IBIMA Publishing
Journal of Supply Chain and Customer Relationship Management
https://ibimapublishing.com/articles/JSCCRM/2021/435883/
Vol. 2021 (2021), Article ID 435883, 17 pages, ISSN: 2326-7046
DOI: 10.5171/2021.435883

Research Article

IT security in SMEs – Threats and Chances for Supply Chains

Marcel Rolf Pfeifer

Faculty of Business and Management,
Brno University of Technology, Kolejní 2906/4, 612 00 Brno, Czech Republic,
Email: pfeifer@vutbr.cz

Received date:4 March 2021; Accepted date :5 July 2021; Published date: 29 October 2021

Academic Editor: Gabriela Prostean

Abstract

SMEs contribute to 95% of the volume in global manufacturing. While supply chains are usually dragged by the big players, SMEs have a large share in value-creation through all levels of the chains. Due to their nature, SMEs are struggling with resource constraints and the balancing of priorities. The IT security, securing some of the biggest assets of each company, data and knowledge, is assumed to not match the required level in these companies, while SMEs see themselves as being perfectly prepared. Studies show that SMEs overestimate their preparedness in the case of IT attacks; however, studies show that this field in particular is mistreated because of insufficient finances and insufficient human resource capabilities. Being connected through industry 4.0 and smart technologies, SMEs provide a backdoor for intruders to reach data and knowledge of big companies, even in case of a well-established IT security. Alarming research numbers suggest that more than 50% of companies of all sizes and branches have been fallen prey of IT attacks of any kind. Supply chains try to establish a risk management to mitigate such risks upstream to further suppliers. New technologies, such as Blockchain technology, may provide a new framework for IT security, allowing also for resilience, traceability, and anonymity. While these technologies seem promising, they do not solve the issues of the backdoor provided by SMEs in supply chains and neglected by the supply chain risk management.

Keywords: SME; Supply Chain; Security; Supply Chain Risk Management; Industry 4.0; IT security

Cite this Article as: Marcel Rolf Pfeifer (2021), " IT security in SMEs – Threats and Chances for Supply Chains" Journal of Supply Chain and Customer Relationship Management, Vol. 2021 (2021), Article ID 435883, DOI: 10.5171/2021. 435883

Introduction

Newly evolving technologies always inhibit chances and risks. While being introduced for their chances, risks have to be thoroughly controlled and managed. With the integration of suppliers and customers into supply chains, the risk of supply chains comes into focus. Supply Chain Risk Management (SCRM) should ensure the coordination of all actions of supply chain members to target these risks. It is also known that downstream enterprises try to shift their risks upstream to their suppliers in the supply chain.

While the downstream companies pull performance and quality from their suppliers and push risks towards them, these supplies have to secure the chain against these risks. Delays and disruptions, resulting from realised risks, have a direct impact on the performance and the competitiveness of the supply chain. While making use of the mixture of enterprises of various sizes and specialities providing room for complexity and differences, the SCRM has to establish activities and methods to prevent the supply chain from damages and losses. Disruptions in supply chains may bring the whole supply chain to a standstill.

SMEs are believed to be the weakest members of supply chains. While they lack the complexity and bureaucracy of Large Enterprises (LE), these companies are able to adapt faster to new circumstances by playing out their flexibility. While SMEs represent the vast majority of companies in many countries, reaching to a number above 90% in Germany, most of the research is conducted on LEs and on downstream enterprises. With the further integration of companies into supply chains, also SMEs are more and more coming into the focus of research and case studies.

SMEs are known for showing worse performances in keeping quality and process capability over time. The close cooperation with SMEs may have an impact on the vulnerability of LEs in the same supply chain (Svensson, 2000). The extent of the organizational vulnerability of a company seems to determine whether a company is able to provide a successful performance (Alexić et al., 2014). The integration of suppliers and customers into the supply chain was found to have a positive impact on the SCRM (Munir et al., 2020). Suppliers and customers, likewise, benefit from SCRM to be a part of the supply chain's strategy (Jüttner, 2005).

SMEs are known to be constrained in technical, financial, and human resources (Hannan and Freeman, 1984). Studies showed that SMEs were not able to exploit their competences while striving to exploit new opportunities (Partanen et al., 2020). Supply chains were supposed to be able to provide ambidexterity, combining the mentioned exploitation of competences and opportunities likewise (Kauppila, 2015), having a positive impact on the risk exposure of the individual members. This was believed to have a positive effect on the performance of the members and on their contribution in the supply chain.

Studies on SMEs, from the manufacturing sector, showed that this category of companies was not able to make use of ambidexterity. Moreover, these companies suffered from lower performances (Kauppila, 2015). Being known for the reluctance to introduce new technologies, timely SMEs were going with the trend or had to be forced by supply chain pressure to adapt to new requirements. The transition towards industry 4.0 and smart manufacturing knocking on the door brings challenges and risks to all enterprises at the same time. With SMEs not being able to increase performance while simultaneously exploiting changes through eliminating the related risks, SMEs have to determine their aim, either for performance or for security.

Relations of Risks, Vulnerability and Flexibility in Supply Chains

Supply Chain risks are risks that might have a direct impact on the supply chain's performance, security or members. A vast number of research papers dealt with the definitions, approaches, and strategies of risks in the past. These publications divided risks into internal and external to the supply chains. These identified risks may be divided according to four different sources: supply risk, process risk (also known as operational risk), demand risk, and control risk (also referred to as security risk) (Christopher and Peck, 2004; Manuj and Mentzer, 2008). In addition to the risk sources found, the insufficient exchange of information and requirements may add up to create further confusion and myopia within the supply chain (Christopher and Peck, 2004). While the insufficient data exchange is not a primary risk for the supply chain, it shows off in the supply risk and in the demand risk.

As an alternative example of the previous classifications of risks, they may also be divided into macroeconomic risks, policy risks, competitive risks, and resource risks (Ghoshal, 1987). This classification deals with risks arising from external factors. Furthermore, the competitive risks also compare between the external performances and the performances of the specific company. A common characteristic between all these risks is that they do not seem to be fully independent. One risk occurring might trigger another risk coming up. What these risks have in common is the impact they always have on the supply chain performance, as performances of one member spreads downstream in the supply chain. Corrective actions taken afterwards and pushed upwards try to increase the stability of the performance while decreasing the flexibility of the members. A further result of these corrective actions is the increased complexity of supply chains and the accompanying risk management (Merschmann and Thonemann, 2011). While companies try to maintain flexibility in order to be able to adapt to new situations fast (Swafford, Ghosh and Murthy, 2005), some authors argue that this flexibility is expensive, exposing the supply chain to additional risks (Pujawan, 2004). As flexibility is proposed to be the answer for uncertain concerns, members and supply chain should have a higher degree of flexibility in environments with a higher uncertainty. The choice of strategy is ought to play a major role in determining the required degree of flexibility while having a major focus on the characteristics of the product itself (Fisher, 1997).

Five case studies from China suggest that along with the supply chain risk strategy, a supply chain flexibility strategy has to be established as well (Yi, Ngai and Moon, 2011). The vulnerability and risk exposure of a supply chain depend, to a great extent, on the design and characteristics of the supply chain itself (Bode and Wagner, 2011). While the initial challenges may have changed due to globalisation and the increased speed of technological innovation (Curkovic et al., 2013), supply chain managers had to adapt to a new context (Kurniawan et al., 2017). However, the fundamental understanding and target of the SCRM remain the same.

Case studies found that the implementation of SCRM and the internal and external integration into the supply chain have positive impacts on the flexibility of the company (Chaudhuri, Boer and Taran, 2018). Hence, it can be said that the introduction of SCRM does not necessarily lead to a decrease in flexibility but rather facilitates it. Despite these findings, being known for their lower complexity and for their higher flexibility, SMEs did not implement any kind of supply chain management (SCM) in 2017 (Kumar and Singh, 2017). Trends in supply chains show the requirements for a full traceability of production and parts tending towards an even higher degree of complexity (Abeyratne and Monfared, 2016).

SMEs are known for being hesitant or even reluctant when investing in new technologies

(Quayle, 2003; Vaaland and Heide, 2007). It was found that the reason for SMEs to adapt more slowly to trends was the fact that these companies underlay constraints in technological, financial and human resources (Mittal et al., 2018). While governments have launched programmes in order to strengthen and exploit the potential of SMEs by adopting new technologies (Li, 2018), research showed that the awaited outcome did not yet occur (Camarinha-Matos, Fornasiero and Afsarmanesh, 2017). In order to get closer towards the reality of SMEs, strategies working for larger-sized enterprises have to adapt to the smaller-scale circumstances (Brozzi et al., 2018).

The hesitation of SMEs to adopt new technologies was also found in a Norwegian study. This study retrieved that, even in 2007, SMEs had issues to implement ERP systems (Vaaland and Heide, 2007). Since that time, the development brought up further technologies and trends (Hu et al., 2019) that required the usage of such resources limited for SMEs. Due to the same reason, SMEs are also limited in applying actions against risks. According to a study from India for SMEs, external risk, information technology risk, and financial risk are the most significant (Babu, Bhardwaj and Agrawal, 2020). Depending on LEs being part of the supply chain farther downstream, SMEs seem to be trapped in an agency problem. While working for the interest of the customer, the SME has to work also for its own interest (Cragg and McNamara, 2018).

In their study, Babu et al. mentioned the information technology risk. With the newly-arising concept of industry 4.0 and smart manufacturing, companies have to have a rising focus on their IT securities and risks. Bigger investments would be required in order to bring the IT infrastructure to a level mutually acceptable in the supply chain (Thakkar et al., 2012). All companies are supposed to benefit from the integration into the supply chain through exchanging information (Song et al., 2016). While the research on information security in supply chains in the light of industry 4.0 and smart manufacturing is still rare (Durowoju, Chan and Wang, 2021), intruders may already search for a way to infiltrate supply chains. Today, supply chains do not only comprise of the tangible product, but they are also resembled by a digital dataset that consists of all information and attributes on the product being called the digital twin (Chen and Paulraj, 2004). The conducted case studies suggested that the future development shall lead to a digital supply chain, resembling the real supply chain as a digital twin (Mandolla et al., 2019).

Supply Chain Risk Management

The SCRM came into focus as an independent discipline in the 2000s (Svensson, 2000; Monahan, 2003). At this time, researchers have already found that there is a fundamental difference between the approaches of SMEs and LEs (Peck et al., 2003). Moreover, SMEs seemed to be exposed to a higher risk when being part of a global supply chain (Ritchie and Brindley, 2000). The partnership with globally-acting LEs brought additional risks to the company that were beyond the capabilities of the SMEs (Jüttner and Ziegenbein, 2009). The additional risks brought to SMEs involve exchange rate risks arising from an international trading sphere, cultural specifics and habits, as well as the global transportation and logistics (Thun, Drüke and Hönig, 2011). These challenges, belonging to the fundamentals of supply chains in today’s world, were not met by SMEs (Peck, 2005).

Including further concepts into supply chains, such as lean principles, SMEs are standing in front of another hurdle to climb. Being leaner and showing a higher degree of integration make supply chains more exposed to risks (Norrmann and Jansson, 2004). Lean supply chains show a requirement to facilitate the competitiveness of the supply chain; however, it makes the supply chain more vulnerable as a whole (Thun and Hönig, 2011a). While LEs might be able to reduce the impacts of the higher vulnerability for themselves, SMEs might not be able to do so.

LEs make use of supply chains in order to transfer risks, outsource production, decrease costs, and reduce unnecessary buffers (Norrmann and Jansson, 2004). LEs become fully dependent on the supply chain through decreasing resources and thinning out the supplier base to qualified suppliers (Christopher et al., 2002). While the customers try to transfer risks upwards in the supply chain, these enterprises are still prone to these risks if the suppliers are not able to fully eliminate them (Souter, 2000). An approach proposed by Lambert and Cooper is to share not only risks, but also benefits within the supply chain (Lambert and Cooper, 2000).

While effectivity-driven technologies and principles seem to decrease the ability of supply chains to minimize the impacts of risks (Snyder et al., 2015), globalization puts companies at risks that are unfamiliar for them. Natural catastrophes in South-East Asia might affect the supplier for a component, having an impact on other members of the supply chain (Chopra and Sodhi, 2014). In order to target the risks, companies may adopt proactive or reactive strategies. In general, proactive strategies seem to be preferred in comparison with reactive ones. Reactive strategies also seemed to have damaging impacts rather than helpful ones (Baryannis et al., 2018).

Risk management in supply chains has such an important role due to research done on expected disruptions. These studies found out that even smaller disruptions of supply chains led to significant negative changes in the prospect and development of the companies in the supply chain (Hendricks and Singhal, 2003; Hendricks and Singhal, 2005; Hendricks and Singhal, 2009). The increasing complexity uncertainties, such as lead uncertainty, capacity uncertainty, and yield uncertainty, within the supply chains, (Snyder et al., 2015) call for protective measures. Research on the structure of supply chains has shown that most structures are well known, and the risks and potential impacts are also anticipated by the SCRM (Vilko, Ritala and Edelmann, 2014). Without the full knowledge of the supply chain structure, the SCRM cannot be designed effectively (Ho, 2015).

SCRM is applied in order to develop strategies in terms of risks occurring. Using a Supply Chain Risk Management Process (SCRMP) contains the phases of risk identification, measurement, assessment, evaluation, mitigation, control and monitoring (Tommala and Schoenherr, 2011). However, strategies such as risk transfer and risk sharing seem to only be appropriate for risks that combine low probability and high impacts (Lai, Debo and Sycara, 2009).

A screening of over 2000 articles showed that SMEs have an impact on the supply chain and the other members. This research found that SMEs, as supply chain partners, also increase the risk exposure for further companies (Finch, 2004). Since about 99% of all economic activities globally can be tracked back to SMEs, the impacts on SMEs most probably spread to LEs in later stages. SMEs are known to be prone to interest rate risks, raw material prices risks, E-business and technological risks, supply chain risks, growth risks, and management and employees risks (Falkner and Hiebl, 2015). Research on SMEs has additionally shown that these companies may also be considered a risk for themselves by applying lax practices on security and risk management (Sukumar, Edgar and Grant, 2011).

Research on the application of risk management and supply chain risk management practices in SMEs shows an ambiguous picture. While Brustbauer claims that many SMEs work proactively with the risks (Brustbauer, 2014), other SMEs are found to reactively deal with risks when occurring (Poba-Nzaou, Raymond and Fabi, 2014). The latter may also be a consequence of missing knowledge and expertise (Gao, Sung and Zhang, 2012) which should be handled with the facilitation and development of risk management capabilities (Falkner and Hiebl, 2015). According to Faisal et al., there is a misunderstanding of the characteristics of risk by SMEs. These companies understand risk management as a concrete plan rather than a strategy applicable for a variety of events (Faisal, Banwet and Shankar, 2006).

While integrating SCRM in SMEs has come into the focus of research in the recent years, new technologies still inhibit a further risk. This risk is rarely targeted while being known. The IT security risk in the course of industry 4.0 becomes a topic of increasing importance. With crucial data being exchanged as digital twins by companies in supply chains, data and interfaces may become targets of attacks. The investments needed to lift the sophistication of IT infrastructure to a unilaterally acceptable level are vital, but big (Thakkar et al., 2012). The information exchange and the risks inhibited with it have to be managed by a competent risk management.

It is unclear whether SMEs, being seen as weak and not able to get over bigger financial obstacles, ERP systems, and formal risk management approaches, would be able to achieve the required level of IT security. With the vast majority of companies being SMEs, data and intellectual property right security in a knowledge-based environment should be a key component of their risk management as well as of the risk management of the supply chain.

IT Risk and Security

The integration of supply chains horizontally and vertically (Czaja, 2016; Wang et al., 2016) is an ongoing trend. While being in the transition towards supply chain management 4.0 (SCM 4.0), it is expected that the trend will continue towards a further integration (Zekhnini et al., 2020). In fact, the digitalization of supply chains has been already in focus in several industries for a long time (Korpela, Hallikas and Dahlberg, 2017). The decision for the integration or outsourcing of processes and components depends on the company's individual belief. Making use of a digital twin allows for the integration of cyber-physical networks in production, logistics, and supply chains (Ivanov and Dolgui, 2020).

Cyber-physical networks resemble sensors of any kind in production that are able to track the current status of production, machines and devices, or of any part or component. As supply chains always inhibit a workflow, there are services and functions in the background that have to be covered by an efficient data exchange (Viriyasitavat, 2013; Viriyasitavat et al., 2018). Data gathered from the cyber-physical system allows for viable insights into the process and its instabilities, and brings companies one step further towards smart factories (Yao et al., 2017). SCM plays a crucial role in the development towards those factories (Abdirad and Krishnan, 2020).

Exchanging data within the company and outside the company in a digital supply chain might make companies vulnerable in several areas. While digital twins should be able to allow for real-time monitoring of any physical object (Negri, Fumagalli and Macchi, 2017), they should also be able to allow for precise predictions based on computer models fed with the most recent data available (Papadopoulos et al., 2017). Likewise, the exchange of data in the supply chain allows other members to predict the most probable future with the help of the most actual data available. According to a research from the Italian service sector conducted on more than 1000 SMEs, issues and the cost of coordination seem to account for the limited application of new technologies (Scuotto et al., 2017).

While a German research questions whether the motivation of SMEs to withhold investments into the IT security is only due to limited resources, the understanding of slow SME-investments into this area is supported (Heidt, Gerlach and Buxmann, 2019). With the application of the Internet of Things (IoT), it is possible to link all machines and devices directly to the company network, including Programmable Logic Controllers (PLC), (Hu et al., 2019). Individual characteristics and reasons seem to have a far higher impact on this decision than they were thought to have. Prominent cyber criminal attacks targeted SMEs as the weakest member of the supply chain in order to get access to LEs (Heidt, Gerlach and Buxmann, 2019).

The cooperation and knowledge exchange through supply chains is expected to to support SMEs in areas where those enterprises in areas where SMEs are lacking expertise, such as the IT security (Cragg, Mills and Suraweera, 2013). AS LEs try to shift their risks upwards in the supply chain by focusing on auditing, quality and cost, the transfer of knowledge in these areas seem to be somehow neglected. Keeping in mind the damages done by IT threats, cybersecurity is becoming the core and key element of the organizational survival (Chatterjee, 2019). By using SMEs as a backdoor to data from LEs, the risk transferred from LEs to SMEs backfires towards them.

While the majority of researchers understand SMEs as the weakest players in supply chains, not matching the requirements in IT security and not being able to cover the IT risks, an overwhelming majority of the responsible IT personnel in SMEs rate their preparedness to be above average (Benz and Chatterjee, 2020). On the other hand, half of the concerned companies were identified as being outdated in terms of cybersecurity, and seemed to lack ideas and visions on how to improve the current situation (National Center for the Middle Market, 2016).

In order to facilitate the cybersecurity in SMEs, there are several options available. These options include establishing an internal team or relying on external expertise (Benz and Chatterjee, 2020). The latter approach may lack taking the specific individual characteristics of the particular SME into account. A reason for companies' lack of experience in cybersecurity can be found in the organization of the SMEs. Risk management, including cybersecurity risks, was organized as part of the operations of the company, without receiving the top-level priority (Javaid and Iqbal, 2017). A reoccurring issue is the insufficient and incomplete mitigation of risks due to insufficient awareness among companies (Oliva, 2016).

The majority of companies, SMEs and LEs, admitted, in a survey, that they had already been subject to a cyber-attack (Heidt, Gerlach and Buxmann, 2019). Thus, the matter is not fictive; it is real and has to be solved by a risk management strategy, mostly in the cybersecurity area. SMEs, being assumed to work informally also in the risk management, should be able to succeed with a higher flexibility. Through higher flexibility, the supply chain responsiveness is increased, whereas a lower degree of uncertainty decreases it (Yi, Ngai and Moon, 2011). This suggests that a stiff SCRM design may slow down the reaction to the occurring risk.

The importance of data, information, and knowledge is known. Cyber-attacks are known publicly to have put companies, like British Airways, out of service for some time. Moreover, studies show that a large number of companies from all sizes and backgrounds have already faced such attacks. SMEs sub-suppliers, with a limit share of process and knowledge, might act as a backdoor to LEs. Knowledge as the only source of competitiveness could be at stake. Moreover, malware has the ability to damage or delete valuable data. The increasing complexity and sophistication of the attacks require an increased level of security measures and risk management (Stevens, 2019).

For supply chains and their members, the situation calls for the risk management to adapt to the new threats, either in a particular company or in a supply chain. Previous research suggests that companies are overestimating their cybersecurity abilities. Hence, companies might search for solutions that are easily adaptive, maintainable, cheap, and secure at the same time. New technologies, such as Blockchain Technologies (BCT), which are known for their success related to cryptocurrencies (Nakamoto, 2008), are suggested to boost cybersecurity for all enterprises, regardless of their industry or size.

Blockchain Security for Supply Chains

The integration of supply chains horizontally and vertically (Czaja, 2016; Wang et al., 2016) should be facilitated by new technologies following industry 4.0 and smart principles. Smart supply chains will be based on flexible structures to adapt to sudden and unpredicted changes (Ivanov et al., 2015). The impacts may involve changes in the whole supply chain or may only affect a particular enterprise (Ketchen et al., 2014). As real-time data is expected to present the key value for digital supply chains in the future (Brettel et al., 2014), its acquisition, processing, and distribution will be of a major role. The exchange of data between information systems and the supply chain members has to be designed with a focus on data security (Timm and Lorig, 2015). BCTs allow for a fast data transfer, being believed to provide secure interfaces (Zheng et al., 2020). As blockchains identify their predecessor and successor by an individual identifier in their chain codes, the blocks are linked to each other in the correct order (Ayed, 2017). These technologies are believed to be not only good enough for the organisation of cryptocurrency, but also for the organisation of electronic elections (Ayed, 2017; Noizat, 2015). While cryptocurrencies attract investors because of their untraceable anonymity, to a high extent, BCTs may also allow for the traceability of whole manufacturing data when required. A publicly-existing history is already a feature of today's cryptocurrencies, such as Bitcoin (Back et al., 2002; Reid and Harrigan, 2013).

The belief of an unharmed and fully secure technology was destroyed by Reid and Harrigan. Their research showed, in a case study, that a 51%-attack circumvents all security measures. Being in possession of 51% of the Bitcoin key was enough to seize full ownership of the cryptocurrency on stake (Reid and Harrigan, 2013). Other studies showed potentials for further manipulations, such as the adding of transactions to related accounts (Ye et al., 2018) and in the whole BCT network (Keenan, 2017). This being allowed, the blockchain will be cut, new blocks will be inserted fitting to both original sides of the cut, and the data is understood as correct in the system. This unfolds potentials for illegal activities (Lin and Liao, 2017).

There are eight different consensus algorithms known for BCTs, differing in their features and being used in different blockchains (table 1)

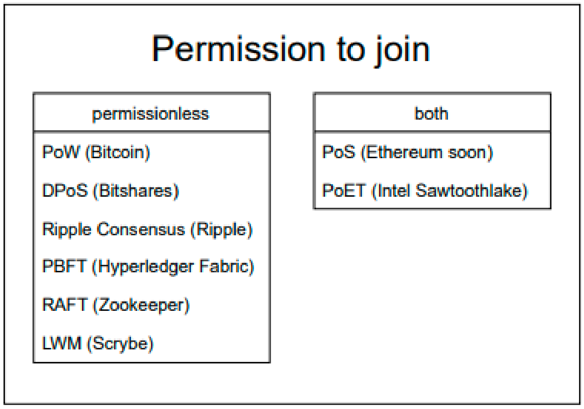

Figure 1: Blockchain consensus algorithms and blockchain technologies according to their permission to join (according to Altarawneh et al.,2021)

All mentioned BCTs are vulnerable in a different way. Recently-developed BCTs are also known as second-generation blockchains striving for the elimination of initial failures in the architecture of the technology (Worley et al., 2020). This is even more true in the case when the security is not kept up-to-date. Therefore, a BCT network by SMEs is unlikely to be secure enough for a longer time. A potential way to overcome this situation has been adopted by the German company “ascribe GmbH”, building its BCT infrastructure on the Bitcoin technology (Keenan, 2017). Using already-existing and verified BCT for a piggyback could be a strategy for enterprises that are not able to care for their IT security alone.

A recent focus of research is the application of BCT for manufacturing, logistics, and supply chain data, meeting the requirement for a reduction of processing and distribution time, as well as cost, (Jung, 2017). Case studies have proven the usefulness of BCT for manufacturing, health care and logistics (Al-Jaroodi and Mohamed, 2019; Hackius and Petersen, 2017). While these technologies allow for a wide application, inheriting the positive aspects of BCTs, they also inherit the negative aspects and weaknesses from them (Ahram et al., 2017; Petersen et al., 2016; Xu, 2016).

There is a further potential unfolded through BCT by integrating further technologies into the framework. BPIIoT is a blockchain-network that integrated IoT into its network (Bahga and Madisetti, 2016). A cornerstone of such approaches is the targeted decentralization of the network, as BCT ensures it, to cut cost in centralized data centers (Koomey et al., 2007). Beside these aspects, BCT may also be considered for organizing industrial applications data, as they inhibit a pre-defined workflow. This workflow is used today on BCT-based smart contracts, releasing a BCT payment in case of contract fulfilment (Cong and He, 2019).
With the steadily-increasing complexity of supply chains (Monfared, 2016) traceability and transparency are two important features a supply chain has to secure (Abeyratne and Monfared, 2016). Further research showed that disintegrated processes can also be linked through BCT (Álvarez-Diaz et al., 2017).

Despite these positive outsights, the threat of an attack is still apparent. Recalling the findings from previous researches, SMEs may put whole supply chains at risk, including LEs, through a failed risk management (Falkner and Hiebl, 2015). It is worth mentioning that not only SMEs fall prey of cyber-attacks, as figure 1 also shows how simple the mechanism is for a distribution of a cyber-attack.

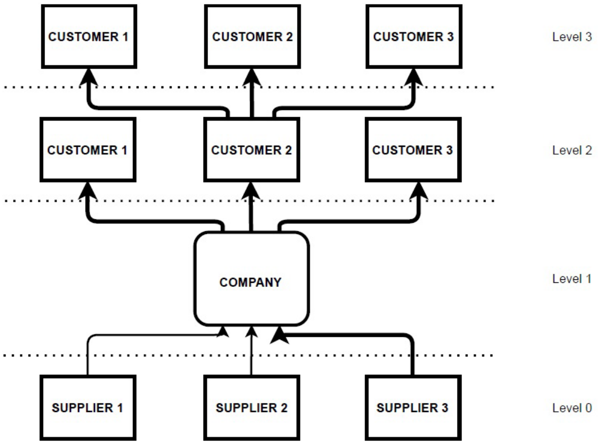

Figure 2: Corruption and attack distribution through the supply chain (own proceeding)

In order to eliminate the spreading of risks, companies have to pay attention to internal and external risks likewise (Busse et al., 2017). Being in the interest of all members of the supply chain to eliminate these risks and their spreading, companies might benefit from cooperation in the field of risk management (Fan et al., 2017). If downstream customers try to mitigate their risks just by transferring it to their suppliers, they do not get rid of these risks but they rather lose control over them. BCTs may seem as an option for enterprises of all sizes to achieve IT security. In particular, for SMEs, piggybacking on already-developed technologies boost security and may also allow for a cost-efficient way of implementing it. While it may still take some time for research, SMEs would have to see their part of the supply chain in a different light. Being hesitant to incorporate new technologies might hinder them from taking a crucial step towards secure supply chains for all members. Currently, many researchers see SMEs as a cyber-risk for themselves (Bandyopadhyay et al., 2010) and their customers (Ritter, Barrett and Wilson, 2007).

Conclusion and further outlook

Considering the findings from previous research, SMEs seem to play a crucial part in the supply chain. Lacking the maturity of LEs' risk management puts the whole supply chain with all its members at risk. Research has been conducted throughout the years on the vulnerability of supply chains and several studies suggest that SMEs show a lower risk-resilience together with a lower level of a risk management strategy. Also, widely-applied practices, like the risk-mitigation, do not limit this situation, as risks transferred upstream to suppliers may backfire in a later stage.

An area coming into focus in the most recent years is the insufficient IT security provision. While cyber-attacks have been registered publicly, studies found that more than 50% of the companies, SMEs and LEs, were already subject to such an attack. SMEs are suggested to provide the backdoor for intruders towards valuable data from LEs by circumventing their cyber-protection measures. Research suggests that the issues in SMEs are due to overestimating their cyber-protection skills and the missing availability of resources and expertise.

As the data exchange will be the core of industry 4.0 and smart manufacturing, it is of major interest of all supply chain members to protect these data. BTC as an upcoming technology has proven its applicability in cryptocurrencies. Second-generation BTCs are expected to boost the security in manufacturing, logistics, and supply chain data exchange. The security measures of these BTCs allow for a safe and cost-effective solution also for SMEs that are able to use the initial BTC mechanism for a piggyback.

Research in this area is still scarce, but a rapidly-growing number of articles show the potential of the BTC for supply chain security. SMEs and LEs can benefit likewise from these technologies in fostering data security and protecting each other. Case studies show a promising outlook for SMEs and the supply chains. However, also in BTC, there are ways to attack companies through a cyber-attack. Nevertheless, it is important to bring the IT security into the focus of SMEs.

References

- Abeyratne, S., & Monfared, R. (2016), 'Blockchain ready manufacturing supply chain using distributed ledger,' International Journal of Research in Engineering and Technology, 5(9), p.1–10.
- Aleksić, A., Stefanović, M., Tadić, D., & Arsovski, S. (2014), 'A fuzzy model for assessment of organization vulnerability,' Measurement, 51, p.214–223.
- Altarawneh, A.,Sun, F., Brooks, R. R., Hambolu, O., Yu, L. & Skjellum, A. 'Availability analysis of a permissioned blockchain with a lightweight consensus protocol,' Computers & Security, 102, p. 102098, Mar. 2021, doi: 10.1016/j.cose.2020.102098.
- Al-Jaroodi, J., & Mohamed, N. (2019), 'Industrial Applications of Blockchain,' 2019 9th Annual Computing and Communication Workshop and Conference (CCWC), IEEE.
- Ayed, A. (2017), 'A conceptual secure blockchain-based electronic voting system,' International Journal of Network Security & Its Applications, 9(3), p.01–09.
- Babu, H., Bhardwaj, P., & Agrawal, A. (2020), 'Modelling the supply chain risk variables using ISM: a case study on Indian manufacturing SMEs,' Journal of Modelling in Management, ahead-of-print(ahead-of-print).
- Back, A. (2002). 'Hashcash-a denial of service counter-measure,'
- Bahga, A., & Madisetti, V. (2016), 'Blockchain Platform for Industrial Internet of Things,' Journal of Software Engineering and Applications, 09(10), p.533–546.
- Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010), 'Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest,' Information Technology and Management, 11(1), p.7–23.
- Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2018), 'Supply chain risk management and artificial intelligence: state of the art and future research directions,' International Journal of Production Research, 57(7), p.2179–2202.
- Benz, M., & Chatterjee, D. (2020), 'Calculated risk? A cybersecurity evaluation tool for SMEs,' Business Horizons, 63(4), p.531–540.
- Bode, C., & Wagner, S. (2015), 'Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions,' Journal of Operations Management, 36(1), p.215–228.
- Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014), 'How virtualization, decentralization and

network building change the manufacturing landscape: An Industry 4.0 Perspective,' International journal of mechanical, industrial science and engineering, 8(1), p.37–44.

- Brozzi, R., D'Amico, R., Pasetti Monizza, G., Marcher, C., Riedl, M., & Matt, D. (2018), 'Design of Self-assessment Tools to Measure Industry 4.0 Readiness. A Methodological Approach for Craftsmanship SMEs,' Product Lifecycle Management to Support Industry 4.0. PLM 2018. IFIP Advances in Information and Communication Technology, vol 540, p.566–578, Chiabert P., Bouras A., Noël F., Ríos J. (eds), Springer, Cham, https://doi.org/10.1007/978-3-030-01614-2_52.
- Brustbauer, J. (2014), 'Enterprise risk management in SMEs: Towards a structural model,' International Small Business Journal: Researching Entrepreneurship, 34(1), p.70–85.
- Büchi, G., Cugno, M., & Castagnoli, R. (2020), 'Smart factory performance and Industry 4.0,' Technological Forecasting and Social Change, 150, p.119790.
- Busse, C., Schleper, M., Weilenmann, J., & Wagner, S. (2017), 'Extending the supply chain visibility boundary,' International Journal of Physical Distribution & Logistics Management, 47(1), p.18–40.
- Camarinha-Matos, L., Fornasiero, R., & Afsarmanesh, H. (2017), 'Collaborative Networks as a Core Enabler of Industry 4.0,' Collaboration in a Data-Rich World. PRO-VE 2017. IFIP Advances in Information and Communication Technology, vol 506 , p.3–17, Camarinha-Matos L., Afsarmanesh H., Fornasiero R. (eds), Springer, Cham. https://doi.org/10.1007/978-3-319-65151-4_1.
- Chatterjee, D. (2019), 'Should executives go to jail over cybersecurity breaches?,' Journal of Organizational Computing and Electronic Commerce, 29(1), p.1–3.
- Chaudhuri, A., Boer, H., & Taran, Y. (2018), 'Supply chain integration, risk management and manufacturing flexibility,' International Journal of Operations & Production Management, 38(3), p.690–712.
- Chen, I., & Paulraj, A. (2004), 'Understanding supply chain management: critical research and a theoretical framework,' International Journal of production research, 42(1), p.131–163.
- Chopra, S., & Sodhi, M. (2014), 'Reducing the risk of supply chain disruptions,' MIT Sloan management review, 55(3), p.72–80.
- Christopher, M., McKinnon, A., Sharp, J., Wilding, R., Peck, H., Chapman, P., Jüttner, U., & Bolumole, Y. (2002), 'Supply chain vulnerability,' Cranfield University, Cranfield.
- Christopher, M., & Peck, H. (2004), 'Building the Resilient Supply Chain,' The International Journal of Logistics Management, 15(2), p.1–14.
- Cong, L., & He, Z. (2019), 'Blockchain Disruption and Smart Contracts,' The Review of Financial Studies, 32(5), p.1754–1797.
- Cragg, P., Mills, A., & Suraweera, T. (2013), 'The Influence of IT Management Sophistication and IT Support on IT Success in Small and Medium-Sized Enterprises,' Journal of Small Business Management, 51(4), p.617–636.
- Cragg, T., & McNamara, T. (2018), 'An ICT-based framework to improve global supply chain integration for final assembly SMES,' Journal of Enterprise Information Management, 31(5), p.634–657.
- Curkovic, S., Scannell, T., Wagner, B., & Vitek, M. (2013), 'Supply Chain Risk Management within the Context of COSO's Enterprise Risk Management Framework,' Journal of Business Administration Research, 2(1).
- Czaja, F. (2016), 'Auswirkungen von Logistk 4.0 auf Mittelstand und

Handwerk,' Hochschule für Logistik und Wirtschaft, Hamm.

- Durowoju, O., Chan, H., & Wang, X. (2021), 'Investigation of the Effect of e-Platform Information Security Breaches: A Small and Medium Enterprise Supply Chain Perspective,' Transactions on Engineering Management, p.1–16.
- Faisal, M., Banwet, D., & Shankar, R. (2006), 'Supply chain risk mitigation: modeling the enablers,' Business Process Management Journal, 12(4), p.535–552.
- Falkner, E., & Hiebl, M. (2015), 'Risk management in SMEs: a systematic review of available evidence,' The Journal of Risk Finance, 16(2), p.122–144.
- Fan, H., Li, G., Sun, H., & Cheng, T. (2017), 'An information processing perspective on supply chain risk management: Antecedents, mechanism, and consequences,' International Journal of Production Economics, 185, p.63–75.
- Finch, P. (2004), 'Supply chain risk management,' Supply Chain Management: An International Journal, 9(2), p.183–196.
- Fisher, M. (1997), 'What is the right supply chain for your product?,' Harvard business review, 75, p.105–117.
- Gao, S., Sung, M., & Zhang, J. (2012), 'Risk management capability building in SMEs: A social capital perspective,' International Small Business Journal: Researching Entrepreneurship, 31(6), p.677–700.
- Ghoshal, S. (1987), 'Global strategy: An organizing framework,' Strategic Management Journal, 8(5), p.425–440.
- Hackius, N., & Petersen, M. (2017), 'Blockchain in logistics and supply chain: trick or treat?,' Chapters from the Proceedings of the Hamburg International Conference of Logistics (HICL).
- Heidt, M., Gerlach, J., & Buxmann, P. (2019), 'Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments,' Information Systems Frontiers, 21(6), p.1285–1305.
- Hendricks, K., & Singhal, V. (2003), 'The effect of supply chain glitches on shareholder wealth,' Journal of Operations Management, 21(5), p.501–522.
- Hendricks, K., & Singhal, V. (2005), 'Association Between Supply Chain Glitches and Operating Performance,' Management Science, 51(5), p.695–711.
- Hendricks, K., & Singhal, V. (2009), 'An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm,' Production and Operations Management, 14(1), p.35–52.
- Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015), 'Supply chain risk management: a literature review,' International Journal of Production Research, 53(16), p.5031–5069.
- Hu, J.W., Yeh, L.Y., Liao, S.W., & Yang, C.S. (2019), 'Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for Internet of Things devices,' Computers & Security, 86, p.238–252.
- Ivanov, D., Dolgui, A., Sokolov, B., Werner, F., & Ivanova, M. 2015. A dynamic model and an algorithm for short-term supply chain scheduling in the smart factory industry 4.0. International Journal of Production Research, 54(2), p.386–402.
- Ivanov, D., & Dolgui, A. (2020), 'A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0.,' Production Planning & Control, p.1–14.
- Javaid, M., & Iqbal, M. (2017), 'A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME), 2017 International Conference on Communication Technologies (ComTech). IEEE.
- Jung, J. (2017), 'Computational Collective Intelligence with Big Data: Challenges and Opportunities,' Future Generation Computer Systems, 66, p.87–88.

- Jüttner, U. (2005), 'Supply chain risk management: Understanding the business requirements from a practitioner perspective,' The international journal of logistics management.
- Jüttner U., Ziegenbein A. (2009), 'Supply Chain Risk Management for Small and Medium-Sized Businesses,' Supply Chain Risk. International Series in Operations Research & Management Science, vol 124, Zsidisin G.A., Ritchie B. (eds), Springer, Boston, MA. https://doi.org/10.1007/978-0-387-79934-6_13.
- Kauppila, O.P. (2015), 'Alliance management capability and firm performance: Using resource-based theory to look inside the process black box,' Long Range Planning, 48(3), p.151–167.
- Keenan, T. (2017), 'Alice in blockchains: surprising security pitfalls in PoW and PoS blockchain systems,' 2017 15th Annual Conference on Privacy, Security and Trust (PST), p. 400–4002, doi: 10.1109/PST.2017.00057.
- Ketchen, D., Crook, T., & Craighead, C. (2014), 'From supply chains to supply ecosystems: implications for strategic sourcing research and practice,' Journal of Business Logistics, 35(3), p.165–171.
- Koomey, J., Brill, K., Turner, P., Stanley, J., & Taylor, B. (2007), 'A simple model for determining true total cost of ownership for data centers,' Uptime Institute White Paper, Version, 2, p.2007.
- Korpela, K., Hallikas, J., & Dahlberg, T. (2017), 'Digital Supply Chain Transformation toward Blockchain Integration,' In Proceedings of the 50th Hawaii International Conference on System Sciences (2017). Hawaii International Conference on System Sciences.
- Kumar, R., & Singh, R. (2017), 'Coordination and responsiveness issues in SME supply chains: a review,' Benchmarking: An International Journal, 24(3), p.635–650.
- Kurniawan, R., Zailani, S., Iranmanesh, M., & Rajagopal, P. (2017), 'The effects of vulnerability mitigation strategies on supply chain effectiveness: risk culture as moderator,' Supply Chain Management: An International Journal, 22(1), p.1–15.
- Lai, G., Debo, L., & Sycara, K. (2009), 'Sharing inventory risk in supply chain: The implication of financial constraint,' Omega, 37(4), p.811–825.
- Lambert, D., & Cooper, M. (2000), 'Issues in Supply Chain Management,' Industrial Marketing Management, 29(1), p.65–83.
- Li, L. (2018), 'China manufacturing locus in 2025: With a comparison of Made-in-China 2025 and Industry 4.0,' Technological Forecasting and Social Change, 135, p.66–74.
- Lin, I.C., & Liao, T.C. (2017), A survey of blockchain security issues and challenges,' IJ Network Security, 19(5), p.653–659.
- Mandolla, C., Petruzzelli, A., Percoco, G., & Urbinati, A. (2019), 'Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry,' Computers in Industry, 109, p.134–152.
- Manuj, I., & Mentzer, J. (2008), 'Global supply chain risk management strategies,' International Journal of Physical Distribution & Logistics Management, 38(3), p.192–223.
- Maryam Abdirad, & Krishna Krishnan (2020), 'Industry 4.0 in Logistics and Supply Chain Management: A Systematic Literature Review,' Engineering Management Journal, p.1–15.
- Merschmann, U., & Thonemann, U. (2011), 'Supply chain flexibility, uncertainty and firm performance: An empirical analysis of German manufacturing firms,' International Journal of Production Economics, 130(1), p.43–53.

- Mittal, S., Khan, M., Romero, D., & Wuest, T. (2018), 'A critical review of smart manufacturing & Industry 4.0 maturity models: Implications for small and medium-sized enterprises (SMEs),' Journal of manufacturing systems, 49, p.194–214.
- Munir, M., Jajja, M., Chatha, K., & Farooq, S. (2020), 'Supply chain risk management and operational performance: The enabling role of supply chain integration,' International Journal of Production Economics, 227, p.107667.
- Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system,' Manubot.
- National Center for the Middle Markets (2016), 'National Center for Middle Market Study,' [Online], [Retrieved March 24, 2021], https://bitcoin.org/bitcoin.pdf.
- Negri, E., Fumagalli, L., & Macchi, M. (2017), 'A Review of the Roles of Digital Twin in CPS-based Production Systems,' Procedia Manufacturing, 11, p.939–948.
- Noizat, P. (2015), 'Blockchain electronic vote,' Handbook of Digital Currency, p.453–461.
- Norrman, A., & Jansson, U. (2004), 'Ericsson - proactive supply chain risk management approach after a serious sub-supplier accident,' International Journal of Physical Distribution & Logistics Management, 34(5), p.434–456.
- Olhager, J. (2013), 'Evolution of operations planning and control: from production to supply chains,' International Journal of Production Research, 51(23-24), p.6836–6843.
- Oliva, F. (2016), 'A maturity model for enterprise risk management,' International Journal of Production Economics, 173, p.66–79.
- Papadopoulos, T., Gunasekaran, A., Dubey, R., Altay, N., Childe, S., & Fosso-Wamba, S. (2017), 'The role of Big Data in explaining disaster resilience in supply chains for sustainability,' Journal of Cleaner Production, 142, p.1108–1118.
- Partanen, J., Kohtamäki, M., Patel, P., & Parida, V. (2020), 'Supply chain ambidexterity and manufacturing SME performance: The moderating roles of network capability and strategic information flow,' International Journal of Production Economics, 221, p.107470.
- Peck, H. (2003), 'Creating Resilient Supply Chains: A Pracitcal Guide,' Cranfield University, School of Management, Centre for Logistics and Supply Chain Management, Cranfield.
- Peck, H. (2005), 'Drivers of supply chain vulnerability: an integrated framework,' International Journal of Physical Distribution & Logistics Management, 35(4), p.210–232.
- Peck, H. (2006), 'Reconciling supply chain vulnerability, risk and supply chain management,' International Journal of Logistics Research and Applications, 9(2), p.127–142.
- Petersen, M., Hackius, N., & Kersten, W. (2016), 'Blockchains für Produktion und Logistik,' Zeitschrift für wirtschaftlichen Fabrikbetrieb, 111(10), p.626–629.
- Poba-Nzaou, P., Raymond, L., & Fabi, B. (2014), 'Risk of adopting mission-critical OSS applications: an interpretive case study,' International Journal of Operations & Production Management, 34(4), p.477–512.
- Pujawan, I. (2004), 'Assessing supply chain flexibility: a conceptual framework and case study,' International Journal of Integrated Supply Management, 1(1), p.79–97.
- Quayle, M. (2003), 'A study of supply chain management practice in UK industrial SMEs,' Supply Chain Management: An International Journal, 8(1), p.79–86.
- Reid, F., & Harrigan, M. (2013), 'An analysis of anonymity in the bitcoin system,' Security and Privacy in Social Networks, p.197–223, Altshuler Y., Elovici Y., Cremers A., Aharony N., Pentland A. (eds), Springer, New York. https://doi.org/10.1007/978-1-4614-4139-7_10
- Ritchie, B., & Brindley, C. (2000), 'Disintermediation, disintegration and

risk in the SME global supply chain,' Management Decision, 38(8), p.575–583.

- Ritter, L., Barrett, J., & Wilson, R. (2007), Securing Global Transportation Networks. A Total Security Management Approach, McGraw-Hill, New York.
- Scuotto, V., Caputo, F., Villasalero, M., & Del Giudice, M. (2017), 'A multiple buyer - supplier relationship in the context of SMEs' digital supply chain management,' Production Planning & Control, 28(16), p.1378–1388.
- Snyder, L., Atan, Z., Peng, P., Rong, Y., Schmitt, A., & Sinsoysal, B. (2015), 'OR/MS models for supply chain disruptions: a review,' IIE Transactions, 48(2), p.89–109.
- Song, H., Yu, K., Ganguly, A., & Turson, R. (2016), 'Supply chain network, information sharing and SME credit quality,' Industrial Management & Data Systems, 116(4), p.740–758.
- Souter, G. (2000), 'Risks from supply chain also demand attention,' Business Insurance, 34(20), p.26–28.
- Sreedevi, R., & Saranga, H. (2017), 'Uncertainty and supply chain risk: The moderating role of supply chain flexibility in risk mitigation,' International Journal of Production Economics, 193, p.332–342.
- Stevens, C. (2019), 'Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet,' Contemporary Security Policy, 41(1), p.129–152.
- Sukumar, A., Edgar, D., & Grant, K. (2011), 'An investigation of e-business risks in UK SMEs,' World Review of Entrepreneurship, Management and Sustainable Development, 7(4), p.380.
- Svensson, G. (2000), 'A conceptual framework for the analysis of vulnerability in supply chains,' International Journal of Physical Distribution & Logistics Management, 30(9), p.731–750.
- Swafford, P., Ghosh, S., & Murthy, N. (2005), 'The antecedents of supply chain agility of a firm: Scale development and model testing,' Journal of Operations Management, 24(2), p.170–188.
- Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017), 'Blockchain technology innovations,' In 2017 Technology & Engineering Management Conference (TEMSCON). IEEE.
- Thakkar, J., Kanda, A., & Deshmukh, S. (2012), 'Supply chain issues in Indian manufacturing SMEs: insights from six case studies,' Journal of Manufacturing Technology Management, 23(5), p.634–664.
- Thun, J.H., Drüke, M., & Hoenig, D. (2011), 'Managing uncertainty - an empirical analysis of supply chain risk management in small and medium-sized enterprises,' International Journal of Production Research, 49(18), p.5511–5525.
- Thun, J.H., & Hoenig, D. (2011), 'An empirical analysis of supply chain risk management in the German automotive industry,' International Journal of Production Economics, 131(1), p.242–249.
- Timm, I., & Lorig, F. (2015), 'Logistics 4.0-A challenge for simulation,' 2015 Winter Simulation Conference, p.3118–3119.
- Tummala, R., & Schoenherr, T. (2011), 'Assessing and managing risks using the Supply Chain Risk Management Process (SCRMP),' Supply Chain Management: An International Journal, 16(6), p.474–483.
- Vaaland, T., & Heide, M. (2007), 'Can the SME survive the supply chain challenges?,' Supply chain management: an International Journal.
- Viriyasitavat, W., (2013), 'A framework of trust in service workflows,' PhD Thesis. University of Oxford, Oxford.
- Viriyasitavat, W., Xu, L., Bi, Z., & Sapsomboon, A. (2018), 'Blockchain-based business process management (BPM) framework for service composition in industry 4.0.,' Journal of

Intelligent Manufacturing, 31(7), p.1737–1748.

- Vilko, J., Ritala, P., & Edelmann, J. (2014), 'On uncertainty in supply chain risk management,' The International Journal of Logistics Management, 25(1), p.3–19.
- Wang, S., Wan, J., Li, D., & Zhang, C. (2016), 'Implementing smart factory of industrie 4.0: an outlook,' International journal of distributed sensor networks, 12(1), p.3159805.
- Worley, C., Yu, L., Brooks, R., Oakley, J., Skjellum, A., Altarawneh, A., Medury, S., & Mukhopadhyay, U. (2020), 'Scrybe: A Second-Generation Blockchain Technology with Lightweight Mining for Secure Provenance and Related Applications,' Blockchain Cybersecurity, Trust and Privacy. Advances in Information Security, vol 79, p.51–67, Choo K.K., Dehghantanha A., Parizi R. (eds), Springer, Cham. https://doi.org/10.1007/978-3-030-3181-3_4.
- Xu, J. (2016), 'Are blockchains immune to all malicious attacks?,' Financial Innovation, 2(1).
- Yao, X., Zhou, J., Lin, Y., Li, Y., Yu, H., & Liu, Y. (2017), 'Smart manufacturing based on cyber-physical systems and beyond,' Journal of Intelligent Manufacturing, 30(8), p.2805–2817.
- Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018), 'Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting,' In 2018 5th International Conference on Dependable Systems and Their Applications (DSA). IEEE.
- Yi, C., Ngai, E., & Moon, K.L. (2011), 'Supply chain flexibility in an uncertain environment: exploratory findings from five case studies,' Supply Chain Management: An International Journal, 16(4), p.271–283.
- Zekhnini, K., Cherrafi, A., Bouhaddou, I., Benghabrit, Y., & Garza-Reyes, J. (2020), 'Supply chain management 4.0: a literature review and research framework,' Benchmarking: An International Journal, ahead-of-print(ahead-of-print).
- Zheng, T., Ardolino, M., Bacchetti, A., & Perona, M. (2020), 'The applications of Industry 4.0 technologies in manufacturing context: a systematic literature review,' International Journal of Production Research, p.1–33.