Resilience as key competency in case of crisis

Concluding report | 6. FSS Security Talk on the 10th of September 2020, Webinar

In the VUCA world (Volatility, Uncertainty, Complexity, Ambiguity), the triggers of failures and disturbances have multiplied. Resilience as a security concept, in addition to classical risk management, is necessary for the survival of interlinked systems. The speakers agreed that particularly soft factors are decisive for maintaining and building resilience in organisations.

Around 80 interested parties attended the 6th FSS Security Talk, which was organised by the FORUM SICHERHEIT SCHWEIZ (FSS) together with the AWK Group. Fitting to the topic, an FSS Security Talk was for the first time held online as a webinar. The Covid 19 situation had made it necessary to shift the event and move it to the digital space. After a short welcome by Fredy Müller, Managing Director of the FSS, the floor was given to the speakers, who came from Switzerland, Italy and - in the case of National Councillor Judith Bellaïche - direct from the Federal Parliament.

Resilience as an answer to the complexity issue

In his introductory presentation, **Dr. Benjamin Scharte**, Head of the Risk and Resilience Research Team at the Center for Security Studies (CSS) at ETH Zurich, explained the concepts of complexity and resilience and their interrelationship from a scientific perspective. Using the example of the formation of a traffic jam on a motorway, Dr. Scharte illustrated the most important property of **complex systems**, **emergence**: in complex systems, results cannot be explained by the behaviour of the individual components of the system, but only at the level of the overall system. In many cases, a traffic jam does not occur because a single driver causes an accident, but because small deviations in the individual behaviour of each driver add up to the jam.

The second important property of complex systems is **uncertainty**. Therefore, **strategies** are needed to **deal with** this **uncertainty**, which is the link to resilience. Resilience, however, does not simply mean a return to an initial state. The **roly-poly toy** is consequently **not a good symbol** to explain resilience. Instead, according to Dr. Scharte, a **systemic understanding** of **resilience is needed:** Resilience is the ability to **react and adapt to changes**, especially unexpected ones.

Source: Presentation Dr. Scharte

As complex systems **always** become **more complex**, we must deal with more and more unexpected, disruptive events. Resilience is becoming more and more necessary. **Complexity** is not only a driver, but also a **prerequisite for resilience**. Only complex systems can adapt when confronted with unexpected events. Resilience-increasing system principles are modularity, diversity, decentralisation and redundancy.

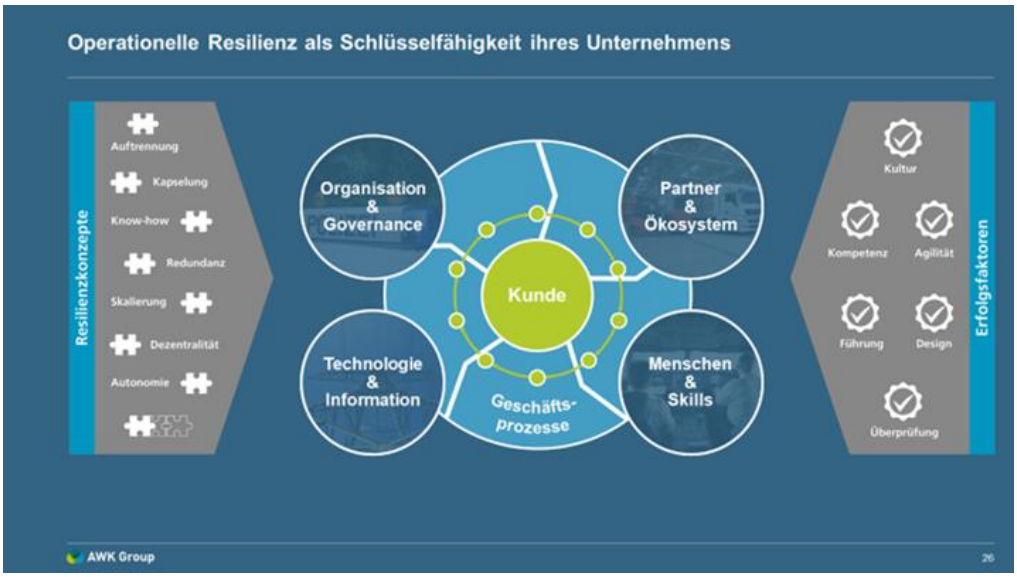
Resilience as security concept for organisations

Dr. Adrian Marti, Head of Cyber Security and Privacy at the AWK Group, supplemented this scientific perspective with practical experience in the second introductory presentation. Dr. Marti listed four reasons why resilience is becoming an increasingly important topic for companies and public sector organisations: Firstly, such organisations are increasingly **embedded in ecosystems** and dependent on other organisations in the value chain. Secondly, resilience is a **market need**; in certain segments customers expect uninterrupted service. Thirdly, in some segments the **regulator** makes regulations on resilience. And fourthly, the **quality of threats** is increasing, especially in the cyber environment. It is therefore no longer a question of fending off an attack, but of recovering as quickly as possible from a successful attack.

In a new study conducted by the AWK Group on **cyber security**, **70% of the organisations** surveyed stated that cyber security was a **differentiating factor** for them in the market. However, only **20% of the organisations** considered their **cyber-resilience capabilities** as **sufficient**. According to Dr. Marti, there is therefore a **blatant contradiction** between the importance of the topic and the achieved level of preparation. Thus, the question is how organisations can become more resilient.

According to Dr. Marti, organisations have a whole **building block of concepts** at their disposal to promote resilience. In particular **soft factors** are crucial for building and maintaining resilience: the culture, leadership and agility of the organisation. Resilience must be built into the design of processes and systems right from the start and must also be built up **across company boundaries**. After all, one's own resilience concepts need to be **regularly reviewed**. Ultimately, however, each organisation must decide for itself how much resilience it needs. The more **time-critical and interchangeable** its own services are, and the more **public attention** is

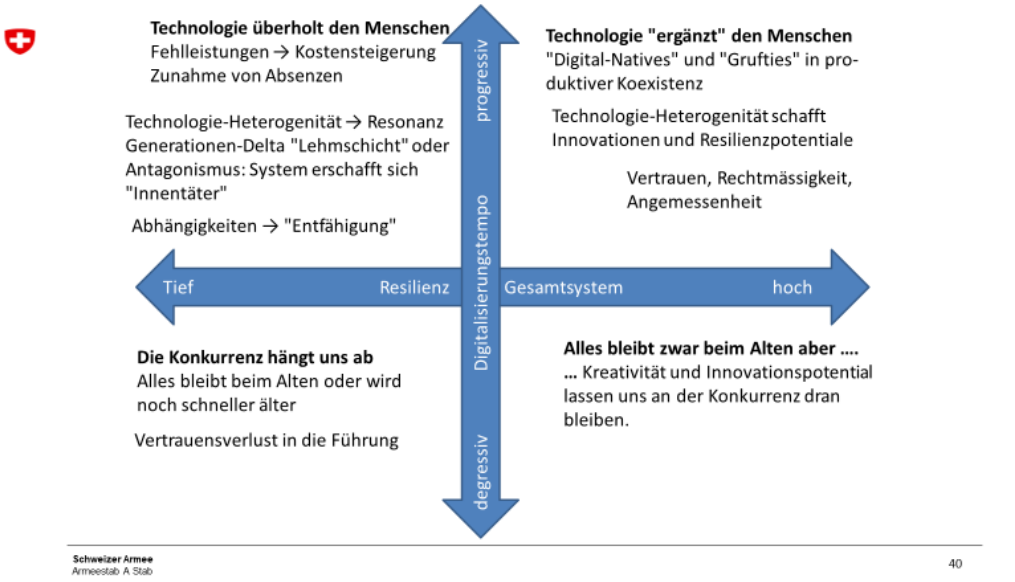
paid to its own organisation, the more resilience is needed. The most important success factor, however, is that resilience is discussed **daily at all levels of decision-making.**



Source: Presentation Dr. Marti

Reconciling human and social needs with technological needs

In the first case of the event, **Dr. Martin Krummenacher**, KPM Doctrine Research in the Armed Forces Staff, addressed the potential for resilience in the socio-technical system of the **Swiss Armed Forces**. For Dr. Krummenacher, resilience is not developed despite, but rather **because of adverse circumstances**. It is developed in a lagging process and has a learning effect on the entire organisation. Resilience can therefore be regarded as a **product of successful risk management**. Regarding Switzerland, he considered **particularly federalism as a system characteristic that increases resilience.**



Source: Presentation Dr. Krummenacher

Dr. Krummenacher used a scenario cross to demonstrate the effects of a high development speed of digitisation on organisations with a low level of resilience. The consequences were **stress disorders** and **break lines through generations** up to deliberate sabotage by internal perpetrators. Therefore, digitisation requires a guided process and an integral resilience culture, which aims to ensure that **technology complements** rather than replaces **people**. One way of doing this would be to offer so-called "**offline days**", on which a part of the company is forced to work conventionally. It became apparent that the digital natives were dependent on the **experience of the "gothys".** Often innovations and resilience potentials emerged on such offline days and fears of digitalisation were reduced.

The Swiss Armed Forces' research on resilience in crisis situations showed that **soft psychological factors** were often the **most robust elements** that contributed to the management of critical situations. In particular, over-regulation and outside interference by the leadership seemed to have a destructive effect on resilience. Overall, it was shown that **elements that destroy resiliency promote digitisation** and, conversely, elements that promote resiliency are damaging to successful digitisation, e.g. decentralisation and the self-regulation of groups. According to Dr. Krummenacher, this area of tension must be considered, and **human and social needs must be reconciled with technological needs.**

Even as an SME you can be resilient and secure

In the second case, **Martin Leuthold**, head of the "Security & Network" department at Switch, illustrated how Switch creates resilience and cyber-security for the operation of critical infrastructures. Switch was established as a service provider and self-help organisation for Swiss universities and is now a non-profit foundation supported by the federal government and cantons. As an SME, Switch today operates **three national critical infrastructures**: the DNS infrastructure for .ch and .li, the Swiss research network and the national Multisector Computer Emergency Response Team (CERT).

Source: Presentation Martin Leuthold

Using the example of the **Swiss research network**, Mr. Leuthold demonstrated the wide range of measures that are necessary for the secure and resilient operation of critical infrastructures. Switch solely rents fibre optic cables and otherwise has all the skills and the technical and operational know-how in-house. The structure of the research network is characterised by **redundancies**. There are approximately 3,000 km of fibre optic lines and at least three independent weaves in the north-south and east-west direction, so that there is **no single point of failure**. International connections are ensured by five Internet Exchange Points. All universities are connected to the network with two geographically redundant fibre optic lines. Switch also operates **two independent data centres** in Zurich and Lausanne. In addition, Switch has large **bandwidth reserves** at all levels, which even managed to cope with the load change by switching completely to **distance learning** in early spring. Switch also maintains a minimum of **self-sufficiency** in terms of replacement material and creates organisational resilience through a **cooperative operating approach** with the universities.

The **DNS infrastructure** is the critical element for the **domain registry**. It translates all Internet addresses into IP addresses; in the event of a failure, no .ch or .li address would be accessible. The DNS infrastructure uses all these resiliencies in the basic infrastructure and is operated by Switch itself. Both the research network and the domain registry benefit from the third critical infrastructure, the **multisectoral CERT**, which ensures the internal capability for crisis management. Overall, it appears that even an **SME** can be **resilient and secure** when providing **critical services.**

Technology is only a component of resilience

In the final third case, **Sandra Hauser,** Head Transformation & Technology at Zurich Insurance, gave an insight into the financial sector's perspective on the topic of resilience. According to Ms Hauser, resilience means overcoming crises in an unstable environment and continuing to generate value. **Technology** is an important component for this, but from the perspective of the financial sector there are **many other components** that are necessary for resilience. Besides the **technological components** mentioned above, these include **legal components, people components and regulatory components.**

In practice, in terms of resilience, preparation must be separated from action during crisis itself. Sandra Hauser particularly emphasised **change readiness** as an important asset in the preparation phase: An organisation that is not prepared to change is not able to react to specific problems in the event of a crisis. In the Corona crisis, this meant in concrete terms enabling Zurich's employees to work from **home office**, **ensuring accessibility for customers**, managing **cyber risks** and dealing with significantly **increased insurance claims**. At the same time, an organisation learns with every crisis. For Zurich, it became clear that despite good preparation, additional measures were necessary, such as expanding call centre functionality, enabling remote customer identification or making cyber threats more relevant.

Source: Presentation Sandra Hauser

In general, Sandra Hauser identified four essential characteristics of cyber-resilience: resilient corporate management, the **tone-from-the-top** must be set right, a resilient corporate culture, the exchange of information in resilient networks, and resilient change readiness. Resilience obviously includes **all components**. Like Dr. Marti, Sandra Hauser emphasised that resilience must be ensured along the **entire value chain**. At the same time, she was also convinced that the issue of resilience must be given space in the **entire strategic planning**.

Creating awareness of resilience and cyber-security

The panel discussion that followed was attended by the aforementioned speakers as well as **National Councillor Judith Belläiche** (GLP, ZH), Managing Director of the Swico trade association. With regard to the Corona crisis, Judith Bellaïche noted that the legislature had slipped into the crisis somewhat unprepared. The executive had been better prepared, but what had not worked at all was **data generation and data exchange.** This problem must be solved in the future, no matter what the crisis.

She also noted that **external relations** are crucial for the survival, recovery and normalisation of society and the entire economy. This concerned, on the one hand, **communication during the crisis** and, on the other hand, economic recovery. Given the high degree of external dependence, all domestic measures are only effective if **foreign trade** is also functioning. In this context, Ms Bellaïche notes the importance of **resilient relations**.

From Swico's point of view, Judith Bellaïche's conclusion from the crisis was clear: there was a need to focus more on **digitisation**, create **redundancies**, increase **digital literacy** and, finally, **cyber-security**. She was convinced that the Corona crisis had shaken up the administration and companies to finally tackle the existing deficits in these areas.

The importance of soft factors and the human being as a key insight

Asked about their key insights from the event, all panelists were pleased about the many things they had in common. **Dr. Adrian Marti** emphasised the importance of **soft factors** to create resilience: You must establish the culture from the top down, set the tone, so that resilience becomes an important issue in your own organisation. **Dr. Benjamin Scharte** emphasised that resilience cannot be implemented in a purely technical way, the human being must and should always play a role. In the end, it is a question of how to support the human's own **improvisational ability and creativity with technology**. For **Dr. Martin Krummenacher,** it was central that everyone had mentioned **redundancies, decentrality and soft factors**. Interestingly, the latter were the most robust in the crisis. **Martin Leuthold** considered it crucial that **resilience and cyber security** are anchored in the **DNA of a company**. One had to get away from the idea that we could save ourselves with technology alone. **Sandra Hauser** stressed that it was crucial to think about the entire value chain during the preparation phase. For Zurich, it had become clear that there was a great deal of exposure, especially with its **outsourcing partners.**

Asked by the audience about the resilience of Swiss society, **Dr. Benjamin Scharte** replied that Swiss society is very resilient from the point of view of **social resilience**. This is expressed strongly in **social networks** and the **social capital** that is formed. The Swiss population may not even be aware that it is resilient. But from a research perspective, the speed with which new ideas for supporting fellow citizens developed bottom-up during the pandemic shows that there is a great deal of social resilience.

In her closing message to the audience, **Sandra Hauser** again emphasised the importance of **preparation** and the inclusion of soft and hard factors in this preparation. **Dr. Benjamin Scharte** pleaded for **people** not to be viewed as the greatest risk and the greatest possible weakness, but rather as the **greatest asset** and actual **source of resilience**. **Dr. Martin Krummenacher** emphasised the importance of **informal structures**. These must be kept open, because they would ensure that it would function even if the management were to fail. **Dr. Adrian Marti** dedicated his concluding sentence to an appeal: Start **building resilience where it matters most** to you.

In his closing words, **Oliver Spiess**, partner in the field of Public Safety and Defense at the AWK Group, thanked all speakers and summarized the event. From Dr. Benjamin Scharte he had learned a new foreign word, emergence. He had heard from Dr. Adrian Marti that resilience must be built up systematically, that the modular system is very important and that resilience does not stop at the company's boundaries. With Martin Leuthold, he was reassured to discover that the .ch infrastructure contains so much redundancy that it can withstand almost anything. He thanked Sandra Hauser for her description of the current situation and how Zurich Versicherung had mastered it. And with Mrs Bellaïche he heard again that external relations are important. Resilience does not stop at one's own company boundaries, but rather the whole ecosystem must be considered. Finally, Oliver Spiess thanked **Martin Leuthold** and **Switch** for **sponsoring the event.**