SMALL ENTERPRISE

PORTUGAL

The risk story 3

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

Small enterprise from Portugal

Context of the Company and the Supply Chain

With about 30 employees and almost 30 years in transport consulting, the company has three main business areas: traffic studies, planning transportation networks, and public road transports. Their work can range from planning railroads for public entities to parking lots for shopping centers.

For some of their planning, the company has access to some sensitive data provided by their clients to develop forecast models, e.g., detailed financial data of customers or detailed traffic data of certain roads.

Digitalization of SC

The company has two main systems: one for project financial management and another for project requirements management. Both systems are unique, developed explicitly for the business, and hosted on a local server.

However, both systems are heavy and archaic, presenting limitations on use, computation power, and scalability and therefore requiring some workarounds from external sources for day-to-day work, such as relying on excessive use of excel files.

The development of both systems has been halted mid-way. Migration of the data in those systems is also a problematic and expensive venture. The system's backups used to be done manually every month to hard drives but have recently switched over to a daily backup through a cloud service.

Because of the limitations of both systems, the whole interaction with the rest of the supply chain is done through other means, with the most common information sharing being through emails.

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

Risk Management

Practice of Risk Management

The confidentiality of sensitive data is currently dealt with through NDAs and multi-factor authentications. Some higher-level data is also only accessible by project managers and not disclosed to other employees. The company backs up information daily to prevent loss.

To solve their dependence on the unique systems, the company has hired external consultants to find alternatives to their current IT infrastructure problems. As a result, a large budget has been set aside for IT development in 2021. They hope to switch to new systems with the ability to deal with big data, integration with external entities, and future scalability to keep up with business requirements. Closed projects will remain in the old system and backups; only active projects will migrate to the new systems to reduce data migration costs.

Risks

With their dependence on the uniquely built systems hosted on the company's servers, the whole company's work can be jeopardized for a long time with a single system flaw. The systems themselves are prone to failures, and only one technician is available in the company.

The use of detailed, sensitive data requires special attention. Thus, cybersecurity becomes a must-have. However, with only one IT employee and some information sharing through emails, security may be severely compromised.

A failure from the two systems would represent a halt in the company's work during the failure duration. If the old servers expire, the damage would be significant. It could mean several weeks of halting the company's business, either in time spent repairing damages or lacking access to critical data.

A leak of sensitive data would also represent a severe problem. It would damage the company's reputation and go against signed NDAs, potentially resulting in repairs for contract violations or further barring the company from future work in many areas with sensitive data.

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

Cyber Risks

Dealing with sensitive data is a risk, so its exposure to the internet and employees should be as limited as possible. Keeping the sensitive data in the intranet only and restricted to access only by some people helps reduce potential leaks.

Covid-19 related risks

Since the covid19 epidemic, most employees have worked from home using their private networks to access work-related emails and systems through VPN services. This situation raises the risks of malware entering the system and further requires cybersecurity measures as more entry points to the systems also represent potentially more security breaches.

Benefits of Risk Management:

With multi-factor authentication and NDAs, the company reduces the risk of loss and leakage of sensitive information.

The future investment in new IT solutions ensures that the company can deal with more information and operations without system collapse while ensuring more scalability.

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