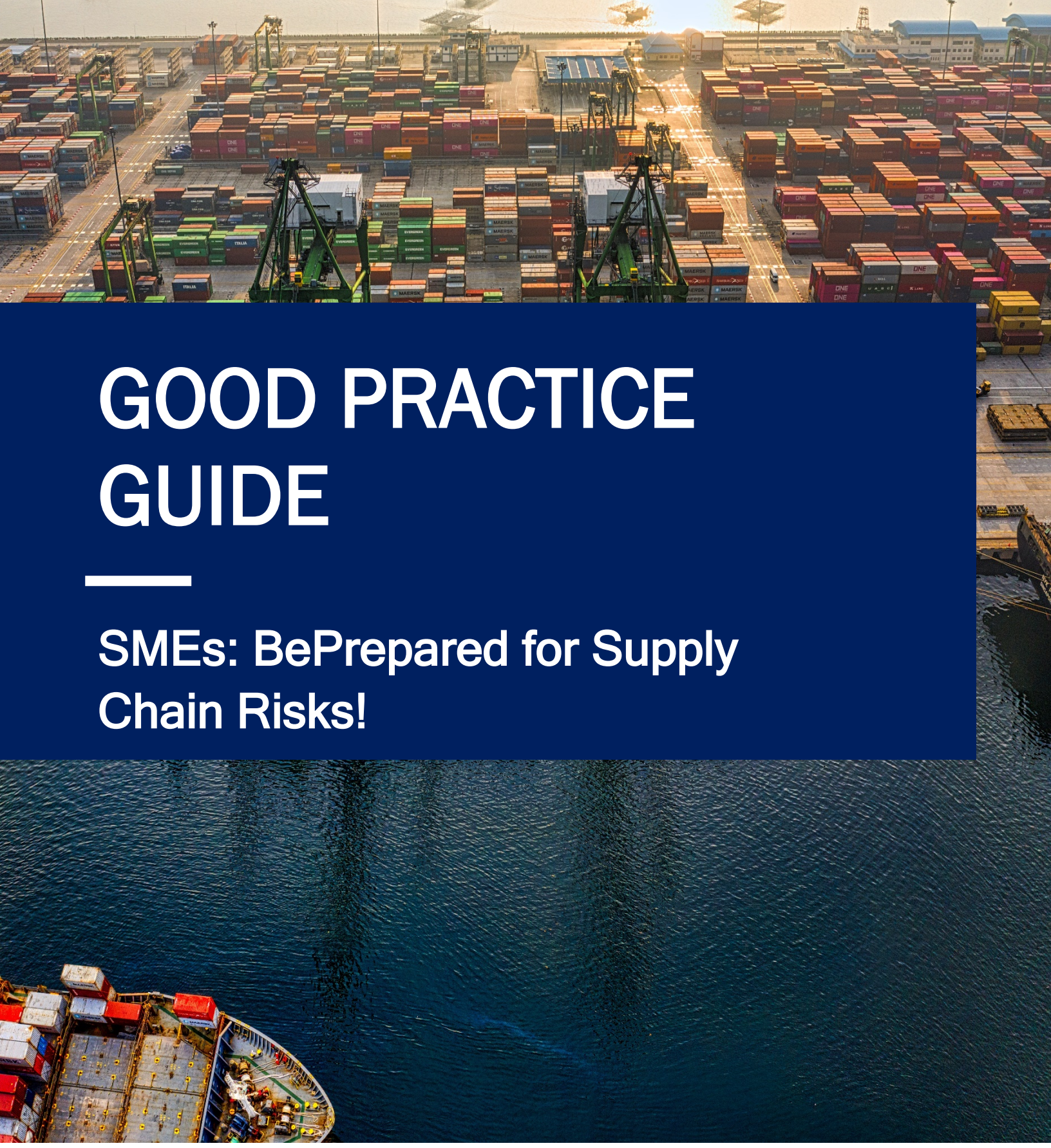
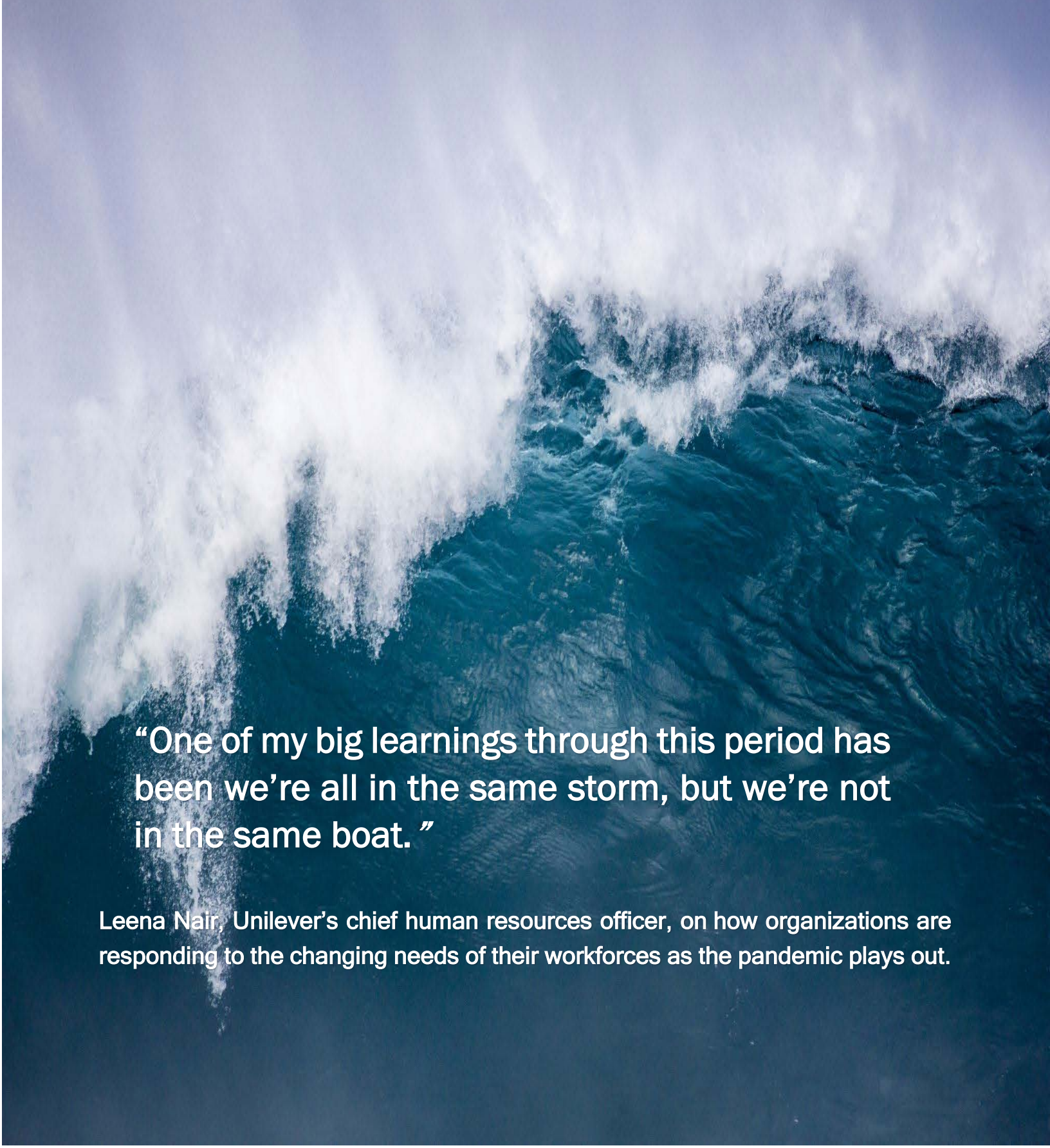


GOOD PRACTICE GUIDE

SMEs: BePrepared for Supply Chain Risks!

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

SMEs BEPREPARED



“One of my big learnings through this period has been we’re all in the same storm, but we’re not in the same boat.”

Leena Nair, Unilever’s chief human resources officer, on how organizations are responding to the changing needs of their workforces as the pandemic plays out.

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

BEPREPARED

Introduction

Supply chains have become more and more connected and globalized. Data exchange has increased over the years due to the Information and communications technology (ICT) advancements. Even though this increased data exchange can contribute to certain benefits such as improved processes and planning it also bears several risks such as the loss of proprietary knowledge or unintended revelation of crucial business insights to other actors. Further, the increasing digital integration of supply chains bears the risk of being in the focus of cyber-attacks. Both threats, (1) not to know which business insights or critical knowledge can be derived from shared data, and (2) to be the target of a cyber-attack are major concerns of companies regardless of size. For example, the Allianz Risk Barometer 2020 ranked cyber incidents for the first time the number one business risk. Recent reports further show, e.g., 8th annual ENISA Threat Landscape (ETL) 2020 report, that small and medium-sized enterprises (SMEs) have become equally vulnerable. Thus, a sound understanding of risks that can occur in supply chains is an essential part of the overall competences SME professionals should have to act in confident, critical and responsible ways.

This guide is one of the outcomes developed in conjunction with the Erasmus+ project “SMEs: Be prepared for supply chain risks” which was intended to support SMEs to be better prepared for identifying and handling risks associated with supply-chains.

The guide is based on insights collected from SMEs located in six EU countries (i.e., Austria, Estonia, Germany, Greece, Italy and Portugal). These SMEs represented different sizes (i.e., micro, small and medium-sized) and industries.

The primary aim of the present guide is to help SMEs owners and managers to learn from the experience of other SMEs as to how to operate and approach a number of selected risks.

The partners of the “SMEs: BePrepared” project wish a pleasant and knowledgeable lecture!

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

Risk management - why and how?

We start with a short introduction to risks and their management.
Risks have been defined, for example, by the adverse impact on profitability of several distinct sources of uncertainty. Even though the construct of risk refers to positive and negative outcomes, in our everyday language it appears that risk is mainly associated with danger. Risk can be divided into financial and non-financial risks. The former category establishes a relationship with something monetary and quantifiable, while the latter does not.
Risk management is primarily about identifying, assessing, monitoring and controlling firm risks. Thereby, firms should focus on all types of risks and their management. In recent years, the requirements for risk management approaches have increased significantly and thus there is a need for integrative approaches to better handle present and forthcoming risks. The significance of risk management approaches is, for example, stressed in quality standards such as ISO 9001:2015. Good risk management approaches assess the impact of different sorts of risks on one another and are based on an understanding that managing risks must not mean that business activities are stopped, but on the contrary they are there to facilitate a more manageable and proactive way of handling risks.
Research on risk management in SMEs suggests that these firms often lack both dedicated approaches to risk management and the necessary skills as well as competencies needed to do risk management.1 At the same time the firms are exposed to several challenges such as skills shortage, climate change (keyword circular economy), the progressive digitalization, and succession planning to name a few in addition to the still ongoing pandemic. This not only increases the danger of new or different risks, but also the need for risk management.
In the following several risk scenarios are presented. They were derived from the project's data collection and brought together with past and other ongoing research activities being conducted by the project members involved in the project "SMEs: Be prepared for supply chain risks".

In this study, the SME definition as proposed by the Commission of the European Communities (2005) is followed. Accordingly, firms can be classified as micro, small, or medium-sized depending on the number of employees and annual turnover or balance sheet totals. Referring to the number of employees, a company with fewer than ten employees is considered to be a micro firm, with between ten and 49 employees a small firm, and with between 50 and 249 employees one speaks of a medium-sized firm.

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

1 Risk exposure: Internal vulnerabilities due to people

The situation

Unforeseen internal risk situations can and will happen in any organization, regardless of size and type. Additionally, all organizations depend on skilled people to address present and future challenges. This is true for smaller companies, in particular given the situation that often there "are more tasks than heads". This situation makes smaller firms rather vulnerable. In contrast to their larger counterparts, smaller firms often have difficulty in attracting and retaining skilled persons. There are several examples around showing that a skilled professional was trained and developed within the small firm only to be poached by a (bigger) competitor. The data collected for this project has unfortunately further confirmed the above-mentioned.
For example, the participant from a micro firm located in Estonia reported:

> *It takes from several months up to a year to train an employee to have a complete set of professional skills. Often, a large company poaches that employee and offers her a significantly bigger salary. The worker quits, and then we need to find, hire, and train a new one. In a small market like Estonia, one can do nothing to prevent this situation.*

While a participant from a small Austrian company mentioned:

> *The selective poaching of personnel is a knowledge risk that has inhibiting factors for risk management. Trained personnel take the accumulated knowledge with them and thus pose a risk.*

Possible consequences

Possible consequences of the above-described situation are easy to imagine. In case of a turnover, it is rather likely to assume that one or several of the remaining organization members must take over the tasks of the leaving person, which in turn increases the likelihood of stress as well as demotivation and in turn may result in the worst case in further turnovers. However, it is also conceivable that no one in the firm can take over the tasks of the leaving person due to knowledge concentration found with the latter. Thus, the firm concerned might be forced to halt the operations. Furthermore, the above-described situation increases the

danger of a permanent reinvention of the wheel, which is rather costly; considering both the direct and indirect costs involved in personnel development. Finally, the departure of a person to a competitor also increases the risk of knowledge loss, as certain skills or competencies are no longer available and can only be developed again with a very considerable investment of time.

Possible solutions/countermeasures from a risk management perspective

A good practice to make visible the vulnerability of the firm due to people could be the development and use of a dashboard or risk map. A form of visualization that is available to every organization member, so that an understanding of the areas where the company is vulnerable is there. At the same time, what helps is the development of a risk aware culture, so that again everyone is aware of the firms' vulnerabilities and empowered to report any sign that could cause problems in the firm. But, ideally also with ideas how to address them or even better prevent them right from the beginning. To avoid knowledge concentration, which puts the company at risk in case of a voluntary or involuntary turnover, the owner/manager of the firm may think of actively using job rotation, so that knowledge is shared among several persons. This approach is something that should be easier in SMEs, as there are often more generalists, i.e., persons who assume different tasks and roles than specialists.

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

2 Risk exposure: Progressive digitalization

The situation

The rapid (and due to the pandemic forced) digitalization among SMEs has led to several new opportunities such as improved resource management, increased agility, and innovativeness as well as new streams of revenues. At the same time, the progressive digitalization requires the development of new business models, digital strategies, leadership, culture, and infrastructure exposing SMEs to a set of new risks as well as challenges.
The companies involved in the study that formed this guide presented many illustrative examples of the described scenario.
As regards the need for digital skills, competences, and organization the following was reported:

> *Among the hampering factors, some lack of awareness for digital risks at the top management level was revealed. After a failure in the database system in December 2020, the firm's leadership acknowledged the imperious need to buy reliable IT. The problem took two days to solve, but without an assessment of the real costs, urgency dispatched, and new servers just were acquired six months later. It is much more worrying for the decision maker if a stacker stops working. (Small firm from Portugal)*

> *A small Italian firm stressed that in this new way of working, having internal resources with adequate IT literacy was helpful, especially for having a smooth transition to the use of the new digital platforms.*

> *The company has projects that deal with very sensitive data. Customers provide historical data so the company can develop forecast models. The company has access to privileged financial data of customers or partners in consortium. However, the IT infrastructure is obsolete and prone to failures. (Small firm from Portugal)*

As regards the new challenges and thus the potential for new risks, the following examples are worth mentioning.

> *A small company from Portugal pointed out many efforts in digital integration with customers and suppliers by making use of specific portals. However, the*

increasing dependency on digital integration, when making interventions at the IT infrastructure level, have not taken in account the digital risks, namely, for customers. For example, recent replacement of servers led to IP address conflicts that did not allow customers to access the portal of the company.

While a medium-sized German company reported an awareness about cyber-risks and the existence of a modern and sophisticated fire wall. The firm's IT department and the CEO are sure that there are and have been unknown trials of attack and breaches not known in every case.

A small Austrian firm mentioned the occurrence of cybercrime, sometimes without an attack, for example a call from a pretend Microsoft employee. In addition, network problems, phishing mails and malware increase.

Possible consequences

The possible consequences of the potential mismatch between what the company should or can know for dealing with the rapidly progressing digitalization have already been made clear by the examples given above. In addition to the direct and indirect costs connected with tackling the challenges, there is also the danger that the entire company is brought to a standstill. Finally, vulnerable IT systems increase the danger of information and knowledge leakage, too.

Possible solutions / countermeasures from a risk management perspective

First, the handling of the above-mentioned issues should be understood as top priority and thus a matter for the leadership. These issues should not be delegated to the IT department or the persons in charge of IT in the firms, as these persons usually lack an understanding of business and management issues. Yet, the firm's leadership should involve these persons as well as other business functions to increase the likelihood that solutions are developed that address the challenges at hand from a broad perspective.
The challenges ahead also underline that all organization members including the leadership need to update their digital skills and competences to make better and thus more informed decisions regarding the changes that need to be initiated in the firms. The increasing availability of online courses (many of them are also free of charge) offered by reputable organizations has made skills developments easier, for smaller companies with less financial resources in particular. Again,

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

the entrepreneur / owner-manager will need to take the lead on both upskilling and reskilling.

In the run-up to the adoption of a new technology/technological solution the company will need to carefully check the compatibility of it with the extant IT system/infrastructure. In case of incompatibility, the company must find out what would be needed to make a fit. In the case of missing in-house skills, the company should turn to external sources such as chambers of commerce, universities, etc., thus, organizations supporting SMEs and also having an understanding of SME operations and business practices.

As a possible solution to address the danger of increased inefficiency and thus costs, the small firms should make sure that the technologies and software programmes (including security software) in use are continuously updated and checked for their continued relevance for the firms' business operations.

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

3 Risk exposure: “Flawed” communication

The situation

During a risk situation, the need for information, and thus communication, increases proportionally to uncertainty. Meanwhile, the ability to process information diminishes because of stress and additional business and organizational challenges. Therefore, risk communication requires special attention.

Communication has become (even) more difficult recently because despite the advantages, digital meetings have significant limitations, for example, in terms of clarity and the coherency of the information exchanged. Precisely when supplier and partner relationships demand more bonding, the boundaries between the physical and the digital world have been amplified even further by COVID-19 or have become more visible. Simply put, while somewhat productive, virtual meetings cannot substitute for physical meetings.

The companies involved in this research provided specific illustrations of communication challenges and even gaps within their supply chain. For example, a small Italian company pointed out the increased importance of effective communication during a crisis:

> *Experience and a good relationship with our historical business partners help in reducing these risks. Communication is especially crucial with business partners to be aware of potential risks and avoid them as much as possible.*

A medium-sized company from Portugal mentioned the potential risks of conducting business without face-to-face communication:

> *The biggest risk emerged at the commercial level with the reduction, or even elimination, of face-to-face interactions at business exhibitions. To get projects, it is critical is to visit potential customers and allow them to visit the company. The risk of losing business is higher now because the majority of them require the development of a trusting relationship.*

The lag between personal and digital communication was stressed by a micro company from Estonia:

Business is very personal because it involves enormous trust and trust you can only gain by personal meetings. When personal meetings are off, then you have to explain, and you have to be convincing–you have to be trustworthy. It is much harder via an online meeting.

Possible consequences

The problems in communication described above can lead to faults in operations (internal conflicts or poor workflow efficiency) as well as mistakes, delays, and, in the worst case, even a breach of trust with supply chain partners. They can also impede a company's future business because solely focussing on digital meetings for developing new ideas and concrete projects disregards that face-to-face interactions with the partners will be needed.

Possible solutions/countermeasures from a risk management perspective

A SME owner may invest in the development of a risk communication strategy as an integral part of its overall approach to risk management. This type of strategy is targeted to provide first-hand information and the grounds for carefully considered decision-making.
During a crisis, SMEs owners should take all necessary steps to reduce uncertainty in its value chain, i.e., the immediate risks and challenges should be identified, assessed and addressed. The communication should be based on facts and explanations need to be provided as early as possible to eliminate potential rumours inside as well as outside the company. Each employee understands what to do and what not to do. Communication channels and frequency of communication should be established to keep the business network (suppliers, partners, and customers) updated and involved.
All organization members should be made aware/are continuously aware of the possible additional communication challenges in an increasingly blurred world. They are also aware of the pros and cons of both digital meetings and physical meetings and based on that understanding know when to apply to what format.

4 Risk exposure: Drawbacks of using social media (also) for business purposes

The situation: Accidental information spillovers

The increasing use of social media for both business and private issues expands the danger of accidental information and knowledge leaks. People may use the same channel(s) due to convenience or time pressure instead of separate ones and thereby put the company at risk unintentionally.
A small company from Portugal provided an illustration of extensive usage of social media for work purposes.

> *Social networks are regularly used by employees: Facebook, Instagram, LinkedIn, but mainly, WhatsApp. Information exchange via social media has been a practice even before COVID-19.*

Meanwhile a small company from Austria noted the lack of data protection typical for SMEs.

> *Unwanted knowledge spillovers can happen all the time in SCs. Legal measures are difficult to enforce, especially for SMEs and in foreign countries, and it takes time to build a sufficient level of trust.*

Possible consequences

An unfamiliarity with digital culture and the basics of cyber safety among employees may lead to unintentional “sensitive” information disclosure. In addition to legal complications, the consequences include leakage of unique knowledge developed within a company (“know-how”).

Possible solutions/countermeasures from a risk management perspective

The leadership of the company should ensure that all organization members are aware of the communication channels to be used for official communication with colleagues and also external partners. Each organization member must be made aware of the possible consequences when using social media or other less

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

secure channels for work purposes. In case something happens, i.e., information or knowledge gets leaked, every organization member should understand where to turn to report this incident.

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

5 Risk exposure: Supply chain vulnerability related to distant partners

The situation:

The current crisis has demonstrated the shortcomings of value chains. High dependency on distant and very long supply chains, involving a large number of companies often spread around the world – which has put many businesses on hold because of disruptions caused by delays, etc. Consequently, existing approaches to supply chain management had to be revised to ensure the continuity of operations.

The participants in this research weathered the business demands of the ongoing external crisis, such as delivery delays, supply shortage, and production interruptions.

For example, a small company from Austria faced a shortage of supply materials and the risk of a production halt:

> *There are a lot of suppliers from abroad and slowly the supply chain is at the end. Because if you try to maintain the warehouses and you have to be able to deliver relatively quickly and in the time like now, when a part is missing, then production is at a standstill and that is of course very critical for the company.*

A micro company from Italy also experienced supply shortages:

> *A challenge is that we have fewer products available from suppliers because production was stopped for several months. In some cases, it is no longer even possible for us to pre-order the product because our suppliers do not know for how long they will have products in stock, or when they are going to receive new batches from the producer.*

A medium-sized company from Italy had an issue with production and financial liquidity due to supply delays and shortages:

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

The main vulnerability is that the origin of most of our raw materials is outside Italy. That exposes us to the risks of prices fluctuation, and as well of potential disruption in the value chain. Moreover, raw materials must show a specific quality, otherwise the quality of the final products will be influenced. Our production plant works on a continuous cycle, and a shortcoming of raw materials, or even a reduction of quantities available, increases the risk of not fulfilling the demand, or of running out of budget, for the production.

Possible consequences:

The consequences of supply chain disruption may result in delayed or partial fulfilment of obligations or a halt to production, an inability to serve the demand and in an even more extreme case to bankruptcy.

Possible solutions/countermeasures from a risk management perspective

In order to minimize the risks associated with supply chain disruption, companies should carefully evaluate current and potential suppliers in terms of reliability and long-term potential, as well as price, speed, and quality. Moreover, the substitution of distant suppliers with local ones should be evaluated as a potential strategy whenever possible. As a consequence, the current crisis demonstrates the added value of sustainable development.

The sourcing strategy should be carefully evaluated to minimize all potential risks. As a precautionary measure, it is best to adopt a dual sourcing strategy and to maintain extra stock for the most crucial parts, as possible.

The participants involved recalled the value of strong, trust-based partnerships and moved to substitute distant suppliers with local ones. For example, a medium-sized company from Germany reported:

Now we are working on risk reduction by selecting contract manufacturers aiming for long-term partnerships, strict supplier contracts. We realized that a redundancy strategy for suppliers of important products is needed, with increased sourcing from Europe (and Germany in particular). Currently, our aim is to bring back to Germany as much production as economically feasible. A micro enterprise from Estonia also characterized the benefits associated with local

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

suppliers: The advantage for the local producers is now bigger than it was before. The benefits of nearby suppliers include shorter distribution networks and the absence of language barriers and consequent miscommunication (language barriers are very big in our business because even terms which should be international are not understood in the same way in different countries). Also, it is very convenient to visit physically suppliers to show how it is done.

Summarizing recommendations

Risk management matters to all companies regardless of business cycle and size. Besides conventional business challenges, an external crisis spawns a multitude of new risks.

Below there is a checklist to provide a set of guidelines for risk management in SMEs to be better prepared for present and forthcoming risks. This can also be referenced for supply chain members.

- The company is aware of the relevance of having implemented a risk management approach/certain crucial risk management measures. Risk management is a top priority of the company and it is firmly anchored in the firm's overall business strategy.
- This risk management approach/measures does/do consider a variety of risks, i.e., financial and non-financial ones.
- The company continuously monitors current risks but also makes sure that it is aware of new risks.
- The current risks are made visible to all organization members, using dashboards or risk maps.
- The company has a good understanding of how to analyze the potential severity of the risk at hand.
- Depending on the type of risk (financial versus non-financial or internal versus external) the company has some countermeasures in place and is ready to introduce these measures to cope with the risks at hand.
- The company continuously monitors the outcomes of the measures introduced and takes countermeasures in the case the measures do not

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

perform as expected, i.e., do not meet the objectives set (e.g., reducing the danger of business disruptions due to turnover).

- The company reports the critical risks, their management and development over time and thereby learns to better cope with a multitude of different kinds of risks.
- The risk management process is laid down in the company's day-to-day business operations and every organization member is aware of his/her role in addressing present and future risks.
- The company trains its organization members regularly to be informed about the latest and newest risks that may hamper the business operations.

Please share within your network. *Link where report can be downloaded*

About the authors:

Dr. Susanne Durst, Professor of Management at the Department of Business Administration, Tallinn University of Technology, Estonia, is one of the leading subject experts regarding knowledge (risk) management, in small and medium-sized enterprises (SMEs) in particular. One focus of her current research activities is on the role of knowledge risks, such as cybersecurity risks, on organizational performance.

Lidia Davies is a PhD candidate in the Department of Business Administration at Tallinn University of Technology, Estonia. Before joining academia, she worked in international marketing research agencies, sharpening her expertise in strategic marketing and qualitative research. Her academic interests include small and medium-sized enterprises, business model adaptation and innovation, and corporate governance.

The partners would like to thank the participating companies who were willing to share their experiences on the topic and thus made a significant contribution to making this guide possible.