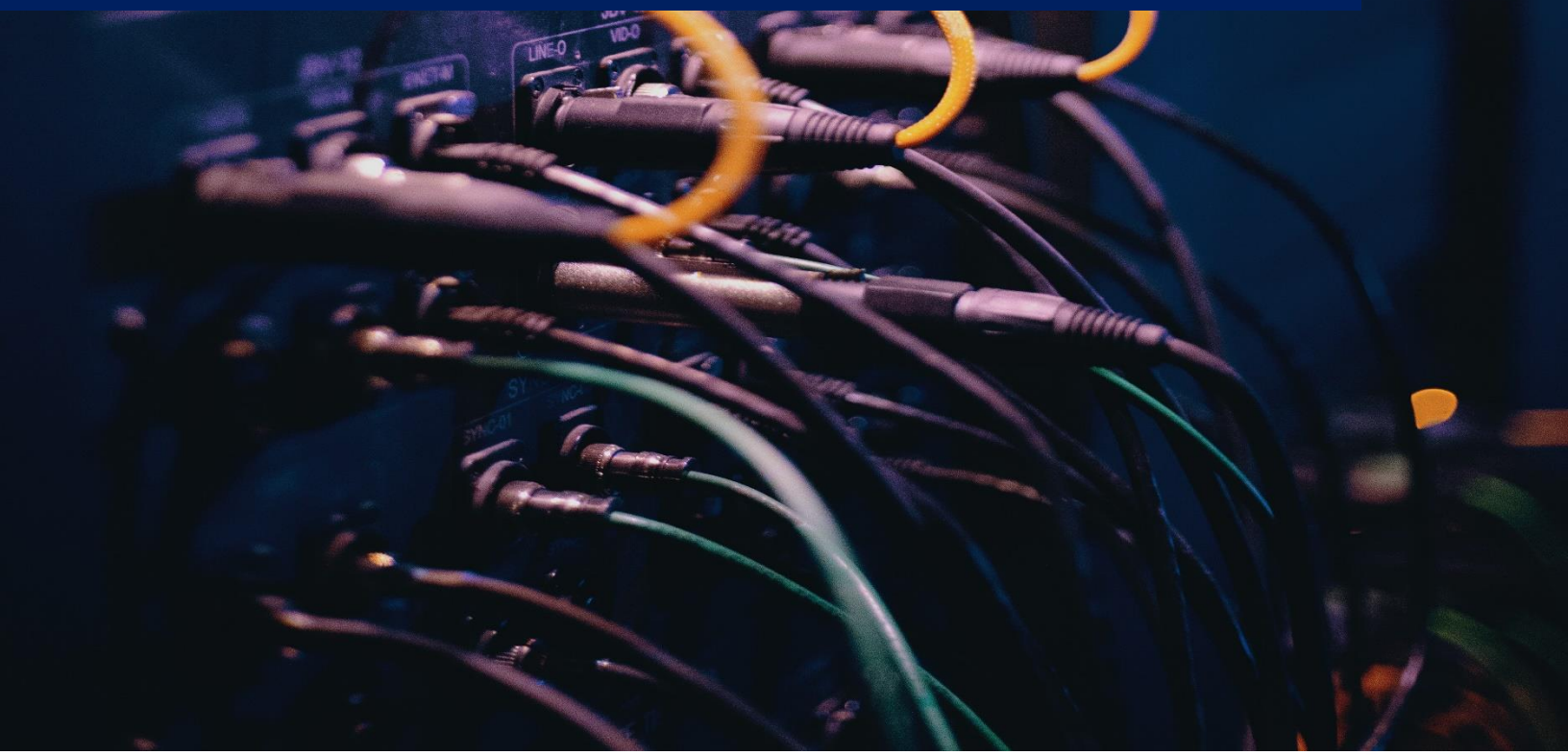
SMALL ENTERPRISE

AUSTRIA

The risk story 5



Co-funded by the
Erasmus+ Programme
of the European Union

BEPREPARED

Small enterprise from Austria

Context of the Company and the Supply Chain

The company is a medium sized company, founded in 2006, with around 30 employees specializing in security service and security consulting. The company performs security or IT penetration tests. Entire companies are tested for protective measures and attempts are made to gain system control over the IT without prior knowledge. This is one part of the portfolio, the second is the complete consulting complex that goes beyond the attack. Afterwards, road maps are drawn up to make the customer more prepared for the future and more capable of defending themselves.

Digitalization of SC

The company has a high level of digitization. The whole business model is based on modern technologies that have emerged in the course of digitalization.

Risk Management

All partners are in charge of risk management.

Practice of Risk Management: Employees have a high number of reading and editing rights, because they have a high level of security awareness. A very strict separation is made between task areas and customer areas, so that every employee can access the documents where a product is currently being developed. Any methodology, any product information or any technology can be accessed. But only the few employees who are involved with a customer can access customer information. The need-to-know principle is applied and there is extremely limited access to everything that is customer data.

Risks: Currently, the company is primarily exposed to operational and COVID-19 risks.

Co-funded by the Erasmus+ Programme of the European Union

- Operational risk. After a customer enters into a cooperation, an initial assessment of the situation is made, possibilities for improvement are elaborated and improved in dialogue with the customer. The risk is that the customer' information is handled either carelessly or not carefully, and the data is lost or sold, by employees. If this happens, this will draw a lawsuit and the company faces a serious reputation loss.
- Financial risk. There were no specific risks reported.
- Market risk. There were no specific risks reported.
- Cyber risk. There were no specific risks reported.
- The COVID-19 related risk. Especially during a pandemic, the problem that security concepts have to be provided with enough resources, both financial and human, and that the management and also the IT management have to take the time for it, is rising. The biggest challenge is resources and awareness.

Benefits of risk management: The need-to-know principle gives control, as well as standardization regarding communication. Data to the customer goes only through selected people to the customer. All technicians involved at that customer, are consulted again before anything is sent out. Coming with risk management, several things are used to protect the data and the customers' data. Classification, multiple encryption solutions, multiple multi-factor authentication, different email protection systems, certificates of the emails, backup systems and multiple locations of the backup systems and the data.