Being connected within Industry 4.0 – Potential for business interruption

Industry 4.0 is based on the concept of the Smart Factory; the merging of the material and virtual worlds to increase efficiency in the production process beyond anything seen before. Due to the high level of integration of stakeholders in the value chain, critical incidents such as business interruption may easily spread over the entire proposition. Similar to previous industrial revolutions, the insurance industry will play a key role in supporting the transition to this new mode of production.

Industry 4.0 with it's concept of smart manufacturing is mainly based on the Internet of Things (IoT). At the very end of the evolutionary process of Industry 4.0 any robot, tool or decision making device in the production process will communicate with everything else in that particular value chain. This process will even go beyond the Smart Factory itself and lead to fully integrated supply chains from producers to the consumer in any given industry. Interconnection of the Smart Factory and a fully integrated supply chain will add to boosting the efficiency of the production process as well as elevating product quality to unknown levels.

With the concept of the Smart Factory and it's constant application of efficiency control, quality monitoring and process excellence (enabled by supporting technology) it is commonly expected that the operating model will gain an increased independence from it's supply chain as well as flexibly adjust to any changes in said chain beyond it's own control. However, as outlined in the previous article, the benefits of the Smart Factory come with costs. Due to the high level of interconnection within the factory and beyond, the operating model's performance is increasingly exposed to external and internal incidents affecting the production process or supply chain. Malfunction of control devices, internal sabotage or consequences of data security breaches (e.g. data theft, cyber attacks, accidental data deletion) can lead to serious incidents such as business interruption. These incidents may in turn significantly affect the entire supply chain with major financial consequences for suppliers and customers.

By it's very design, the Smart Factory is exposed to increased vulnerabilities in the manufacturing process due to it's integration into an interconnected supply chain and further, connection to the internet. The more devices that are connected to the internet, the higher the possibility for data security incidents causing data theft/deletion, sabotage or even business interruption. This raises important questions about cyber security. According to a global PwC survey with 2.000 participants in 9 major industrial sectors across 26 countries, more touchpoints for data collection and exchange in the production process also increase the potential for data-security breaches. In a range of 9 concerns around data security, operational disruption (business interruption) as a consequence of data security breaches was ranked by far the number one priority of corporate data security (Global Industry 4.0 Survey, PwC (2016)).

As outlined in the previous article the risk of business interruption due to internal data security breaches or resulting from external attacks must be mitigated in the first place by implementing and enforcing a sophisticated and appropriate cyber risk governance programme throughout the organisation. This may be a significant step towards reducing potential sources that might cause business interruption resulting from data security breaches.

In history, any technological advancement is always associated with unknown risk and uncertainties. In the material world, major industrial projects could only be realised by the support of appropriate risk cover given by the global insurance industry. In the case of Industry 4.0, this is not different. The path for Industry 4.0 will therefore only be continued by innovative producers in the given supply chain if risks emerging from the convergence of the material and virtual worlds are protected by the insurance industry. To support this process and enable the achievement of the potential in Industry 4.0, insurers need to adapt to the new risk exposures and provide the manufacturing industry with adequate solutions for risks that may still prevail despite the proactive and diligent application of measures to eliminate threats.

ERGO