

Developments in this area include new medical research-based data that can deliver improvements in healthcare. Patients will ultimately be able to benefit from medical research that uses ML and AI to predict medical conditions, enhance patient care, and even develop new and better drugs. A further development will be our growing reliance on machines to carry out tasks that are typically requested of humans. Enhanced voice input-based machine assistance is becoming particularly popular. To date, people use voice-assistant software such as Microsoft's Cortana to carry out simple commands such as finding facts, files, places, other information, setting timers and reminders, etc. Over time, these technologies will become more sophisticated, applying ML and AI to understand the context behind the original command and even to automatically carry out other, related tasks. And last but not least, enhanced and timely detection of cyber security attacks. Cyber threat intelligence derived from the application of ML and analytics will continue to augment cyber security analysts' efforts to protect endpoints, better detect attacks and accelerate responses. ML and data analytics are already used extensively to detect nation-state attacks. For instance, the Microsoft Intelligent Security Graph, based on Microsoft Azure Machine Learning technology, collects trillions of data points from billions of computing endpoints to provide real-time insights that are of great use in this field. The Office 365 Advanced Threat Protection product alone processes 6 billion emails each day.

Do you see current/future risks to the privacy of people (data subjects) as a consequence of using ML and AI? What do you consider to be effective means to mitigate such risks?

It is possible that such risks exist. ML algorithms that don't have security and privacy built-in by design may accidentally or inadvertently expose personal data. For example, we wouldn't want voice-assistant software on our device to share Personally Identifiable Info or PII for anyone to see or hear. One way to mitigate risks would be to ensure all private data, including PII data, is encrypted. And that ML and AI algorithms transact on encrypted data. Fortunately, advancements in the field of mathematics are already enabling this. The medical industry, in particular, is adopting this approach to safeguard patient and hospital data and securely analyze data at scale.

"ML and AI have the potential to drive improvements and help with a variety of use cases for consumers, enterprises and government."

Ann Johnson, Vice President of Worldwide Cyber Security at Microsoft

Do you see current or future cyber risks for individuals, organizations and states as a consequence of using ML and AI? If so, how should these risks be mitigated?

Organizations are responsible for maintaining privacy for a wide variety of data related to the business itself, its employees, customers and partners. If the application of ML or AI compromised these data, the company could suffer reputational, financial or other damage. Meanwhile, nation states similarly need to maintain the integrity and privacy of all types of data covering a wide variety of topics such as industrial, financial and people. It's imperative that vendors of ML and AI technologies fully disclose to state entities how they ensure the privacy of their data. The same goes for individual's privacy, one way to mitigate risk would be to ensure all private data, including PII data, is encrypted and that ML and AI algorithms can process these data.

Which do you consider the most promising use cases for ML and AI for cyber defense? Are you working on such use cases and, if so, what are the potential benefits?

Among the most promising use cases in this regard are the application of the NIST Cyber Security Framework to protect, detect and respond to cyber threats. Protection focuses on applying security controls to minimize the impact of a potential cyber security event. ML-based solutions help prevent compromised identity, secure applications and data, expand device controls (including data encryption), and safeguard infrastructure. Benefits can also be had from using security solutions that use ML and AI to help detect advanced cyber attacks. The solutions seek out signs of malicious behavior, anomalies, and other noteworthy cyber security events. Meanwhile, response focuses on being able to lessen the impact of a potential cyber security event. Organizations should apply a multi-pronged approach of training people, developing and adhering to security best practice processes and implementing cyber security technology. Microsoft offers clients an unparalleled body of threat intelligence that is created from analysis across our customer base, including emails, URLs and endpoints. Our security solutions apply a combination of artificial and human intelligence to provide visibility into suspicious and malicious activity – enabling customers to respond and mitigate cyber threats swiftly.

Do you have any final comments on this subject that may be of interest to our readers?

ML and AI have the potential to drive improvements and help with a variety of use cases for consumers, enterprises and government. However, these technologies will only be adopted and used successfully at scale if they transact on trusted data and do not in any way compromise the security and privacy of personal data. Then, we can see huge benefits across a number of vital fields.

How cyber security advances to the next level

Going beyond the buzzwords, there's potential for Artificial Intelligence and Machine Learning to improve security. Raffael Marty, Vice President Security Analytics at Sophos says that security will only work if we succeed in bringing in contextual information on the suspected attacks. Raffael also argues that good technical solutions exist to deal with the dilemma between security and privacy.

Artificial Intelligence and data analytics play a key role in our everyday lives. Which developments are particularly important?

It starts with data. Huge volumes of data have been collected over the past few years. Then Deep Learning came about, which has brought with it new opportunities to analyze these large data sets with novel approaches for image recognition or sound analysis, for example. These developments have really boosted the whole industry. However, in my view, there's a lot of hype and misunderstanding around Machine Learning (ML) and Artificial Intelligence (AI). Everyone is talking about ML but most people actually mean statistics, and when they say AI they actually mean ML.

How is the area of security developing?

We've made significant progress in malware classification. For example, researchers use ML to analyze millions of file samples and to very accurately determine the characteristics of malware. But these classifications still only work well with very specific problems and data sets. Applying the same approach to, say network traffic, is very hard. It starts with the collection of training data. Being able to get a clean data set that clearly identifies good from bad network traffic is almost impossible. And it gets progressively harder from there. Machines are great at identifying statistical outliers. But without domain knowledge, it's hard to identify actual security issues. Bridging that gap can't be done by any

single algorithm, it's a question of gathering and codifying expert knowledge.

Why is it so difficult for the system to identify whether the anomaly has to be classified as good or bad?

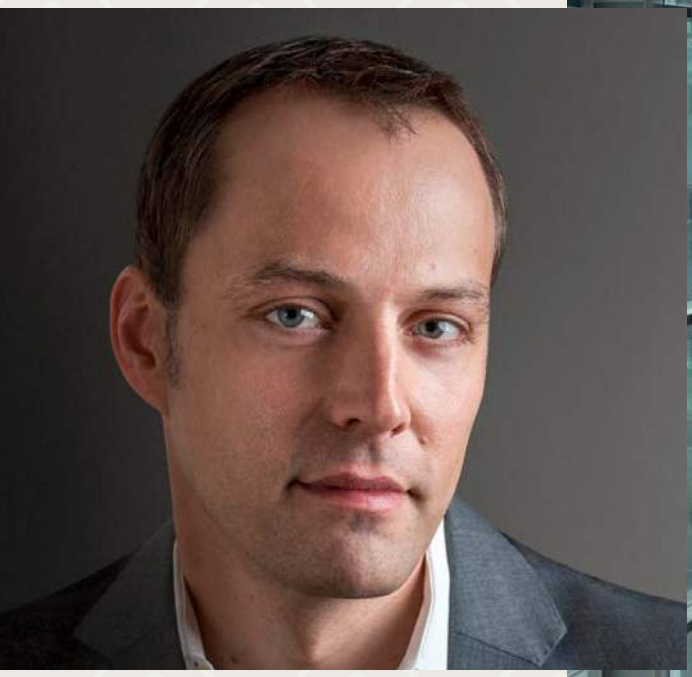
Because the system has no knowledge of the broader context; who are the users controlling these machines, what are the roles of these machines, etc. So a change could still be explained as normal; although the algorithm might still be right – it was a statistical anomaly.

So a problem occurs if there's insufficient contextual information?

Exactly. We are too focused on the data and algorithms that we already have. But companies are in general lacking contextual information. What kind of machine is that anyway? Which applications should it allow to be installed and run? That doesn't sound too complicated, but the difficulty for a company lies in collecting that data and understanding what the 'normal' should be. Everyone has been ignoring that aspect.

This lack of contextual information prevents the engineers from finding more use cases for AI and thus improving cyber security. So what use cases would you find on an advanced level?

Use cases in the field of malware classification are certainly advanced. Basically when you look at a file or binary, you want to determine whether it's a malware file or a normal file. Current algorithms are very good at making these classifications. You can see evidence of that in products on the market. Sophos, for example, is using



Raffael Marty, Vice President Security Analytics at Sophos

deep learning to classify malware on the endpoints with unprecedented precision. Applications of deep learning and other classification algorithms beyond malware classification are tricky, as there are no good training data sets and the algorithms can't learn without training data. But fundamentally, that's also the wrong focus. I see too many companies more or less randomly picking some machine learning algorithms to then apply them to a security problem. They need to start with the problem. From there define what data they need and then find the algorithm that will solve the problem. Most likely it won't even be machine learning, but either simple statistics or rule-based systems.

Where are you expecting major advances in the coming years?

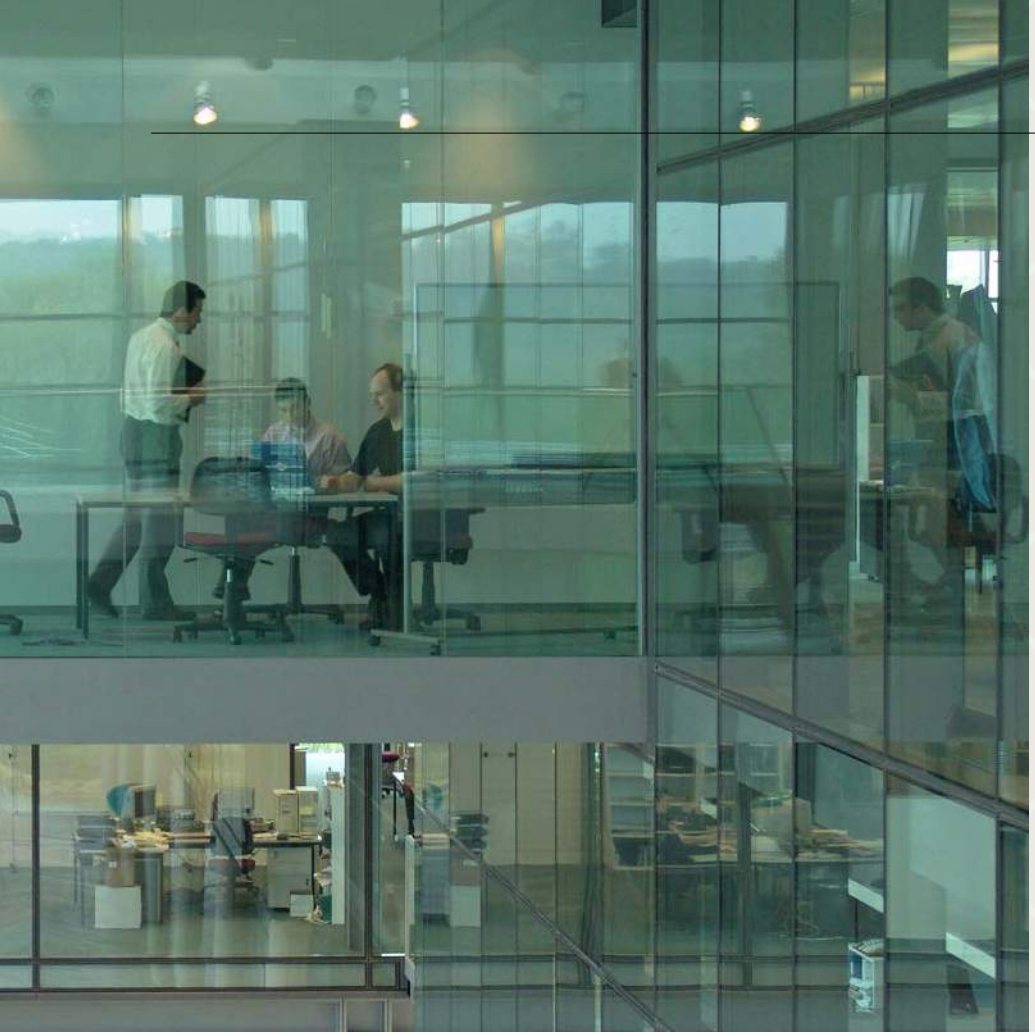
In my previous job, I ran a consulting business where we worked with multi-national companies. One of the problems we constantly found was alert triage. This is the process where a level 1 analyst in the security operations center goes through a stream of alerts to manually identify which alerts are true problems and which ones are not. A couple of startups are beginning to apply intelligence to automate this so that a system can make these decisions. This really interests me – the ROI is incredibly compelling. It will help eliminate level 1 analysis in the next three or four years – freeing up people resources to do more sophisticated work and leverage machines for tasks that they are really good at.

What will we see then?

Today security is about a 0–1 decision. Either it's bad and we block it, or it seems okay and we allow it to proceed. We will see a refinement of this into more of a fuzzy approach. For example, if there's uncertainty around whether a system has already been hacked or not. A risk profile can be developed by observing the unusual behavior of a machine or a user. The risk profile is then used to dynamic policy decisions. For example, a firewall could ask: What is this person's risk level? If my level were slightly elevated, the firewall would no longer allow me to access certain systems, such as file servers hosting critical business files. Or the firewall would decide to perform a deep packet inspection on everything it sees from that user. Moving away from good or bad to a more risk-centric view is one of the areas my team is working on.

The large pool of collected data improves security, but could also be attractive for hackers. This brings us to the issue of privacy.

A thorny issue. On the one hand, we want more insight, but that's completely at odds with the idea of privacy. Just how much data should we and do we need to collect? Facebook is a great example: Sure, I can control my own information, but if, for example, other people upload a photo of me that I didn't necessarily want to be posted, these controls might not be effective. It's similar with the privacy debate around security data. In the US, I have absolutely no privacy on my work computer – my employer can do



whatever they like with my data. As an employee, I'm told about this and I can behave accordingly. In Europe, the laws are different. When designing and building systems, we need to keep those parameters in mind.

On the face of it, this looks like a big dilemma: the more data you draw on to give customers security, the more attractive your work becomes as a target for hackers.

Yes and no. If someone stumbles across this data, they will need to be really lucky first to find anything useful and then to analyze it correctly. But if they have the time and the means, they're probably going to find something useful. It's our job to build systems with secure architectures. There are various approaches to this. One is to apply encryption. Anonymization is another interesting approach. For example, we can anonymize usernames or IP addresses in data streams with a one-way function and keep the keys in a secured store. There are technological solutions to a lot of these problems. Secure development practices and secure architectures become ever more important.

And how should that be collectively implemented?

We need to define guidelines on how people best process and store such data. But a law by itself is often useless. Security organizations and interest groups need to work on defining easy to apply guidelines and ideally development frameworks for companies to implement secure data processing systems. There's some good work out there, but it's still far from done. There's still a lot of work to do by companies that are collecting critical data before we'll have attained this type of security foundation across the board.

Is that an issue even for security firms?

Definitely. Just because you're a security company doesn't mean that all your employees have the appropriate security knowledge and skillset to build highly secure infrastructures. We need to keep exploring the question of how can we build secure systems and how we deploy secure infrastructures. It's important to focus on the simple things. A simple example: How do you define firewall policies? Fundamentally, the process hasn't changed much in the past 15 years. At Sophos we have been working on some interesting improvements like application identification and application layer policies, which make it significantly simpler and more effective to define firewall policies, rather than having to operate on layer three or four. In my opinion, crowd sourcing and crowd intelligence will be one of the hot topics to solve some of these challenges in the years ahead. We have a large data set that covers thousands of users. The insights we can extract from this data are quite interesting. And mind you, we can get to these insights without using complicated math or machine learning. Often simple approaches yield the best results.

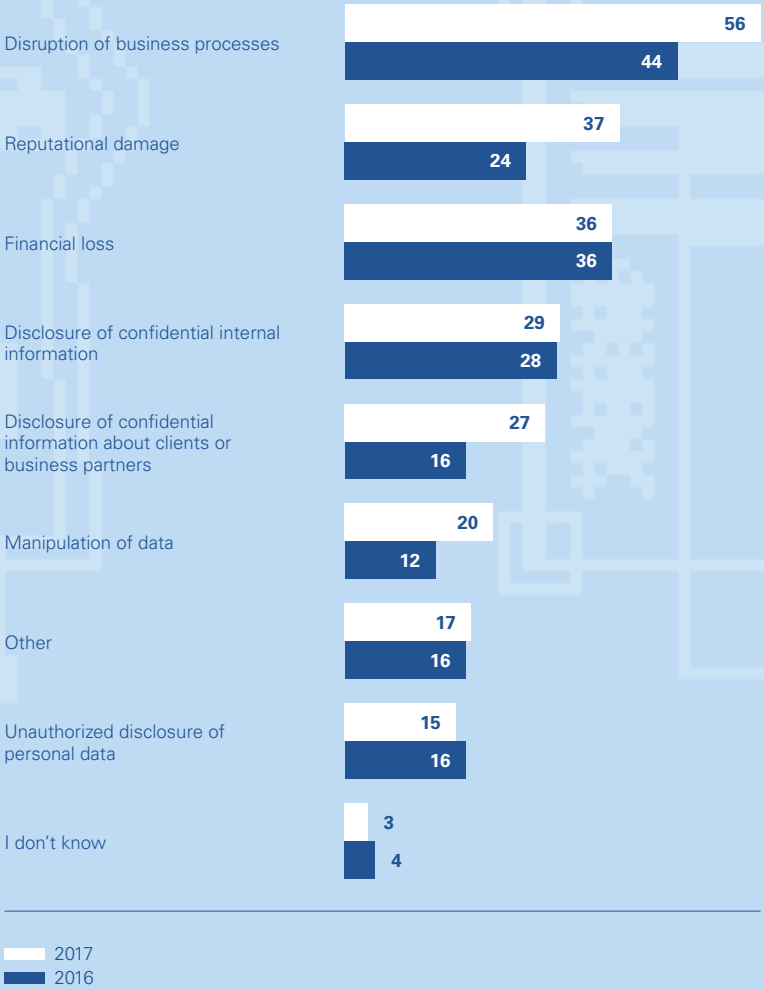
The state of cyber security in Switzerland

No doubt about it. Cyber security is a core theme in today's business reality for most Swiss companies, as it is in other parts of the world. The majority have had to deal with incidents. The attention for the topic is fueled by constant media attention. Elaborating on the impact of these threats is not very useful as this is mostly common knowledge to executives. Repeating the warnings about the risks wouldn't bring us any further.

Risk-based approach is gaining ground

It's a fact that the that an organization's success is often is often highly dependent on digital assets.
An impressive 88% of our respondents had to deal with attacks (2016: 54%). It's therefore of utmost importance to properly safeguard against threats. However, the best way to do so is to look at this topic through a Risk Management lens. A risk-based approach is better than acting out of fear and clears the path to a balanced approach focused on people, process and technology in order to detect, prevent and respond to cyber-threats. This may sound like a familiar message and in fact it is. We have been giving this advice to clients for many years. Does it gain a strong foothold among them? At first glance, the results of the survey are promising. 81% say that over the last twelve months they have gained deeper understanding of risks, 52% have gained a better understanding of the attackers' motivation, strategy and tools and 44% claim that prediction capabilities have improved. To conclude, 49% have achieved a better balanced approach between people and technology – realizing that it's not just about tools.

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

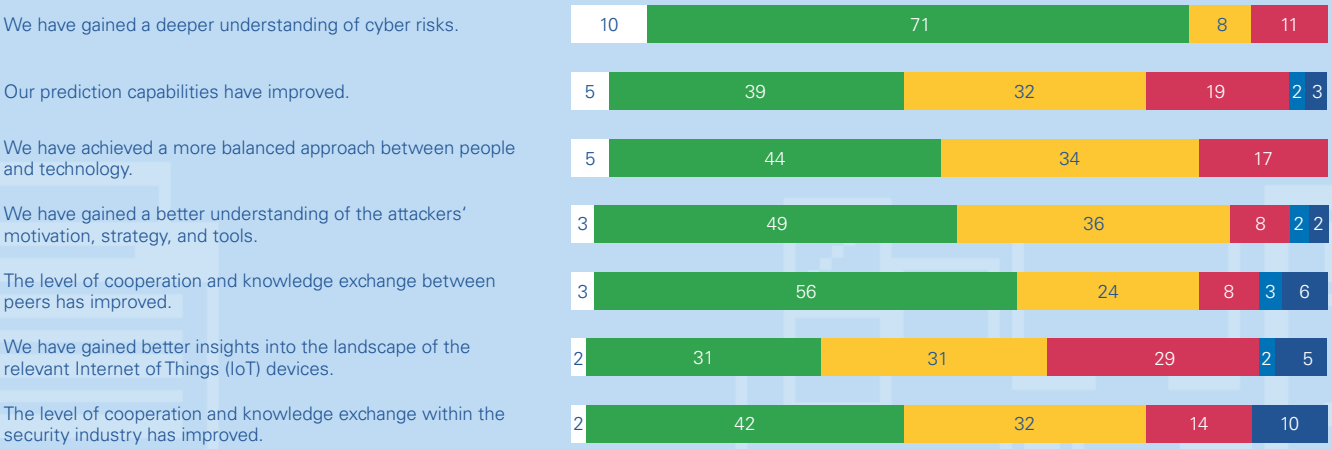


As promising as these figures may appear, one of the basic building blocks is still not very mature. Based on our experience in the market, many organizations don't have good insight into their risk exposure.

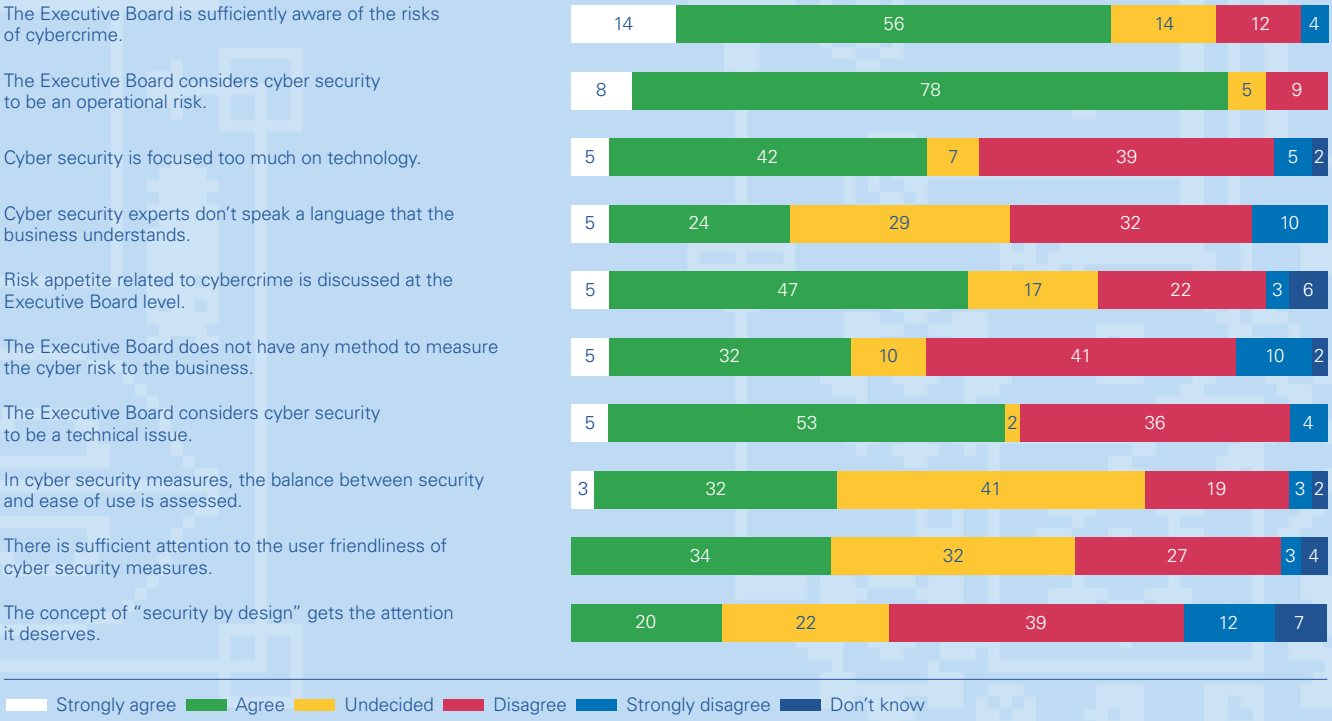
They lack proper understanding of how cyber security is important in the value chain and links to their business objectives – understanding what the crown jewels are and to what extend they are exposed to cyber threats. The survey also gives some indication of this, for instance where it touches upon the role of the board. Many respondents believe that boards don't fully grasp what's at stake. Only half of the respondents agree that risk appetite is discussed at board level. Which brings us to the intriguing question: how can the other half warrant a decent cyber security approach without discussing risk appetite?

88%
of respondents suffered a cyber attack in the past 12 months.

Can you confirm improvement in the past 12 months regarding the following statements? (in percent)



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



81%

confirmed that they have gained a deeper understanding of cyber risks in the past 12 months.

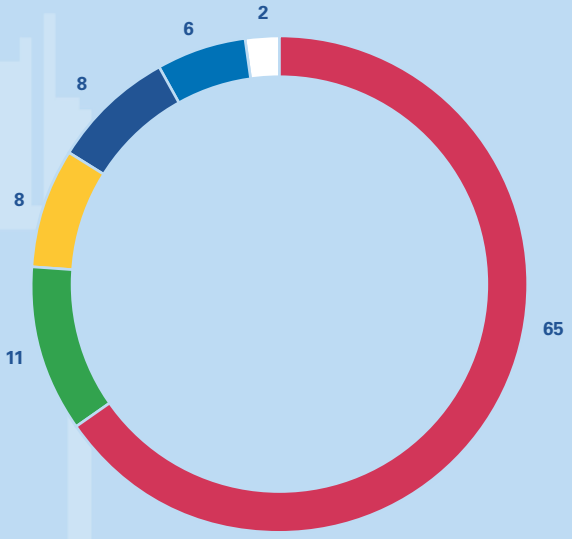
86%

agreed that the Executive Board considers cyber security to be an operational risk.

We must offer a seamless user experience

Cyber security is not a department. It's an attitude.
Many acknowledge that this is true: to be secure, one must make sure that the whole organization's state of mind is in line with security policies. However, in many cases we're not making it very easy for users to live up to this state of mind. Currently, the technology perspective is dominant in the design of tools and authentication methods. We need to get more focus on a seamless user experience. Figures from the survey show that this is a much needed improvement.

Does your organization systematically work on cyber security measures that are user-friendly? (in percent)



- No
- Yes, the involvement of a UX specialist contributes to user-friendly security design
- Yes, with A/B testing we measure what works best
- Yes, with customer journey analytics/mapping we optimize the design of security measures
- Yes, with user surveys we map what users think of the measures
- Other

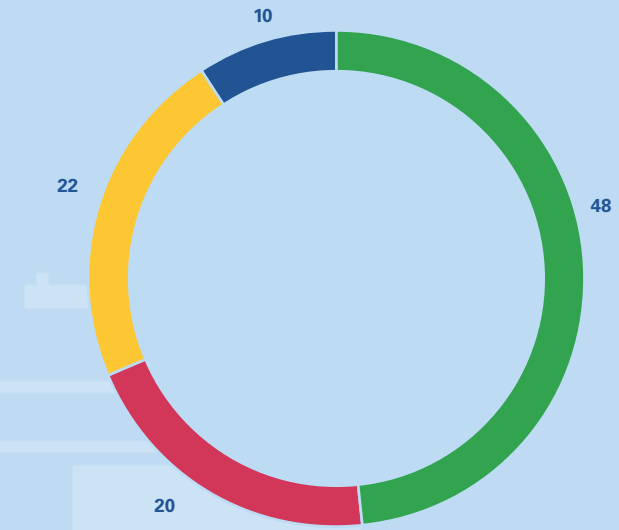
More than half of the respondents acknowledge that they don't even assess the user friendliness of cyber security measures when implementing new tools or concepts. Only 11% say that they involve a user experience specialist to contribute to creating a user-friendly design.

Instead of having a predominantly technological approach towards implementing security measures, we must start thinking about security and user-centered design as two halves of a unified whole. The stakes are high, as the human involvement is often the weakest link. Many breaches of systems can be traced back to human error. One could argue that they are careless. One could, however, also argue that we should develop better user interfaces for security.

Early involvement of both security specialists and designers of user interfaces in the development of products and systems is crucial to reach the next level. Many examples from consumer products show us that easy to use security measures are available.

Security in corporate environments, however, has a bad reputation in this respect for adding complexity to the product development process. It's not uncommon that the user friendliness of security measures are in fact treated more or less as an afterthought. If we can improve this, we'd have great potential to increase security figures.

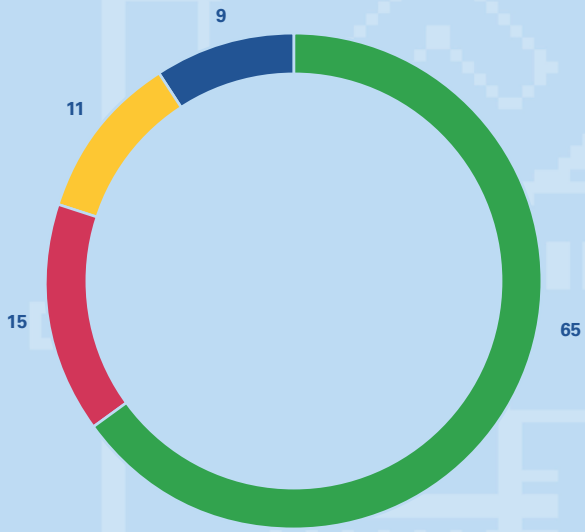
Are cyber security measures systematically embedded in your product/service design process? (in percent)



Yes, they are
No, we don't develop (new) products/services which require such measures
No, they aren't
I don't know

48%
embed cyber security measures systematically in their product/ service design processes.

Are data protection/privacy measures systematically embedded in your product/service design process? (in percent)



Yes, they are
No, we don't develop (new) products/services
No, they aren't
I don't know

65%
embed data protection/privacy measures systematically in their product/service design processes.

Internet of Things

Healthcare

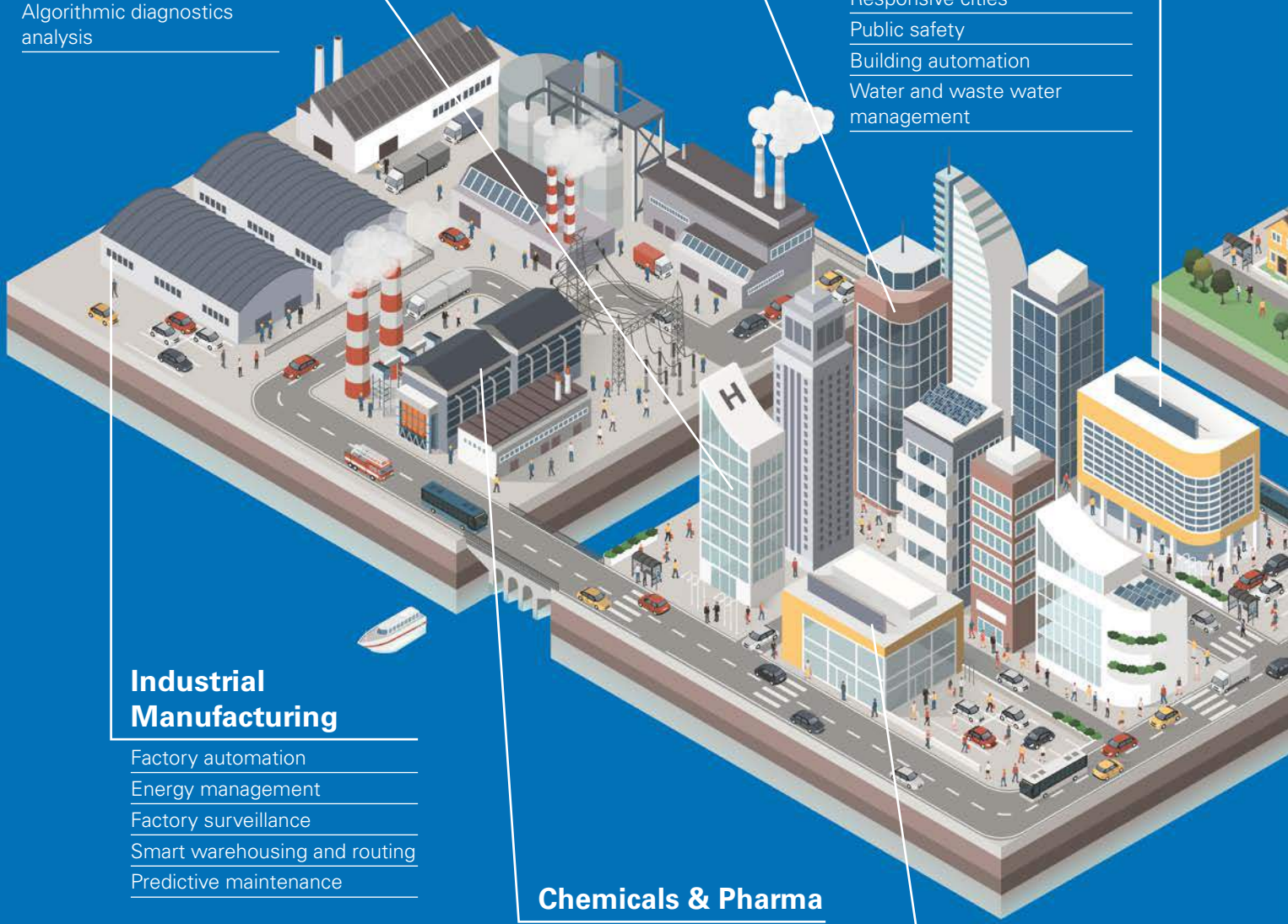
- Remote patient observation
- Smart medical devices
- Smart prescription management
- Algorithmic diagnostics analysis

Banking & Insurance

- Mobile payment and wallets
- Smart ATMs
- Predictive insurance modeling
- Driving data recorder

Smart City

- Video surveillance
- Predictive policing
- Smart management of city infrastructure
- Responsive cities
- Public safety
- Building automation
- Water and waste water management



Industrial Manufacturing

- Factory automation
- Energy management
- Factory surveillance
- Smart warehousing and routing
- Predictive maintenance

Chemicals & Pharma

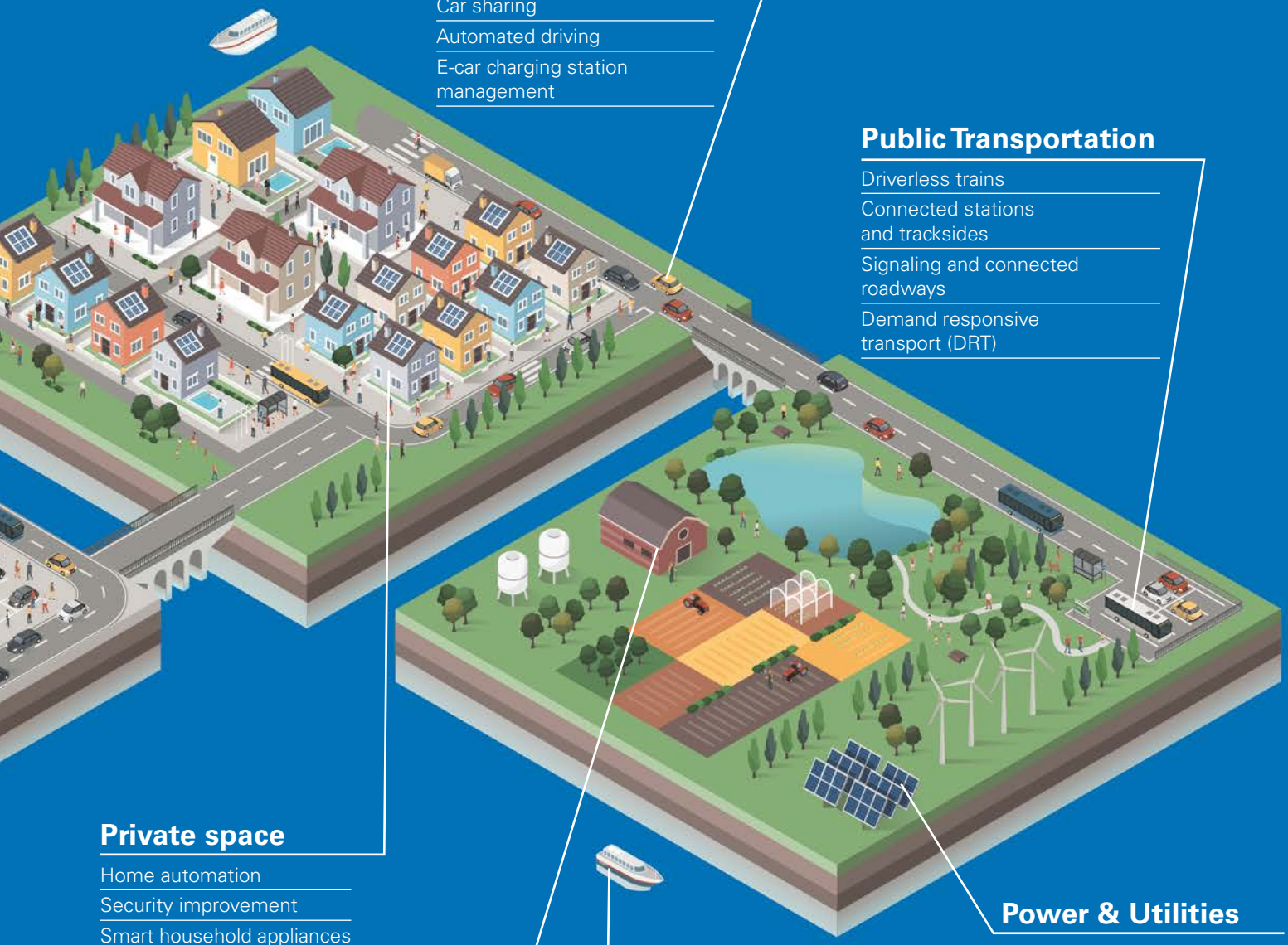
- Drug usage tracking
- Chronic disease management
- Smart pills

Consumer Goods & Retail

- Connected retail
- In-store localization
- Beacon technology
- Connected clothing

There will be 20.8 billion devices connected to the Internet generating over 20 zettabytes of data by 2020.

(Source: Gartner)



Individual Mobility

- GPS
- Car sharing
- Automated driving
- E-car charging station management

Public Transportation

- Driverless trains
- Connected stations and tracksides
- Signaling and connected roadways
- Demand responsive transport (DRT)

Private space

- Home automation
- Security improvement
- Smart household appliances

Agriculture

- Automated field testing
- Automated weeding

Transport & Leisure

- GPS and RFID
- Environment monitoring and management
- Responsive and adaptive supply chains
- Reservation, toll, and ticketing systems
- Guidance and control systems

Power & Utilities

- Supervisory control and data acquisition (SCADA)
- Advanced metering infrastructure (AMI)

Better insights needed to assess the impact of the Internet of Things

The Internet of Things is a burgeoning new market across sectors

Technology firms, car makers, medical firms, etc. all face new cyber threats. In terms of security, it's not only these producers of technology that face new challenges. In fact, nearly all organizations deploy a range of new devices and are faced with corresponding new security issues. This may have far reaching consequences, as the Internet of Things isn't just about the usual suspects (nice to have devices such as TV, handhelds, gadgets) but also about a range of devices that are used in vital processes for production, medical monitoring, traffic, communication and infrastructure.

Being successful in the domain of the Internet of Things is not just about slick applications, connected devices and advanced analytics. It also requires a robust approach to security, privacy and trust.

Trustworthiness is key. Our survey shows that as well: The respondents state that reduced trust from customers is by far the most important trust aspect of security breaches (58% says very impacted), distantly followed by trust from authorities (32%), business partners (28%) and investors (21%).

Lacking insight

It starts with having insight in how the Internet of Things affects business processes and how potential misuse or breaches may affect trust from customers or stakeholders. More than half of the respondents in our survey acknowledge that they do not have an overview of all Internet of Things devices deployed in their company: 35% didn't even try and another 17% tried but failed to get this overview. Given these figures, it may not be surprising that half of the respondents admit that cyber security strategy and the corresponding policies currently do not include the topic of Internet of Things or Operational Technology Assets.

The sheer volume and complexity of the Internet of Things make it hard to get a proper overview and to manage risks appropriately. Nonetheless, this shouldn't be an excuse to defer developing insights into the various categories and corresponding risks of the Internet of Things. Companies must make sense of the chaos. Only then can organizations maintain sufficient governance. They must make sense of the chaos of the Internet of Things.

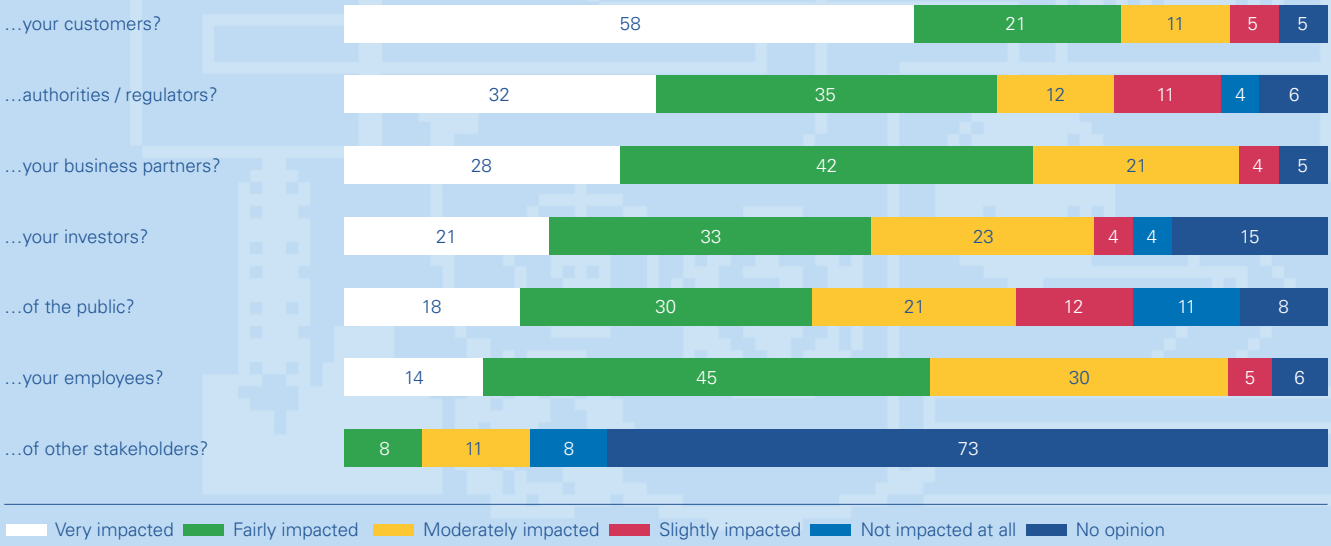
33%

have gained better insights into the landscape of the relevant IoT devices in the past 12 months.

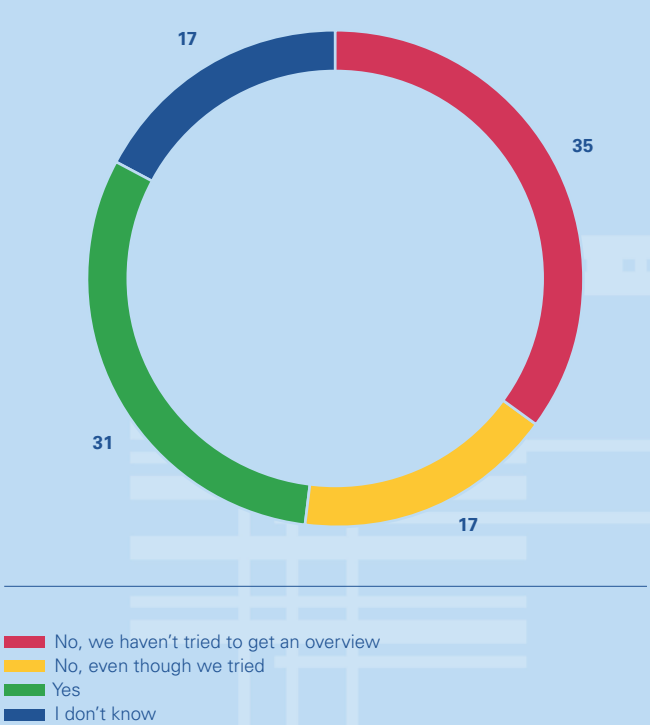
41%

include IoT or OT assets in their cyber security strategy and policy.

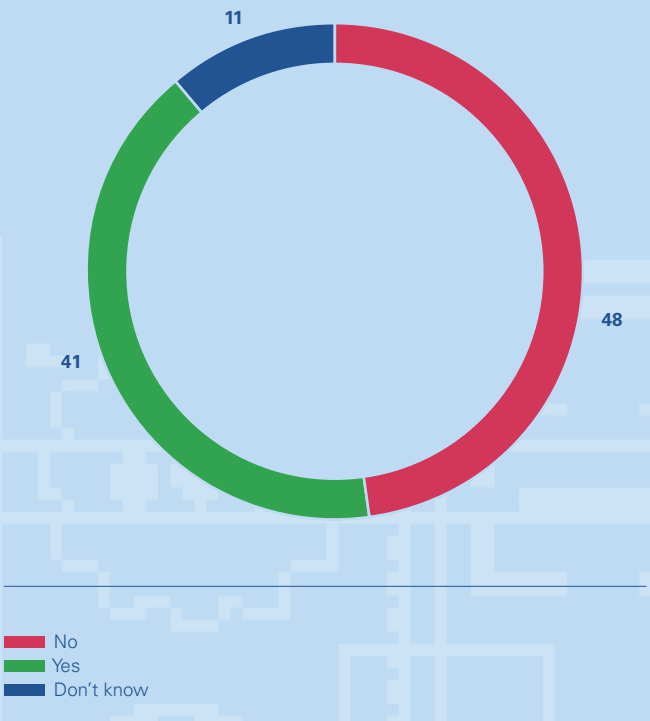
How high do you consider the impact of cyber security breaches on the trust of ... (in percent)



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



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



More focus on security by design

More and more it becomes clear that security is immature in the design of many devices that are part of the Internet of Things. In many cases, security is an afterthought popping up once a device is compromised. It's common practice that devices have default passwords and don't use encryption.

Some experts call for regulation to bring improvement. However, the industry shouldn't wait for this regulation process and raise the bar themselves in ensuring the quality and security of their products.

If the industry can embed security in a user-friendly manner, this will offer them a chance to gain and maintain customers' trust. Which is one of the key factors for success.

This improvement includes a rigid quality control process and ongoing maintenance. Updates for software on laptops and phones are very common to deal with continuously changing online threats; the same level of support should be the standard for other devices.
However, this is far from how the current situation is and our respondents seem to acknowledge this. When asked what their biggest concern regarding Internet of Things is, the most popular answer was: "exotic devices getting introduced to our network" and that "traditional controls are no longer effective (e.g. cannot be patched)." This was acknowledged by 59% of respondents.

This is particularly worrying as consumers and companies expect not only the highest level of convenience but also cheap devices. Manufacturers try to meet their expectations and are sometimes pulled into a race to the bottom of pricing. As a consequence, there's little room for investment in security within the device.

Nobody knows you're a fridge on the Internet

The infrastructure of the early Kahn and Cerf-Internet – that has remained virtually the same since its first creation – was never designed with security as a primary driver. In fact, our security woes lie in the framework and even the interface of our Internet, says MIT professor and AI researcher, Howard Shrobe. "Everything was designed to share in an uninhibited way, so keeping bad guys out has been a matter of ultra-complex alchemy on the part of programmers and designers. We left it to programmers to incorporate security into every line of code they wrote. One little mistake is all it takes for the bad guy to get in."

What we would need, according to Shrove, is nothing less than a complete redesign. Is this a realistic challenge? It's surely ambitious.

It's a fact that this becomes a more pressing issue with the exploding Internet of Things, which brings an extra dimension to the 'alchemy' of being safe. In the Internet's heyday, we used to worry about the real identity of humans using it. Many of us are familiar with the cartoon in the New Yorker – published in 1993 – with the famous quote: "On the Internet, nobody knows you're a dog". Today, this is still true, with the challenge entering a new phase as a consequence of trends such as cloud computing and the Internet of Things. More than 20 years after this cartoon, we must also assess if thermostats, fridges, cars, oil platforms and a variety of other devices are who they claim to be. If we have no idea about this, we have a huge problem in rolling out new business concepts.

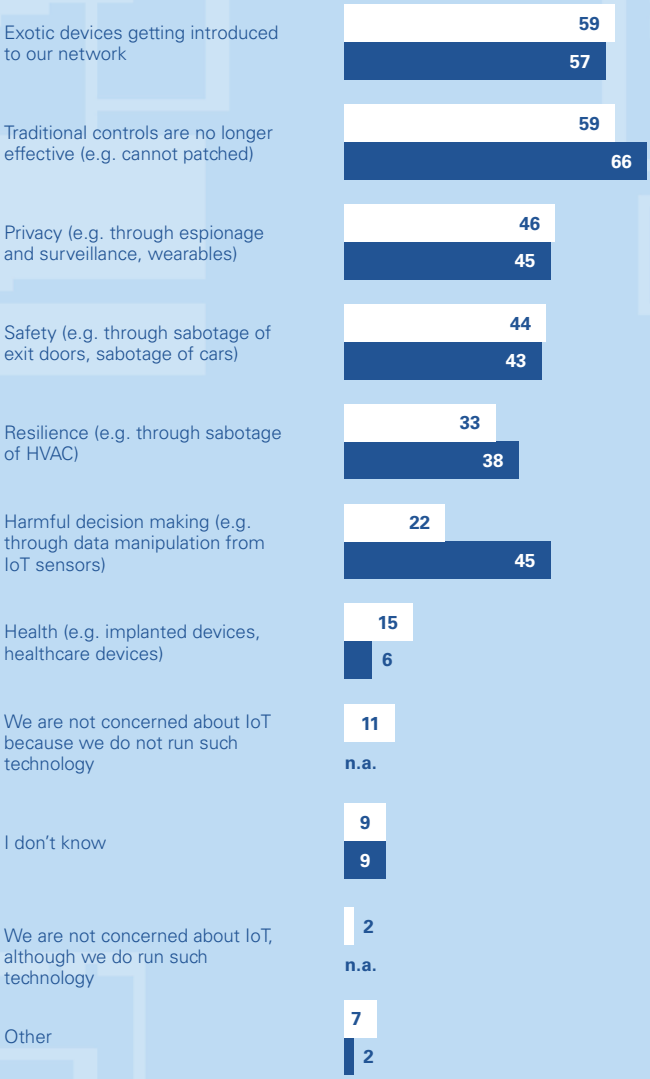
31%

leverage security by design when deploying IoT-enabled assets.

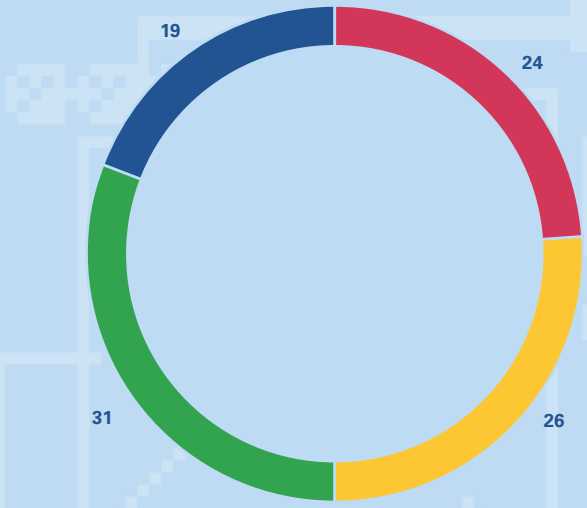
59%

state that their main concerns regarding IoT-related risks are exotic devices that are introduced in the organization's network and the fact that traditional controls are no longer effective.

What are your biggest concerns in regards to IoT?
(in percent)



Do you leverage security by design when deploying IoT-enabled assets (e.g. HVAC, Building Automation, Access Control)? (in percent)

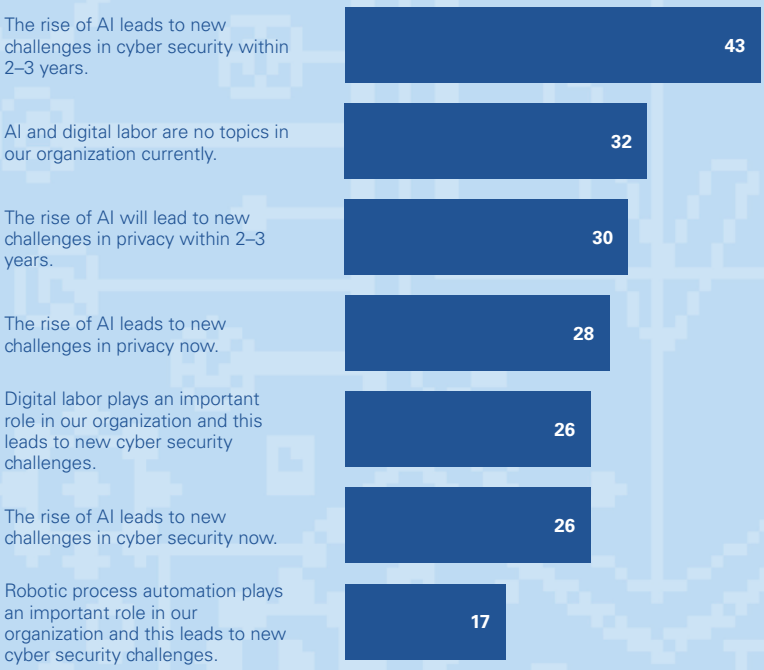


The rise of machines brings new vulnerabilities

The bots are coming!
You can't have missed the reports about robots taking over the (business) world. Armed with artificial intelligence (AI) and machine learning (ML) techniques, they can outperform humans in terms of productivity. They never get bored or sick. What's happening beyond the marketing buzz? A lot, in fact.

First of all, more automation of human tasks inevitably leads to higher impact of successful attacks. Systems become increasingly more interconnected and have stronger dependencies as humans are no longer in the loop. A domino effect may then have serious consequences and this calls for a new perspective on being resilient.

When describing AI in your organization (in the context of digital labor, analytics, etc.) and the corresponding (new) security issues, with which of the following statements do you agree? (in percent)



Second, this domain develops at astonishing speed. Up to now, most applications of Robotic Process Automation can still be found in routine and point-to-point processes. More recently however, we also see emerging examples of more cognitive tasks as robots are entering the AI domain. Cognitive software mimics human activities such as perceiving, inferring, gathering evidence, hypothesizing and reasoning. When combined with advanced automation, these systems can be trained to execute judgment intensive tasks. As such, cognitive automation is creating a new class of digital labor that can enhance human skills and expertise.

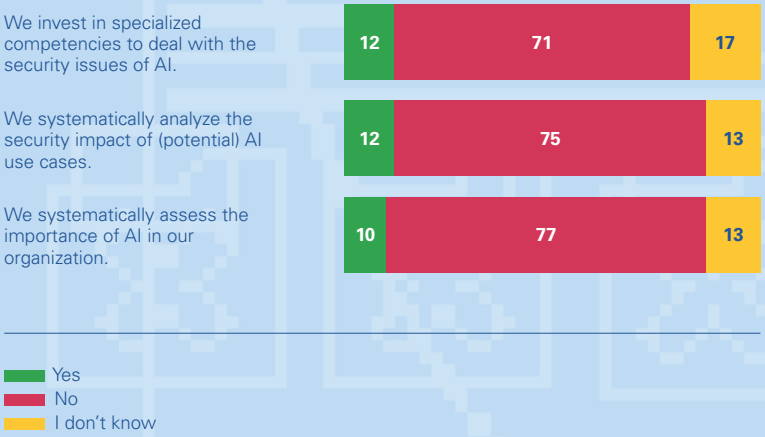
Trendsetting organizations have jumped on the Artificial Intelligence bandwagon. They start using AI techniques such as machine learning, computer vision and natural language processing. This may result in a tremendous shift as white-collar outsourcing is no longer going to the East but is moving to the cloud. A recent example is a Japanese insurance company who replaced 34 employees whose daily job was to calculate payouts. The cognitive technology can think like a human, enabling it to analyse and interpret data, including unstructured text, images, audio and video. What's typical about these technologies is that they learn on the job by studying how people make decisions. This is a world apart with the traditional automation technology that is based on pre-programmed business rules.

How does all this relate to the subject of cyber security? Simple. We become more dependent on machines. Machines take over human decisions and/or play a stronger guiding role in their decisions. We get addicted to algorithms. Therefore we must take proper measures to prevent these algorithms from being compromised.

We asked our respondents what they think of this topic. One of the findings that stands out is that they think it's a topic for the future rather than now. Only 26% agree that there are new security challenges today. When asked about the near future of 2-3 years, this percentage increases to 43%. When the same question is asked regarding the (potential) impact on privacy, 28% believe that there is an impact today and 30% believe they'll see an impact in 2-3 years. It seems that digital labor is still in its infancy among the respondents. Only 17% say that it plays an important role in their organization – raising new cyber security challenges. And one third admits that Artificial Intelligence and digital labor are simply no topics in their organization.

Innovations in this domain emerge at a dazzling speed. As a consequence, even organizations who are in the very early stages of (thinking about) deploying such new technology should be on the watch. Security in the domain of Artificial Intelligence and digital labor may quickly become the next elephant in the room. An impact analysis – understanding the related cyber risks. At a minimum, they should conduct an impact analysis to understand all related cyber risks.

How do you deal with the theme of AI and cyber security?
(in percent)



26%
think that the rise of AI leads to new challenges in cyber security now.

43%
believe that the rise of AI will lead to new challenges in cyber security within 2–3 years.

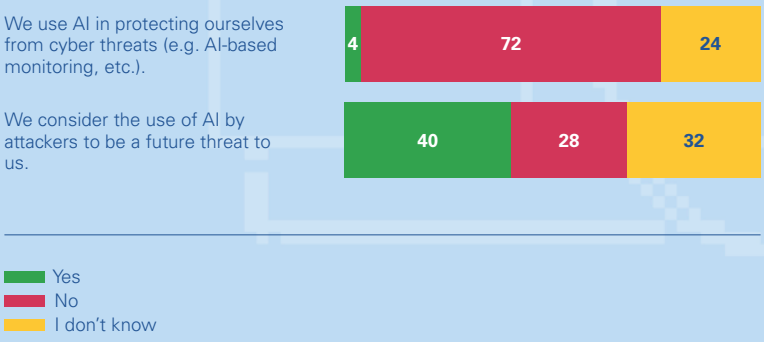
Criminals are discovering the potential of Artificial Intelligence; and so should you

In the past five years, digital criminals have started leveraging new automation technology to launch strikes

They now also embrace Artificial Intelligence concepts. One example is that adversaries can analyse massive amounts of stolen data to identify potential victims and build contextually detailed emails. These emails can target individuals in a tailor-made manner that was previously impossible. Another new option is that criminals use new evasion techniques based on building up intelligence about the defence strategies.They can 'poison' defence models by bombarding an environment with information that's full of false positives and appears to be detectable by a defender's various tools. Thereby, they can 'poison' the defence models.

> **We're only at the beginning of a whole new league in cyber security – machine to machine hacking. The survey shows that companies are starting to be aware of this. 40% says they consider the use of Artificial Intelligence by attackers a (future) threat.**

Your view on Artificial Intelligence in relation to cyber security
(in percent)



Based on our experience, many organizations largely use manual efforts to aggregate security findings and contextualizing them with external threat information. This is no longer a viable strategy in the age of machine-to-machine hacking. To address the new challenges, organizations must use artificial intelligence in their day-to-day cyber security operations. Only 4% of our respondents are actually doing this. A deeper analysis of our survey results also shows a strong correlation between organizations who systematically assess the impact of AI on the one hand and high growth in the annual budget for cyber security on the other. This may indicate that these companies are preparing themselves financially for the next phase in cyber.

It's not hard to predict that this will have to change in the years to come. We're moving towards a tipping point where humans can no longer cope with both complexity and massive volumes of (intrusion) data. Artificial Intelligence can and should help us to detect patterns in the sheer volume and complexity of data. This is not easy, as unsupervised machine learning often contributes to massive amounts of false positives, resulting in alert fatigue.

MIT's Computer Science and Artificial Intelligence Lab speaks of the future of so-called human-interactive machine learning to cope with this. In this concept, systems analyze internal security intelligence, and correlate it with external-threat data to help human analysts to find the needle(s) in the haystack. Humans then evaluate this information and give feedback to the system. The feedback loop enables the system to adapt its monitoring and analysis capabilities based on human inputs. As a result, the system gets better in finding real cyber threats and minimizing false positives.

CaaS: Crime as a Service

We just got used to concepts such as Software as a Service (SaaS), Platforms as a Service (PaaS) in recent years. A new 'star' is now on the rise: Crime as a Service.

In the digital underground economy, each actor, from sophisticated criminal groups to the fledgling cybercriminals, has their own particular skill set and area of expertise. In the underground, cybercriminals don't need to have the capabilities themselves to deploy criminal acts that range from exploit kits to ransomware. The ecosystem simply offers a marketplace for this.

Need for speed

Once vulnerabilities manifest, hackers often take advantage within minutes. Resolving these vulnerabilities often takes much longer. In fact, it can take months to patch things up. The contradiction is in fact a strong call for the use of new techniques to cope with the need for speed.

As the attack surface has ballooned significantly, it's even more pressing to use new techniques. In the past, focussing on network and endpoint protection was sufficient. In the past, it was sufficient to focus on network and endpoint protection. With numerous new applications, cloud services and devices, organizations are battling a broadly extended attack surface.

The consequence is that to be safe, a myriad of data must be analyzed. Without intelligent tooling we would need legions of staff to comb through the huge amount of data to connect the dots and find latent threats. The manual routines often took months, during which time attackers exploited vulnerabilities and extracted data. This is no longer an option.

4%

use AI to protect themselves from cyber threats (e.g. AI-based monitoring etc.).

40%

expect that AI is going to be used by attackers in the future.

Distribution of survey participants by sector

Survey Methodology

KPMG conducted this Cyber Security survey of Swiss companies in January 2017. The survey's goal is to gain insight into the current state of cyber security in Swiss companies. 60 participants completed the online survey consisting of 39 questions. 32 participants were from large enterprises (> 5,000 FTEs) and 28 from small and mid-size companies (SMEs). In addition, personal interviews were conducted with subject matter experts have been incorporated into this study. The analysis of the results was carried out by KPMG's Cyber Security experts. The study's content derives from the survey and is complemented by the expertise of KPMG's consulting practice.

Our approach to cyber security

Cyber Security: It's a business issue, not just an information technology issue

Cyber Security is a strategic enterprise risk that goes far beyond information technology. That's why cyber security demands attention not only from the CIO – but also from the rest of the C-Suite, the board and, indeed, employees and business partners throughout the organization.

Working shoulder-to-shoulder as your approachable, attentive, strategic advisor

Instead of coming to you with a preconfigured approach, we take the time to understand your business priorities, strategic direction and operations – so we can bring an appropriate context to your cyber security risks and help protect your critical business processes.

Translating cyber security into a language your business can understand

Cyber Security affects different parts of your business, and that's why we translate cyber risks into an appropriate language for each. Whether we're working in your boardroom, back office or data center, we seek to provide a jargon-free explanation of your cyber threats, the potential impact to your critical assets and the recommended response.

A business-led approach, supported by deep technical skills

We know how to put cyber security in an appropriate business context because we see the world from your perspective. We bring a combination of technical domain expertise and cross-functional business expertise. With that combined background, we understand cyber security risks in all layers of your business.

Expertise in your industry

As you're navigating cyber security, it's important to have an advisor at your side who understands the challenges, threats and strategies in your industry. That's why, as part of bringing a business context to cyber security, we also an industry context.

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

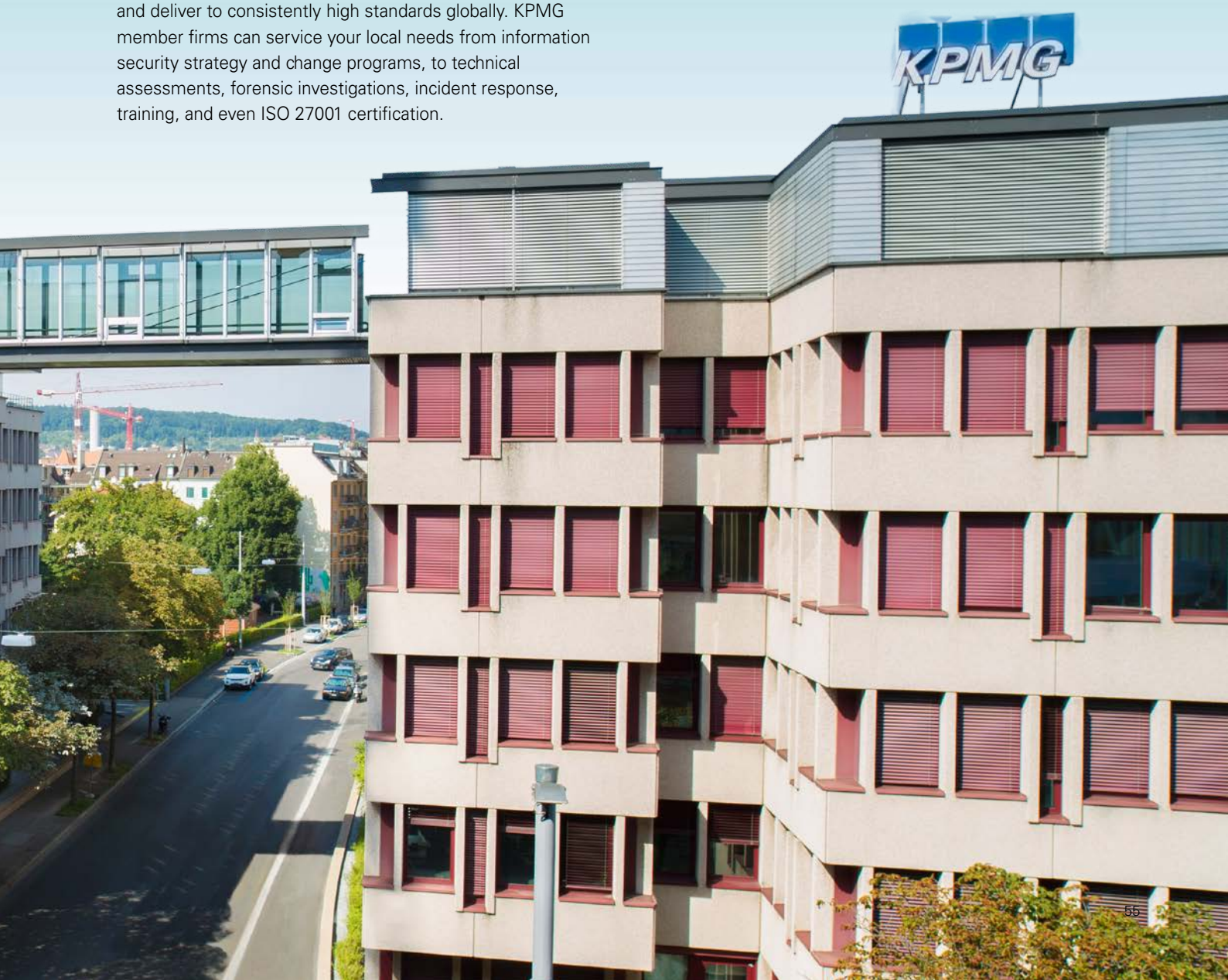
We have more than 2,000 security practitioners working in KPMG's network of firms, giving us the ability to orchestrate and deliver to consistently high standards globally. KPMG member firms can service your local needs from information security strategy and change programs, to technical assessments,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

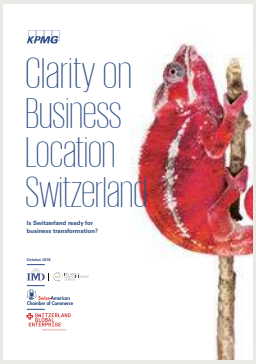
This series of publications from KPMG Switzerland provides insights, analyses and studies on a range of topics. All publications are available as hard copies as well as online. For more information, please contact **kpmgpublications@kpmg.com**

Latest issues

Clarity on
Insurance Digitalization

Clarity on
Swiss Taxes

Clarity on
Transformation in Private Banking



Clarity on
Business Location Switzerland

Clarity on
Healthcare

Clarity on
Transformation

Clarity on
Non-Life Insurance

Special

Shaping Switzerland's digital future

Clarity on
kpmg.ch/clarity-on

KPMG Knowledge App

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

Download on the App Store

GET IT ON Google Play

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

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

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

Marc Bieri
Director,
Cyber Security
+41 58 249 64 05
marcbieri@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
CH-8036 Zurich
+41 58 249 31 31
+41 58 249 44 06 (Fax)
kpmgpublications@kpmg.com

Study and editorial team KPMG
Matthias Bossardt
Roman Haltinner
Yves Bohren
Konrad Schwenke

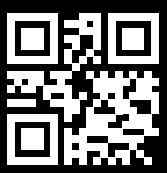
Concept and design
Sabine Lorencez, KPMG
Stephan Erdmann, KPMG
Andi Portmann, Konkret

Print
PrintCenter Hergiswil

Pictures
Shutterstock
iStock

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