

# Exposure to potential top risks and mitigation

## Cyber risk

### Scenario

Worldwide the speed and variety of cyber security events and crimes continue to intensify. Therefore, Solar must increasingly focus on protecting its critical operations, intellectual property and brands from cyber threats.

### Impact

The potential impact of cyber risks is multi-faceted. Business interruptions in the shape of data breaches, intellectual property theft and regulatory consequences as well as loss of reputation are among the consequences of cyber incidents, ultimately leading to financial losses.

### Mitigation

Solar works with a governance structure and continuously strives to communicate appropriate internal information about i.e. security policies to uphold organisational awareness. Monitoring policies and procedures are in place for the main networks and systems. Furthermore, external studies are performed regularly to assess the maturity level of Solar's overall cyber and information security management and to provide recommendations. It is natural for Solar to upgrade security tools regularly in order to protect value and reduce vulnerabilities.

## General Data Protection Regulation

### Scenario

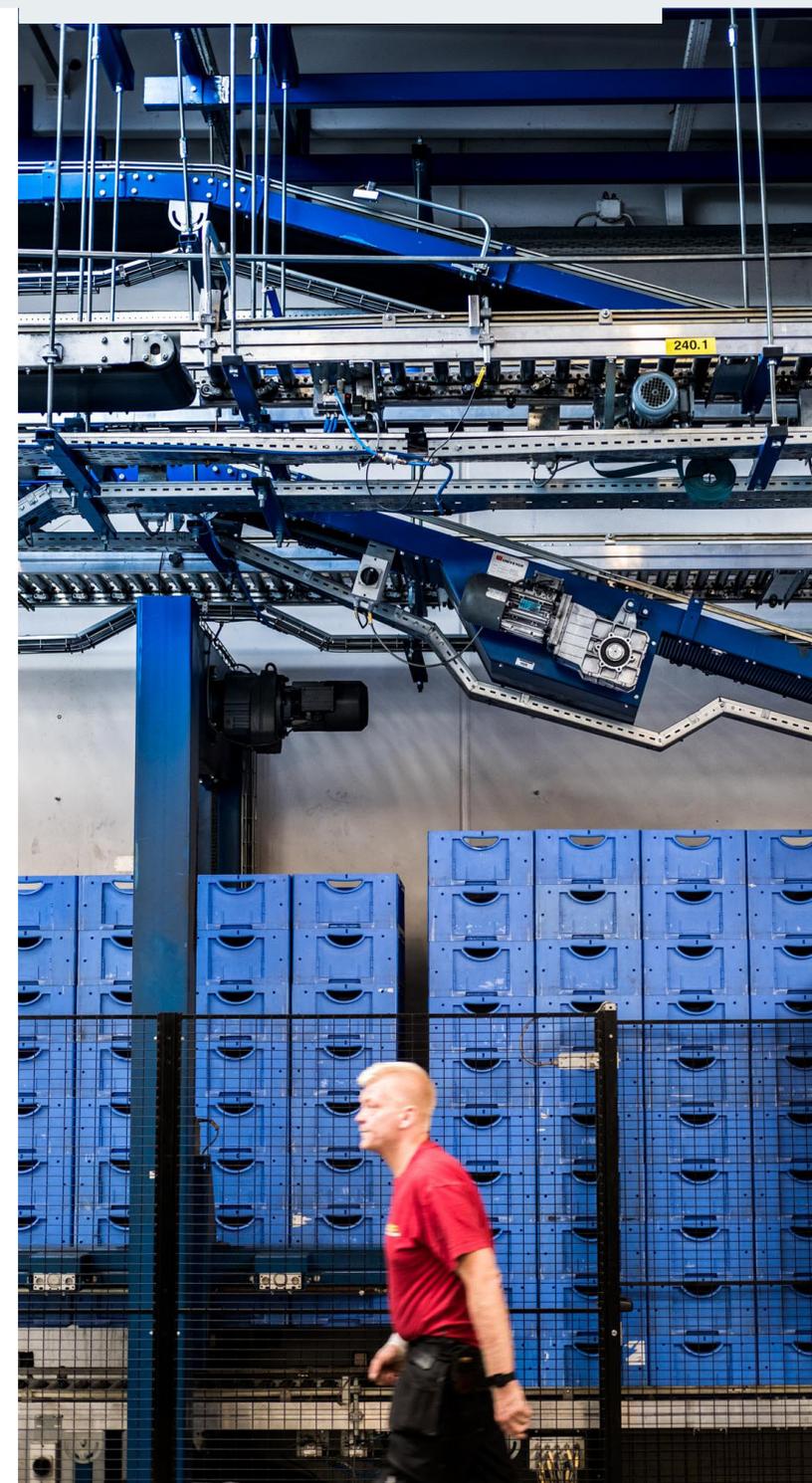
Risk of not meeting the requirements of the General Data Protection Regulation (GDPR) which is effective from May 25<sup>th</sup> 2018 in the whole European Union.

### Impact

Potential financial and reputational consequences coming from not being compliant with the new regulation.

### Mitigation

Necessary precautions have already been started and will continue in order to ensure readiness when GDPR is in place before May 25<sup>th</sup> 2018. With low risk tolerance for non-compliance Solar aims to ensure the right governance for handling this risk in order to build or maintain customers' and investors' trust in the Solar brand. Increased efforts in the communications area will be initiated to increase organisational awareness of the GDPR requirements.





## Central warehouse breakdown

### Scenario

Solar's activities are heavily dependent on a fully functioning supply chain. Consequently, Solar's business is exposed to unforeseen IT systems' disruption or events such as fire, power outages, flooding or other natural or manmade disasters.

### Impact

Unwanted events may potentially lead to partial or complete warehouse breakdown. Accordingly, materialisation of this risk can result in financial losses as well as loss of reputation.

### Mitigation

To reduce the probability of the risk materialising, Solar aims to ensure the optimal warehouse management system and its safe implementation. Apart from that, external audits are conducted regularly, while Solar Group IT monitors performance and software continuously.

Several procedures are in place in case of a potential central warehouse breakdown, including contingency plans, which are updated or developed regularly.

## IT breakdown

### Scenario

Solar's activities rely heavily on IT solutions and are thus exposed to risk of business interruptions during different initiatives, such as developments driven to improve customers' experience.

### Impact

Potential interruptions in the IT solutions area may result in financial losses and/or lead to reputational damage.

### Mitigation

Most of the IT hardware is located at two central IT data centres. To lower the probability of the risk materialising, all business-critical applications are mirrored at these data centres to safeguard IT operations, meaning that the business can continue to run even if one centre experiences downtime.

Solar's IT security board reviews IT security continuously and the IT area is constantly monitored and improved.

Project teams anchor risk management thoroughly in the project plans with mitigations comprising fallback scenarios, involvement of external experts, IT recovery plans and testing.

## Change management

### Scenario

Risk of failure to execute the sourcing and services strategy at sufficient pace as a result of inappropriate mindset and/or lack of competences. With constant focus on Solar's core business, side initiatives may not reach their optimal speed and growth.

### Impact

Currently, the assumed impact of this risk would be low revenue and profits from services sales. In the long term, this situation may challenge Solar's strategic direction and ability to run a successful business.

### Mitigation

To drive the execution of the sourcing and services strategy, a series of initiatives are executed including follow up tools, training, organisational investments and extensive communication on the advantages of the business transformation.

## Contract management

### Scenario

Risk of entering into contracts with terms and conditions (e.g. liabilities and warranties) that exceed Solar's risk appetite.

### Impact

The consequence of not complying with these contracts could be significant sanctions that are not proportional to the delivery and responsibility of Solar and exceed the commitment that the local subsidiary is willing to accept.

### Mitigation

Contracts were reviewed and standard contracts for suppliers and customers were adjusted according to the recommendations of a legal advisor. Escalation plans were also revised and clear guidelines on authority to sign contracts were prepared.

To mitigate the risk further, focus remains on strengthening contract management framework by providing standards and solutions to potential gaps as well as raising awareness within the organisation.