The Covid-19 Effects on the Volkswagen Supply Chain

Koen van den Broek
k.p.c.vdnbroek@tilburguniversity.edu

Floris de Beer
f.g.m.debeer@tilburguniversity.edu

Giel van Amelsvoort
g.l.p.vanamelsvoort@tilburguniversity.edu

Cedric Vanhaverbeke
c.vanhaverbeke@tilburguniversity.edu

Jelmer Nugteren
j.b.nugteren@tilburguniversity.edu

ABSTRACT

The Covid-19 virus pandemic has radically changed demand for products and services in every sector, while exposing points of weakness and fragility in global supply chains and service networks. In this research insights are gained on how the virus affected a big multinational as the Volkswagen Group. The impact on the supply chain will be studied from different dimensions. These dimensions are Business process integration, IT governance and Cybersecurity. In order to be able to make a good analysis, various online sources are used, and interviews were conducted with people who are active in the automotive sector.

Keywords

Covid-19, Volkswagen, digital transformation, supply chain, dimensions

INTRODUCTION

With the Covid-19 pandemic spreading, the effects are more and more visible every day. The consequences of the virus demand different actions from companies than in a normal situation. Especially in the field of IT, think of all the people who work from home and online orders due to closed shops. In this paper, the impact of the Covid-19 virus on the production and manufacturing industry is researched. This industry shows the effects of this occurrence in a clear way. To illuminate that further think of the example mentioned above, people working from home. You can imagine that this is impossible for factory employees. A closed factory means no production, where other companies can compensate through creative solutions.

In this research, the focus is on the German automotive market and even more specific with Volkswagen Group as a case study. Volkswagen Group has been chosen as a case study because it has 35 of its 125 plants in China (Volkswagen AG, 2020) and this is where the Covid-19 firstly has shown its effects. Also, Volkswagen Group can be considered as a market leader, considering its global market share of 12.9% in 2019 (Volkswagen AG, 2020).

This paper gives a clear view of the consequences of a turbulent change. This type of change has the characteristic that it changes faster than the response, and forces companies to change to limit the backlog. The research question of this paper is;

What is the impact of the Covid-19 virus on the supply chain of Volkswagen Group?

Scope

For this article, we used different articles, academic and nonacademic. Different dimensions were used to look at the case study. For the Business Process Integration part, a small part of the supply chain was analyzed, but with the effects for the whole in consideration. The Cybersecurity part looks at the risks and resilience for the supply chain and working from home. IT Governance, the overarching dimensions, looks at the digital transformation and the IT governance in the field of supply chain during the Covid-19 period.

RESEARCH

In this chapter, the research objectives are described. Also, the approach to fill the knowledge gap is stated.

Objective

In this research, the goal is to generate insight into the effects of the pandemic on the production and manufacturing sector. The Covid-19 pandemic is a recent and turbulent change and there is not much knowledge about the effects. It could be compared to the financial crisis in 2008. This crisis had an enormous impact on a lot of industries and also on the automotive industry, however, the Covid-19 situation is more unexpected and had a different impact.

The research question is examined from three different dimensions, namely IT governance, integration of business processes, and potential cybersecurity risks. Dependent on these dimensions, the scope was zoomed out or narrowed.

Approach

The approach to finding an answer to the research question is that firstly, extensive research on the information that is missing was done. News articles about the market and the VW Group were needed. Furthermore, academic literature was needed to support the findings to answer the research question. Based on the information on historical events and the literature, a way of using this missing information was found. From this information, a case study was conducted. As mentioned in the section above, the problem was viewed from three different dimensions. Therefore, information from these dimensions was also needed.

To find the available and relevant data different search engines were used to find sources, e.g. Google Scholar. Data about (IT related) changes in the production and manufacturing sector, with the automotive market as most favorable is meant as relevant data. Furthermore, the usability of the data was examined, reliability was checked as well as the accuracy and whether or not the papers were recently published. Accuracy here means that the paper measures what it should measure.

Also, because the scope is on the automotive market, with a case study on Volkswagen Group, interviews have been arranged with a dealer in Belgium and a supplier of the Volkswagen Group. These people were asked what they think the impact of the Covid-19 crisis was on Volkswagen's supply chain. Their answers and insights were used throughout the paper to support certain conclusions and findings.

3 PRODUCTION AND MANUFACTURING

The sector that is investigated in this research is the automotive industry. The automotive sector is one of the most important industries in many industrialized countries. With over 20.000 parts in one vehicle sourced from thousands of suppliers globally, the automotive supply chain is also among the most complex in the world (Kerna & Wolff, 2019).

The automotive industry encompasses all the companies and activities involved in the manufacture of motor vehicles, including most components, such as engines and bodies, but excluding tires, batteries, and fuel (Alan K. Binder, 2018). Because of the vast scale of the automotive industry, a case study is conducted on one of the key players in the market.

Volkswagen Group

The company selected is the Volkswagen Group. The official website of the group (2019) tells us that it is one of the leading automotive manufactures and the largest carmaker in Europe. In 2019 10,97 million vehicles were delivered to customers and the global car market share rose to 12 percent (The Volkswagen Group, 2019).

The group consists of twelve different brands, with globally 125 production plants and a total of 252.6 billion euros of revenue in 2019. The commercial vehicles business area comprises the development, production, and sales of light commercial vehicles, trucks and busses from Volkswagen, Scania, and MAN brands (The Volkswagen Group, 2019).

Volkswagen's supply chain

The supply chain of Volkswagen is a long process with a lot of different suppliers. You need more than 15,000 stations to go from raw material to a finished car. This automatically makes you highly dependent on your suppliers. A dealer in Belgium (September 2020) told in an interview that Volkswagen works with just-in-time management[1]. A delay in the supply of certain parts can therefore slow down the entire production process or even stop it yourself. The Covid-19 virus has had an enormous impact on this by requiring certain factories to close down, thereby endangering the entire process.

Volkswagen invests a lot in its supply chain. In 2019 they entered into a collaboration with Minespider to optimize the supply chains and make them more transparent (Volkswagen, 2019). With this collaboration, they hope to eliminate the sources of error and to guarantee social and ecological standards. Together with the blockchain specialist, a pilot project is to be set up to achieve transparency in the global supply chain for the lead. Blockchain technology makes it possible to trace the raw material back to the point of origin by means of digital certificates (The Volkswagen Group, 2019). This technology matches the value of Volkswagen that responsibility does not start at the production plant. (From mine to factory: Volkswagen makes supply chain transparent with blockchain, 2019)

4 ANALYSIS

[1] Just in time management is a management strategy that aligns raw-material orders from suppliers directly with production schedules. A supplied part is used immediately in the production process to avoid high inventories and related costs.

In this chapter, an analysis is accomplished with implications for the Volkswagen Group regarding the Covid-19 crisis. This analysis is divided into 3 subsections: IT governance, Business Process Integration, and Cybersecurity. Each subsection looks at how the crisis has affected the Volkswagen Group's supply chain from a different perspective.

IT Governance and Strategic Sourcing

The disruption of the supply chain of the Volkswagen Group due to Covid-19 has been considerable. Numerous suppliers were forced to shut down production (Autovista Group, 2020), leading to serious delays in the overall production (Mercure, 2020). It also led to a domino-effect, where intermediary materials needed for the next part in the supply chain could not be delivered (Miller et al, 2020). In this subsection the IT governance of the Volkswagen Group will be analyzed and if and if so, how Covid-19 affected the governance strategy.

First, the IT governance of Volkswagen is analyzed before and after the Covid-19 crisis. Subsequently, using the Governance design matrix of Weill (2004) an analysis of the five major IT decisions was conducted, providing recommendations for the Volkswagen Group.

IT Principles

Volkswagen already before Covid-19 clearly stated the importance of IT in their core business operations. IT at Volkswagen is seen as a way to further optimize business processes, including the supply chain, to lower costs, and as a way to innovate and to stay ahead of the competition. To implement this strategy Volkswagen created a central group IT division before Covid-19 led by the CIO (AMS, 2019). It was introduced to further develop and optimize their IT strategy. It consisted, among others, of implementing ERP systems to increase communication in the manufacturing process. Covid-19 did not change Volkswagen’s vision of IT entirely. Instead of that Covid-19 led to an acceleration of already initiated IT projects. For example, working from home and online meetings (Volkswagen, 2019). Furthermore, Volkswagen wants to increase communication between suppliers and provide more transparency. Good coordination between partners was crucial to the restart of operations (Automotive Logistics, 2020). However, at its core, the IT principles did not change dramatically. Weil (2004) found IT executives governing with one other group is most effective for companies that strive for balanced growth and profitability. It also enables joint decision making between IT experts and business professionals but remains focused on problems business leaders have to deal with. In this case a duopoly is the best governance structure for Volkswagen.

IT Architecture

Technical choices have not dramatically changed post-Covid-19. Before Covid-19 Volkswagen, for example, used cloud architects to bring new IT systems into the cloud. To better manage the supply chain Volkswagen also uses an industrial cloud to connect all factories worldwide (AMS, 2019). Covid-19 led to a further acceleration of this process. The industrial cloud is supposed to be further expanded for easier communication between factories. Even though Covid-19 disrupted the supply chain significantly, it does not necessarily suggest a change of archetype. In the case of Volkswagen arguably an effective IT governance strategy is the IT monarchy.

IT professionals are capable of translating the IT principles into the IT architecture and are often comfortable making decisions about IT architecture. In this case an IT monarchy could achieve business and technical standardization helping Volkswagen with optimizing their IT architecture. Weil (2004) also argues that IT monarchy is often the most effective for the IT architecture.

IT Infrastructure

The infrastructure of Volkswagen to maintain an optimal supply chain was before Covid-19 mainly based on communication and providing all suppliers with the necessary information to achieve efficiency. The image below illustrates how Volkswagen creates an ideal communication environment. During the Covid-19 Crisis Excel and Skype calls were also important for Volkswagen and its suppliers (Automotive Logistics, 2020). Furthermore, Volkswagen is now also developing new consolidation centers with new networks to increase information sharing between suppliers for more efficiency and to be more cost-effective. The most effective governance patterns often have an IT Monarchy for IT infrastructure. Volkswagen is actively trying to use even more IT systems after Covid-19 and arguably has a strong trust between its business and IT. Therefore, an IT Monarchy is in this case probably the most effective.

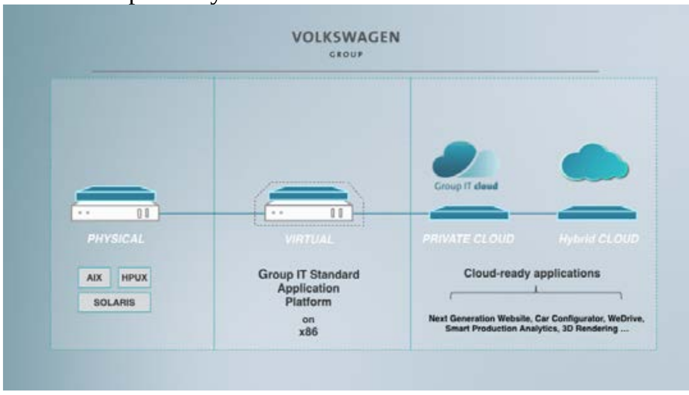

VOLKSWAGEN
GROUP
Group IT cloud
PHYSICAL
VIRTUAL
PRIVATE CLOUD
Hybrid CLOUD
AIX
HPUX
SOLARIS
Group IT Standard Application Platform
on
x86
Cloud-ready applications
Next Generation Website, Car Configurator, WeDrive, Smart Production Analytics, 3D Rendering ...

Figure 1. Volkswagen’s new Hybrid Cloud (Mirantis, 2016)

Business Application Needs

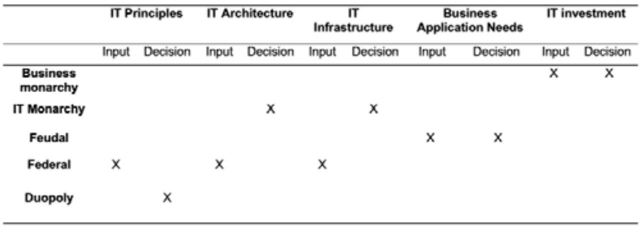
Volkswagen announced during the Covid-19 situation that it had opened a platform for its partners to make their own apps and connect with the Volkswagen plants (Volkswagen AG, 2020). The platform is developed together with Amazon Web Services and Siemens, to speed up and ease the development and integration of the platform (Volkswagen AG, 2020). The platform is based on an industrial cloud. The plants and partners will be able to determine their own business application needs and to translate their needs to an actual application. The decision to develop the platform was made by the Vice President of New Business Development from Volkswagen AG. So, that makes this a feudal archetype since this Vice President is a business unit leader. But the decision to develop an app could be made by anyone from a Volkswagen partner or by anyone from a Volkswagen plant, which makes the archetype partly anarchy. But, all things considered, the biggest decision is to develop the platform, therefore this is a feudal archetype.

IT Investment

In the investment statement for 2020 till 2024, made in 2019, Volkswagen planned to invest 27 billion euros in hybridization and digitization (Volkswagen Group News, 2019). The distribution per part is not given. The plan was discussed and approved in a supervisory board meeting. The input for the IT investments was given by the CEO, thus the board of directors. The decision to approve the plan was taken by the supervisory board. The board of directors includes a Finance and IT manager, but this manager has CFO as its official title (Executive bodies, 2020). So, there is no CIO in the board of directors. Therefore, the input is given by a Business Monarchy archetype, and the decision is also made by a Business Monarchy archetype. With the plan taken as a dominant example, we can say that the IT investments generally are taken in this form.

IT Governance Matrix

All the above described decisions lead to the following IT governance matrix from Weill (2004).



	IT Principles		IT Architecture		IT Infrastructure		Business Application Needs		IT investment	
	Input	Decision	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Business monarchy									X	X
IT Monarchy				X		X				
Feudal							X	X		
Federal	X		X		X					
Duopoly		X								

Table 1. IT Governance matrix for Volkswagen

Business Process Integration

The impact of the Covid-19 virus on the production process of a big car producer as Volkswagen is not to be underestimated. The company had to close its plants for 6 weeks in Europe and even 11 weeks in Mexico. After this period, the factories were allowed to reopen and production could start again, albeit with more limited capacity (on average about 60 to 70 percent of capacity levels prior to the Covid-19 crisis) and very strict safety measures.

The supply chain

VW Group works together with a lot of suppliers from all over the world. For the European plants of the brand alone, Volkswagen purchases about 100,000 different parts from its suppliers. A good relationship with the suppliers is very important because you are dependent on them for the production of your cars. To be able to react very quickly in case of a problem with a supplier, Volkswagen uses 'risk management'. They try to monitor all their suppliers to avoid big delays in the production when there is a problem with the supply.

Volkswagen works with just-in-time management. This means that you order different parts when you need them and helps you to avoid big stocks which can be costly. A big risk from this strategy is that suppliers aren't able to deliver on time which has a big influence on the production. Especially now that the world is hit by a pandemic that has enormous consequences for the economy and for major players such as Volkswagen. In Mexico for example, factories had to close for months due to the Covid-19 virus.

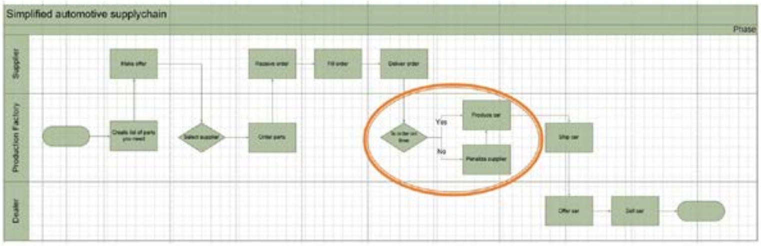


Figure 2. Activity diagram

In this activity diagram (see appendix for clearer view) the flow of activities, from selecting the right suppliers to selling a car can be seen. This is a very simple version based on data we could find online and from an interview with a local dealer. Volkswagen uses 'global sourcing' to select their suppliers to fulfill the need for different parts. They prefer dealers who are not too far from the production factories to avoid too much shipping costs. Once they have selected the right suppliers, they place an order, the supplier tries to fill this order and delivers it to the production factories. It is very important that different parts are delivered on time, so it doesn't interrupt the production process. Volkswagen is very dependent on their suppliers and if they don't deliver on time, they will penalize the supplier. Within the automotive market you could receive a customer claim of XK€ per minute depending how long the customer-line stood still. In case there is no interruption of the product-line you only have to pay a fine.

Impact Covid-19 crisis

Businesses have been undergoing an irresistible trend of globalization. As a result, supply chains have become longer and more complex. This new level of complexity has brought supply chains to an unprecedented level of vulnerability toward risks (Chen et al., 2017). This vulnerability is shown when a supply chain is disrupted. The damage from the disruption of a single process or facility may be compounded as its impact progresses through the supply chain, leading to larger scale damage to the other processes and facilities downstream (Chen et al., 2017), which was the case with VW. Plants in Spain and Mexico were shut down causing a disruption in the supply chain. This ultimately led to a stock shortage downstream of the supply chain. This case is comparable to the Toyota disruption of 2011. As a result of the tsunami and earthquake that struck Japan in 2011, Toyota's parts suppliers were unable to deliver parts at the expected volume and time. This forced Toyota to halt production for several days (Hosseini et al., 2019).

The Covid-19 virus and the closing of the factories all over the world had a serious impact. The red circle in Figure 1 shows on which part of the supply chain the impact was the greatest. From an interview with a Volkswagen supplier and a global account manager from an automotive supplier it became clear that there were many problems and these problems were mainly caused by bankruptcy of the smaller suppliers. A problem to solve this problem and to avoid stock problems at the dealers would be to speed-up the production- and transport process. But it seems that this is very hard due to the limited capacity and strong safety measurements. A local car dealer in Belgium told us that they had not enough cars in stock and that they had to delay the delivery time of the cars. This clearly shows that a supply problem can have a huge impact on the entire process.

As described above, disruptions are a difficulty for firms. Therefore, SC resilience is getting more important. Resilience is the ability to withstand a disruption (or a series of disruptions) and recover the performance (Ivanov, 2020). From the positions of resilience, a car manufacturer can establish an SC with some backup facilities, inventory buffers, flexible capacities, and a visibility control system to enable the robustness and recovery against, e.g., severe natural disasters which may temporarily, adversely affect in- and outbound material flows (Ivanov, 2020).

Another important consequence of the crisis is the rise of e-commerce. Due to the stricter measures and mandatory lock-down, many people went online looking for a new car. This is a trend that was especially noticeable in commercial vehicles. Individuals still prefer to see and test their car first in real life. The use of software such as Microsoft Teams got a huge boost and was often used for drafting and signing documents.

Cyber Security

The Virus acted as a catalysator for the digital transformation in many industries, the pandemic forced many companies to change their way of working. For many enterprises, whatever pre-Covid-19 digitalization strategy they had, it needs to be reimagined or strengthened. Covid-19 interrupted with unprecedented thread and lockdown, pushing organizations and their leaders into waters that were unfamiliar, if not totally uncharted. Sudden decisions about digital solutions were forced, to facilitate a fully remote workforce (de Jong-Elsinga & Dijk van, 2020).

The digitalization due to the pandemic brings many challenges along with it. This chapter analyses the cyber resilience of the supply chain of the Volkswagen Group. To answer this question the changes within the automotive industry are motivated and when possible, solutions are given.

Resilience

Resilience has roots in many disciplines and integrates ecological, social, psychological, organizational, and engineering perspectives and definitions. (Kott & Linkov, 2019) But in the field of cyber as well. This chapter focuses on the digital transformation within the supply chain of Volkswagen and its accompanying digital risks. Therefore, the definition that is important within the constraints of this research is cyber resilience.

Cyber resilience refers to the ability of the system to prepare, absorb, recover, and adapt to adverse effects, especially those associated with cyberattacks (Kott & Linkov, 2019).

Resilience should not be confused with risk, who are often mistakenly used interchangeably. Resilience, unlike risk, is a property of the system and includes a temporal component that risk management does not.

Risk is based on specific performance knowledge or expectation of individual system components

and is often represented by the classic risk triplet equation. When the risk is qualified it can be managed via risk governance, which includes risk management (Larkin, et al., 2015)

The automotive industry is one of the most technologically advanced industries with innovations ranging from hybrid, electric and self-driving smart cars to the Industrial Internet of Things (IIoT) integration in the form of IoT-connected cars. Before Covid-19 the automotive industry is already facing operational inefficiencies and security issues that lead to cyber-attacks, unnecessary casualties, incidents, losses, costs and inflated prices for parts and services (Fraga-Lamas & Fernandez-Carames, 2019). Examples of operational inefficiencies due to cyber-attacks are denial of service and ransomware attack.

Since 1990, a focus on managing the supply chain lies in the improvement of cost efficiency. Companies try to meet the requirements of the competition through the intensive implementation of concepts streamlining supply chains processes. This is incorporated in the automotive industry through concepts such as Just-in-time and just-in-sequence to create a lean supply chain. The trend towards lean supply chain results in low inventories achieved by close collaboration with customers and suppliers. (Thrun & Hoenig, 2011).

To achieve this collaboration in the supply chain, alignment is needed. To achieve this kind of alignment much information needs to be transferred between partners in the supply chain.

A traditional or physical supply chain (SC) is dominated by the movement of products, finance and information (Juttner, Peck, & Christopher, 2003). whereas a modern supply chain is a network of IT infrastructure and technologies that are used to connect, build and share data in virtual networks (Smith, Watson, Baker, & Pokorski Ii, 2007)

A modern supply chain has different risks in comparison with the traditional variant. The supply chain is heavily dependent on the IT infrastructure, which creates risks of disruption.

However cyber risks go beyond mere IT disruptions; they are linked to human Cyberattacks, where hackers intentionally access an organization or a network with the goal of either gaining an economic advantage or causing sabotage. These actions are typically linked to cyberbullying, cyber terrorism, or political issues (Garfinkel, 2012).

Supply chains are the backbone of evolving technological ecosystems; Industry 4.0 concepts such as the Internet of things (IoT), additive manufacturing, virtual reality, artificial intelligence, and blockchain help to reflect, expand, alter and innovate the relationships between supply chain partners. However, developments in cybersecurity responses lag these advances in the digitization of supply chains (Ghadge, Weiss, Caldwell, & Wilding, 2019). Because the digitalization is faster than the security improvement, this could lead to vulnerabilities.

However not all cybersecurity risks are related to the digitalization, the two major cybersecurity breaches can be found in the literature are:

1. A software company could be breached via malware that modifies the source code that is then distributed to the enterprises that use the software (Shackleford, 2015)

2. Theft of vendors credentials that grant remote access to an enterprise the vendors work with, leading to an infiltration of the enterprise network from an already trusted source (Shackleford, 2015).

These major cybersecurity risks can be viewed as the two general cyber risks in a supply chain. All other cyber risks that are found in a supply chain, can be nested under one of these major risks, therefore they can be viewed as categories.

The same applies to the risks that are correlated with the Covid-19 virus, these risks can be split in two effects: the direct and indirect effects of the Covid-19 virus related risks.

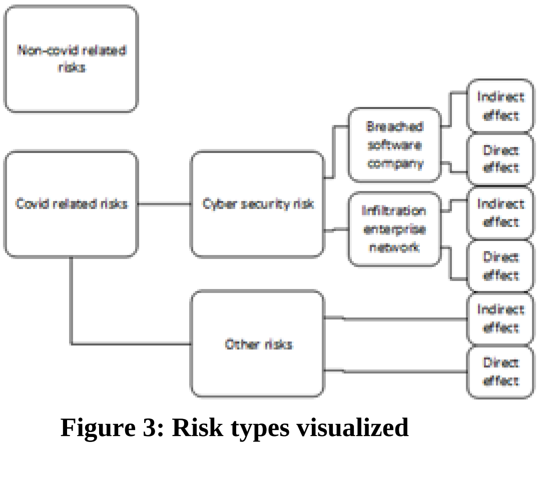


Figure 3: Risk types visualized

Covid-19 related risks are defined as all risks that are directly correlated with the Covid-19 virus and by imposing containment and suppression measures, ranging from strict controls on travel, social gatherings and commercial activities aimed at flattening the curve to less strict measures designed to shield immunologically compromised individuals, treat victims and achieve herd immunity (Guan, et al., 2020).

Performance of the supply chain

Volkswagen has started a modular organization and modular supply chain since 1996. It has not only modularized products but also the organization, by adopting a modular consortium production model. The model is characterized by the absence of a blue-collar work force and by the operations carried out by the suppliers' workforce. The factory consists out of seven subcontracting companies and has become a collection of international suppliers that share responsibility for the supply of components and the final assembly of all vehicles.

In each module, the suppliers undertake sub-assemblies of the components assigned to them and deliver the assembly of a final product. Volkswagen must independently coordinate the workflow and install the components on the chassis (Csizmazia, 2014).

By modularizing the supply chain, there is a shift from producing all the components in one place to scattering the production to many suppliers. This strategy implies that the geographical location of every supply varies, and the suppliers operate in different nations across the globe. This strategy has benefits, both on the economy side as from a risk perspective.

However, a major disadvantage was exposed when Covid-19 became a pandemic. Every country did respond differently to Covid-19, some nations choose for a more radical approach and other nations aimed at herd immunity.

A lockdown sometimes meant the complete shutdown of factories in a specific nation, combine this with the lean production strategy of Volkswagen and a future problem arises.

Not only disruptions are responsible for the production suspension, but also a drop in sales and revenue. The company is too uncertain about the fallout from the Covid-19 virus meant it was impossible to give forecasts for its performance this year (Taylor & Schwartz, 2020).

Traditional forecasting algorithms rely on relatively simplistic statistical tools to extrapolate previous demand, based on the assumption that the relationship between independent variables (such as previous sales) and dependent variables (future demand) will likely remain unchanged. Moreover, companies usually have used only internal data, perhaps in combination with past sales trends and customer signals for future orders. An external shock at COVID-19's scale cripples such a traditional demand-forecasting process (Agrawel, Eloot, & Patel, 2020).

The demand forecast given by the algorithms is no longer trustworthy without the interpretation of a team with good judgment. This could predict a future swift from relying only on forecasts given by algorithms, to a more team-based good judgment from factories and suppliers alike.

Another opportunity would be to implement an artificial intelligence and machine learning algorithm, which is not only by internal data but also by external datasets from supplier, customers and economic indicators. Incorporating these additional variables helps organizations respond to changing dynamics and external shocks more effectively (Agrawel, Eloot, & Patel, 2020).

Remote working

A major direct effect of Covid-19 was the swift remote working in almost all industries, some even dare to already call it the new normal. Many employees are forced to work remotely by regulations enforced by the government, the so-called lock-down. However, some companies, who operate under less strict regulations, still choose to enforce the remote working policy. The pandemic is likely to cause a permanent increase in remote working even after the crisis (Melian & Zebib, 2020).

Moving millions of employees, their computers and their data away from a secure office environment presents tremendous data security risks, ranging from simple technical glitches to full-scale ransomware attacks. It is a fact that cybercriminals are going to exploit Covid-19 to attack businesses and their employees. (Malecki, 2020). By moving all the employees and their computers from a protected and controlled environment and letting them operate from a remote location, increases the risk of an infiltration of an enterprise network.
The network could be infiltrated by an infected device that logs the credentials of an employee, but there is also a spike in the use of social engineering. Social engineering is defined as a method that seeks to exploit a weakness in human nature and take advantage of the naivety of the average person (Aldawood & Skinner, 2019).

There are several additional steps that a business can take to build and maintain a secure remote working environment (Melian & Zebib, 2020):

- Safeguard infrastructure
- Secure the network
- Encourage employees to engage with IT support
- Communicate safely

However it is also quite important to train and inform employees about the risks of remote working because employees play the most important role in safeguarding the interest of organizations when it comes to socially engineered attacks. With innovative and interactive education, training, and awareness programs, corporations seek to prepare their staff with the most current prevention techniques to evade social engineering threats (Aldawood & Skinner, 2019). With social engineering potential intruders can access information that they are not supposed to obtain. If a social engineer gets access to credentials, the whole enterprise network is at risk. Besides training and information sessions, the company should implement good procedures to counter these risks. Because supply chains are getting more and more intertwined, the security of the whole supply chain is as strong as its weakest link. Therefore, cybersecurity should be an integrated part of the strategy, design and operations.

A strategy adopted by many supply chains and by Volkswagen as well, is global supplier partnering. With global supplier partnering there is a shift from just purchasing to more involvement in the organization’s way of doing business, both in planning and in implementation (Palaniswami & Lingaraj, 1995).

A modern part of global supplier partnering is a vendor-managed inventory. a vendor-managed inventory is a collaborative commerce initiative where suppliers are authorized to manage the buyer’s inventory of stock-keeping units.

It integrates operations between suppliers and buyers through information sharing and business process reengineering. By using information technologies, such as Electronic Data Interchange (EDI) or Internet-based XML protocols, buyers can share sales and inventory information on a real-time basis (Yoa, Evers, & Martin, 2007).

In global supplier partnering and vendor-managed inventory, much information is shared between partners in the chain. This information is shared through many systems and protocols, much of this information is business-critical and should not be received by third parties. Before Covid-19 this risk was already existing, however, it is strengthened by the current pandemic.

The attack surface in comparison with the situation before the pandemic is enlarged. Every employee that before accessed this information from a company managed network, now must do so from a home managed network or even worse from a personal device. More (unprotected) devices that access the company systems, means a higher risk of data theft or an infection of the company network.

The attack surface is made up of all the potential access points for an attacker and cyberspace operators should actively seek to make their attack surface as small as possible to help improve cyberspace resiliency (Blowers, 2015).

This could be achieved by categorizing the data and applications, if it is too sensitive then it should only be accessed from a company managed network and device.

Another counter is adding an additional access layer to the data and applications. Not only should the device and the network be protected by authentication, the application containing the data too. By separately securing the applications, the likelihood of infiltration is lowered.

Therefore, cybersecurity should be implemented as part of the strategy of global partnering. Cybersecurity should be a standard with the partnering of the companies, meaning that all the parties can trust each other’s cybersecurity policy without constantly enforcing it.

However, the Volkswagen Group should audit the cybersecurity of the chain periodically. By auditing the chain, Volkswagen is guaranteeing that the standard of security is high. In 2019, much data was stolen from companies including Volkswagen. There was a massive breach in an IT infrastructure service provider; more than 300,000 files across 51,000 folders were stolen by hackers. They have claimed to have stolen more than 516 GB of financial and private data (Winder, 2019). It is of the utmost importance for Volkswagen to decrease the likelihood of attacks to a minimum. Volkswagen is always held accountable for breaches in its network, even if it is not processing or storing the data itself.

But not only is the likelihood of an attack lowered by Volkswagen, but the impact is also lowered. As previously described Volkswagen is operating in a modularized supply chain. The Implementation of this type of supply chain does not lower the impact of a data breach, however, when a company network is infected it is compartmentalized. A hacker can only damage everything within the compartment, instead of the whole supply chain network.

5 DISCUSSION

The digital transformation due to Covid-19 brought some considerations with it.

This research has shown that Covid-19 has a great impact on the supply chain of Volkswagen Group. The impact can be seen from the three different dimensions that were used in this research. Some aspects are important when a forced digital transformation occurs. Firstly, e-commerce becomes very important. In the interview with Volkswagen, it became clear that different software needed to be used, causing a more important role for IT. This can be linked to the IT governance, where Volkswagen handles different IT governance structures for the different IT decisions. The IT decisions need individual attention but cannot be made in isolation. This could be a focus point for Volkswagen, to align the choices more for a clear IT decision strategy.

Another digital transformation that occurred due to Covid-19, was the swift remote working. This swift mostly forced by many governments, therefore the Covid-19 virus did act like a catalysator for this trend. It could be debated that this trend was a positive change, however it also impacted the cyber security of Volkswagen. Remote working increased the attack surface of the supply chain of Volkswagen, and therefore increased the likelihood of a breach. Many mitigating actions can be given to decrease this likelihood again, moreover Volkswagen has one major advantage in the supply chain: it is modularized. The modularization of the supply chain encapsulates any breach that may occur in the supply chain of Volkswagen, and therefore decreases the impact of it.

Also, resilience is very important. A little delay in the beginning of the supply can have an enormous impact on the whole supply chain. From the interview with the Volkswagen dealer it became clear that it was thought that preparation for such an unexpected disruption is not possible. However, this can be discussed, because preparing yourself for disruptions and learning from the past can make a difference already. This is where IT and resilience play a big role.

Further, Volkswagen works with a just-in-time management. This could be beneficial in normal situations, because of the cost and inventory reduction, but in times of disruption it can be a risk. Volkswagen, in this case, and other manufacturers need to find out how to minimize the risk.

The supply chain of Volkswagen adopted a lean and just-in-time strategy to increase the efficiency and decrease the overall costs. This strategy has major benefits in comparison with storing lots of parts for a longer time, however when a disruption like a pandemic occurs this may have a negative effect. Because Volkswagens supply chain is modularized and had very little stock at hand in the supply chain, the pandemic did hit Volkswagens supply chain extra hard.

Factories across the globe were closed for a long duration, and other factories were dependent on the parts that could not be produced at that time.

6 CONSLUSION

The research question is answered from three different dimensions.

For the overarching ITG dimension, Volkswagen Group made some changes in the field of IT, but it is hard to say if the governance structure changed. The IT governance structure during the Covid-19 period was analyzed and clarified with the Governance Matrix, but the differences with the pre-Covid-19 era are tough to identify. We can say that the Covid-19 situation caused changes in the IT field. Also, it can be concluded that Volkswagen does not handle one specific IT governance structure. The structure differs per input and decision and per IT decision.

Since Volkswagen works with just-in-time management and small suppliers went bankrupt, the pandemic had enormous consequences downstream of the supply chain. Different plants were shut down causing disruptions in the supply chain. This led to a stock shortage downstream. The damage from the disruption of a single process or facility may be compounded as its impact progresses through the supply chain, leading to larger-scale damage downstream (Chen et al., 2017). Furthermore, e-commerce is on the rise; software such as Microsoft Teams got a huge boost and was often used for drafting and signing documents.

Covid-19 had many implications for the field of cyber security in the supply chain of Volkswagen. During the short period this research was conducted, it was not possible to highlight and process all the aspects of this disruption. Therefore, the cyber security analyses did study the biggest impact of a lockdown for many employers: remote working. The risk analyses that formed the basis for the research, did have to make assumptions based on results from the past and are therefore subjected to the interpretation of the researcher.

Further research could prove that this interpretation was correct, and companies could use the current analyses to predict and interpret their own risks.

7 ACKNOWLEDGEMENTS

Throughout the writing of this paper we have received great support and assistance of different

people who we would like to thank in this chapter.

Firstly, we would like to thank the supervisors for this course and especially, Francesco Lelli, Andreas Alexiou and Joris Hulstijn. The feedback sessions we had with them were very useful and they provided us with constructive and helpful feedback.

We also would like to thank the global account manager of Nedschroef. He wanted to remain anonymous. He provided us with information about the supply to car manufacturers, which gave us great insight into this process and effects of Covid-19 on the industry.

Lastly, we would like to thank the ultimately responsible of a Volkswagen dealer in Waregem, Belgium. He also wanted to remain anonymous. The insights that he gave us about supply in combination with the interview with the global account manager from Nedschroef gave us a clear image of the processes.

8 REFERENCES

Agrawel, M., Eloot, K., & Patel, A. (2020, July 29). *Industry 4.0: Reimagining manufacturing operations after COVID-19.* Retrieved Oktober 07, 2020, from www.mckinsey.com: https://www.mckinsey.com/business-functions/operations/our-insights/industry-40-reimagining-manufacturing-operations-after-covid-19

Alan K. Binder, J. B. (2018, August 2). *Automotive industry*. Retrieved September 17, 2020, from Encyclopædia Britannica: https://www.britannica.com/technology/automotive-industry

Aldawood, H., & Skinner, G. (2019, March). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, 11(3). doi:https://doi.org/10.3390/fi11030073

AMS. (2019, November 18). *A program of change for Volkswagen Group IT. Automotive Manufacturing Solutions*. https://www.automotivemanufacturingsolutions.com/industry-40/a-program-of-change-for-volkswagen-group-it/39635.article

AMS. (2019a, October 18). *Building Volkswagen's Industrial Cloud. Automotive Manufacturing Solutions*. https://www.automotivemanufacturingsolutions.com/systems/building-volkswagens-industrial-cloud/39633.article

Armano, D. (2020, September 9). '*COVID-19 Will Be Remembered As The 'Great Accelerator' Of Digital Transformation*'. Retrieved October 7th from https://www.forbes.com/sites/davidarmano/2020/09/09/covid-19-will-be-remembered-as-the-great-accelerator-of-digital-transformation/#1aaef1983cb2

Automotive Logistics. (2020, July 27). *Better communication remains key for VW Group's global logistics post-Covid*. https://www.automotivelogistics.media/coronavirus/better-communication-remains-key-for-vw-groups-global-logistics-post-covid/40914.article

Autovista Group (2020, March 18) '*Carmakers take action as coronavirus spreads in Europe*'. Retrieved on October 7th 2020 via https://autovistagroup.com/news-and-insights/carmakers-take-action-coronavirus-spreads-europe

Blowers, M. (2015). *Evolution of Cyber Technologies and Operations to 2035* (Vol. 63). Springer. doi:10.1007/978-3-319-23585-1

Chen, X., Xi, Z., & Jing, P. (2017). *A unified framework for evaluating supply chain reliability and resilience. IEEE Transactions on Reliability*, 66(4), 1144–1156. https://doi.org/10.1109/TR.2017.2737822

Christopher, M., & Holweg, M. (2011). *"Supply Chain 2.0": Managing supply chains in the era of turbulence Build-to-order View project Direct digital* *manufacturing-driven transformations of supply chain management View project.* Article in International Journal of Physical Distribution & Logistics Management. https://doi.org/10.1108/09600031111101439

Csizmazia, R. (2014, December 01). Reconfiguration of Supply Chain at Volkswagen Group to Develop Global. *International Journal of Academic Research in Business and Social Sciences, 4*. doi:10.6007/IJARBSS/v4-i12/1363

Csizmazia, R. A. (2014). *Reconfiguration of Supply Chain at Volkswagen Group to Develop Global*. International Journal of Academic Research in Business and Social Sciences, 4(12), 2222–6990. https://doi.org/10.6007/IJARBSS/v4-i12/1363

de Jong-Elsinga, D., & Dijk van, A. (2020). *Digital transformation after COVID-19*. Retrieved September 26, 2020, from Deloitte: https://www2.deloitte.com/nl/nl/pages/enterprise-technology-and-performance/articles/digital-transformation-after-covid-19-acceleration-with-control.html

DW (2020) *Volkswagen, Audi ordered to keep Mexican factories shut*. Retrieved September 24th from https://www.dw.com/en/volkswagen-audi-ordered-to-keep-mexican-factories-shut/a-53794742

Fraga-Lamas, P., & Fernandez-Carames, T. M. (2019). *A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry*. IEEE Access, 7, 17578-17598. doi:10.1109/ACCESS.2019.2895302

From mine to factory: Volkswagen makes supply chain transparent with blockchain. (2019, April 04). Retrieved September 17, 2020, from volkswagen-newsroom: https://www.volkswagen-newsroom.com/en/press-releases/from-mine-to-factory-volkswagen-makes-supply-chain-transparent-with-blockchain-4883

Garfinkel, S. L. (2012). *The cybersecurity risks. Communications of the ACM, 55*(6), 29-32. doi:10.1145/2184319.2184330

Ghadge, A., Weiss, M., Caldwell, N., & Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. *Supply chain management, 25*(2), 223-240. doi:https://doi.org/10.1108/SCM-10-2018-0357

Guan, D., Wang, D., Hallegatte, S., Davis, S., Huo, J., Huo, J., . . . Gong, P. (2020). Global supply-chain effects of COVID-19 control measures. *Nature Human Behaviour, 4*, 577-587. doi:https://doi.org/10.1038/s41562-020-0896-8

Hosseini, S., Ivanov, D., & Dolgui, A. (2019). Review of quantitative methods for supply chain resilience analysis. *Transportation Research Part E: Logistics and Transportation Review, 125, 285–307.* https://doi.org/10.1016/j.tre.2019.03.001

Ivanov, D. (2020). *Viable supply chain model: integrating agility, resilience and sustainability perspectives—lessons from and thinking beyond the COVID-19 pandemic.* Annals of Operations Research. https://doi.org/10.1007/s10479-020-03640-6

Juttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: outlining an agenda for future reserach. *International journal of logistics research and applications, 6*(4), 197-210.

Kerna, J., & Wolff, P. (2019). *The digital transformation of the automotive supply chain - an empirical analysis with evidence from*

Germany and China: case study contribution to the OECD TIP digital and open innovation project. 23. https://www.innovationpolicyplatform.org/system/files/imce/AutomotiveSupplyChain_GermanyChina_TIPDigitalCaseStudy2019_1.pdf

Kott, A., & Linkov, I. (2019). *Cyber Resilience of Systems and Networks.* doi:10.1007/978-3-319-77492-3

Larkin, S., Fox-Lent, C., Eisenberg, D. A., Trump, B. D., Wallace, S., Chadderton, C., & Linkov, I. (2015). Benchmarking agency and organizational practices in resilience decision making. *Environment Systems and Decisions, 35*, 185–195. doi:https://doi.org/10.1007/s10669-015-9554-5

Malecki, F. (2020, July). Overcoming the security risks of remote working. *Computer Fraud & Security*(7), 10-12. doi:https://doi.org/10.1016/S1361-3723(20)30074-9

Megahed, N. A., & Ghoneim, E. M. (2020, October). Antivirus-built environment: Lessons learned from Covid-19 pandemic. *Sustainable Cities and Society, 61*. doi:https://doi.org/10.1016/j.scs.2020.102350

Melian, V., & Zebib, A. (2020). *How Covid-19 contributes to a long-term boost in remote working*. Retrieved Oktober 06, 2020, from https://www2.deloitte.com/: https://www2.deloitte.com/ch/en/pages/human-capital/articles/how-covid-19-contributes-to-a-long-term-boost-in-remote-working.html

Mercure, M. (2020, April 21) ‘*Next Round of Volkswagen Settlement Delayed Due to COVID-19’*. Retrieved on October 7th 2020 via https://ngtnews.com/next-round-of-volkswagen-settlement-delayed-due-to-covid-19

Miller J., Arnold M. & Johnson M. (2020, February 26) ‘*European companies face coronavirus hit to supply chains.*’ Retrieved on October 7th 2020 via https://www.ft.com/content/67e2d35c-589b-11ea-a528-dd0f971febbc

Newsroom.vw (2020) *#TBT - The rich history of Volkswagen's Puebla plant*. Retrieved September 24th from http://newsroom.vw.com/vehicles/tbt-the-rich-history-of-volkswagens-puebla-plant/#:~:text=As%20one%20of%20the%20largest,is%20located%20in%20Puebla%2C%20Mexico.&text=This%20factory%20exclusively%20produced%20the,more%20than%201.7%20million%20units

NSF (2020, May) ‘*Business Adaptations and Resilience in the time of Covid-19*’. Retrieved on October 7th 2020 via https://www.nsf.org/knowledge-library/business-adaptations-and-resilience-in-the-time-of-covid-19

Palaniswami, S., & Lingaraj, B. (1995, June). Procurement and vendor management in the global environment. *Internation journal of production economics, 35*(1-3), 171-176. doi:https://doi.org/10.1016/0925-5273(94)90078-7

Pandey, S., Kumar Singh, R., Gunasekaran, A., & Kaushik, A. (2020, Januari 13). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*. doi:10.1108/JGOSS-05-2019-0042

Scholten, K., & Schilder, S. (2015). The role of collaboration in supply chain resilience. *Supply Chain Management, 20(4), 471–484.* https://doi.org/10.1108/SCM-11-2014-0386

Shackleford, D. (2015). *Combatting Cyber Risks in the Supply Chain.*

Sans.org. September.

Smith, G., Watson, K., Baker, W., & Pokorski Ii, J. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. *International journal of production research, 45*(11), 2595-2613.

Stechkin, I. (2016, April 26). *Volkswagen: Self-driving cars and the reinvention of IT infrastructure. Mirantis | Pure Play Open Cloud*. https://www.mirantis.com/blog/volkswagen-self-driving-cars-and-the-reinvention-of-it-infrastructure/

Taylor, E., & Schwartz, J. (2020, March 17). *Volkswagen suspends production as coronavirus hits sales*. Retrieved Oktober 07, 2020, from Reuters.com: https://www.reuters.com/article/us-volkswagen-results-2019-idUSKBN2140OF

Thrun, J.-H., & hoenig, D. (2011, May). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics, 131*(1), 242-249. doi:https://doi.org/10.1016/j.ijpe.2009.10.010

Udlap (2012) *Volkswagen Group*. Retrieved September 24th from http://catarina.udlap.mx/u_dl_a/tales/documentos/lni/cedillo_l_e/capitulo2.pdf

Volkswagen (2020). *Supply Chain*. Retrieved September 25th from https://www.volkswagenag.com/en/sustainability/environment/supply-chain.html

Volkswagen AG (2020, July 27th) *Volkswagen brings additional partners to Industrial Cloud*. Retrieved September 28th from https://www.volkswagenag.com/en/news/2020/07/Industrial_Cloud.html

Volkswagen AG (2020) *All Volkswagen plants back to production with effect from today*. Retrieved September 24th from https://www.volkswagenag.com/en/news/2020/06/all-volkswagen-plants-back-to-production-with-effect-from-today.html

Volkswagen AG (2020) *Executive Bodies*. Retrieved September 28th from https://www.volkswagenag.com/en/group/executive-bodies.html

Volkswagen Group News (2019, April 23). *From mine to factory: Volkswagen makes supply chain transparent with blockchain*. Retrieved September 25th from https://www.volkswagen-newsroom.com/en/press-releases/from-mine-to-factory-volkswagen-makes-supply-chain-transparent-with-blockchain-4883

Volkswagen Group News (2019, November 15th) *Volkswagen investing strongly in the future*. Retrieved September 28th from https://www.volkswagen-newsroom.com/en/press-releases/volkswagen-investing-strongly-in-the-future-5576.

Volkswagen. (2020, March 17). *Volkswagen brand suspends production on Thursday due to corona crisis*. https://www.volkswagenag.com/en/news/2020/03/Corona-Krise.html

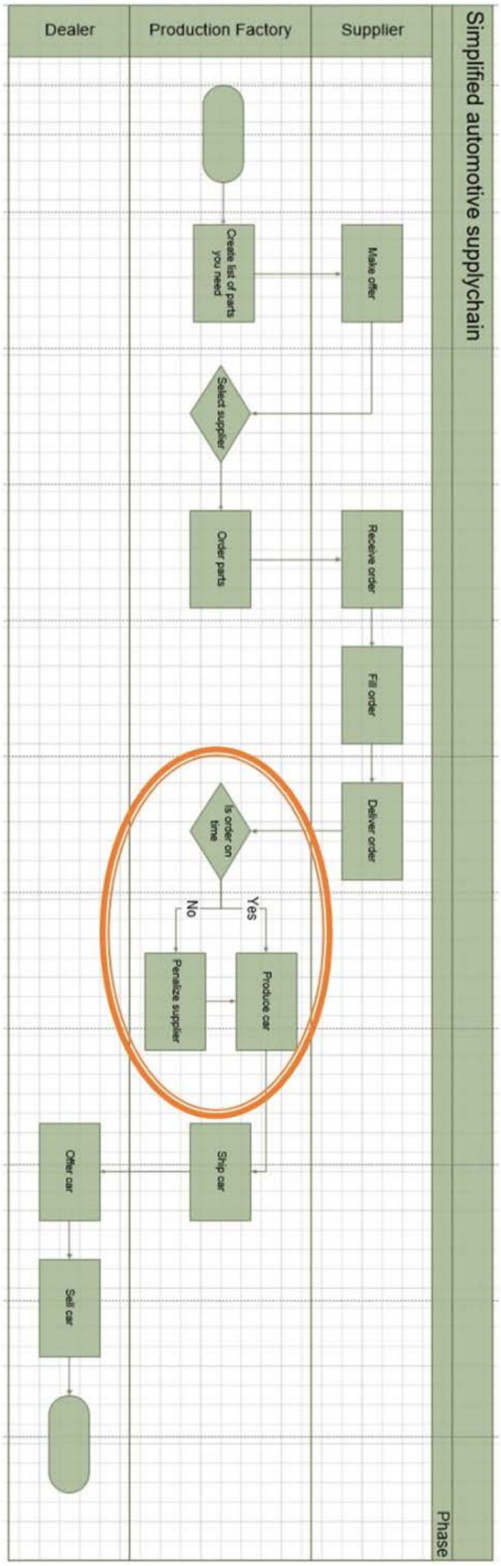
Volkwagen AG (2020) *Portrait & production plants*. Retrieved from https://www.volkswagenag.com/en/group/portrait-and-production-plants.html on september 9th 2020.

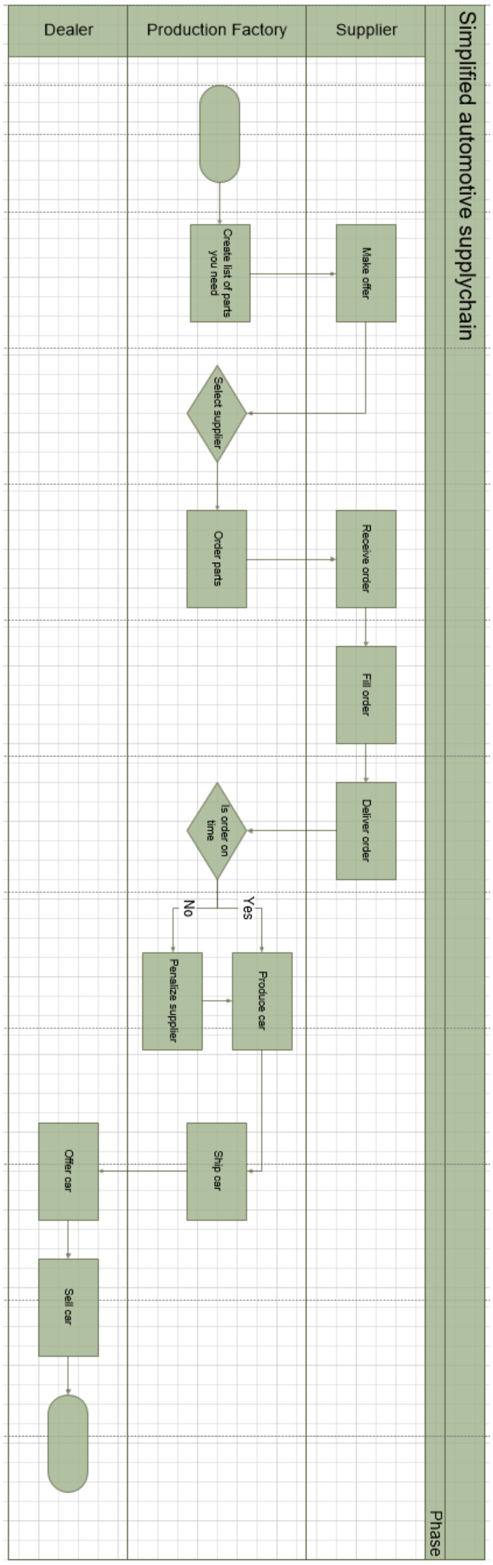
Winder, D. (2019, May 4). *Airbus, Porsche, Toshiba And Volkswagen Data Stolen In Massive Breach -- What You Need To Know*. Retrieved Oktober 10, 2020, from https://www.forbes.com/: https://www.forbes.com/sites/daveywinder/2019/05/04/airbus-porsche-toshiba-and-volkswagen-data-stolen-in-massive-breach-what-you-need-to-know/#378319e4701c

Yoa, Y., Evers, T., & Martin, D. E. (2007). Supply chain integration in vendor-managed inventory. *Decision Support Systems, 42*(2), 663-674. doi:https://doi.org/10.1016/j.dss.2005.05.021

9 APPENDICES

Appendix A



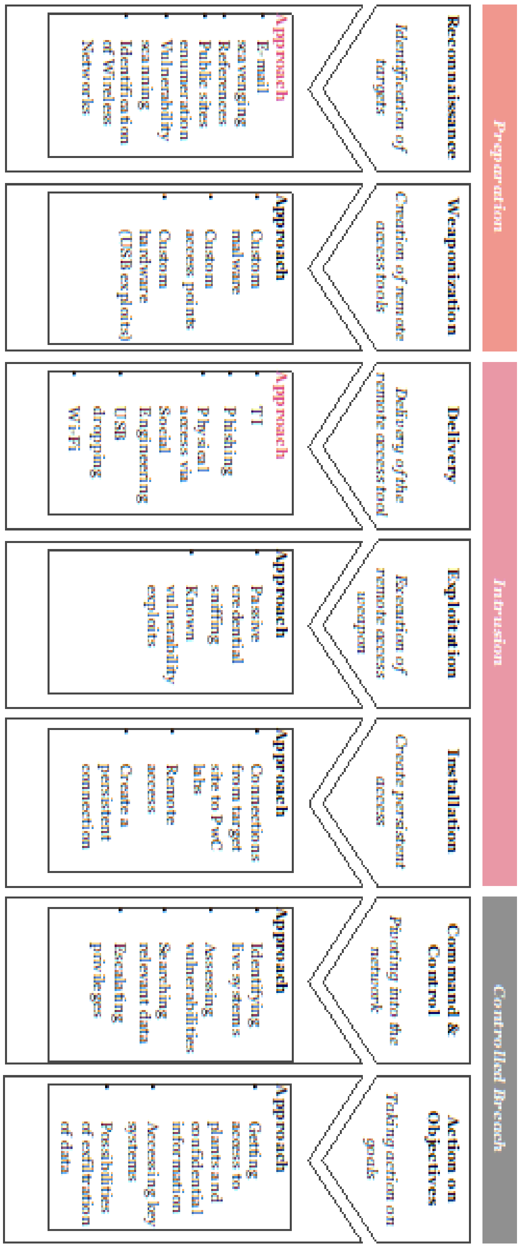


Appendix B

Risk analyses Volkswagen case

Context

The context of this risk analyses is described in the research paper, the general subject of the research is the impact of Covid-19 on the supply chain of Volkswagen Group. The risk analysis tries to answer which cyber risks are enlarged and how they are affected. The framework of the cyber kill chain describes the different stages a cyber-attack goes through and can be used to identify the different risks Volkswagen is facing.



Risk identification

Reconnaissance

The first step in the cyber kill chain is identification of the targets and the probing for weaknesses.

Weaponization

The second step is weaponization, in this face the found vulnerabilities are translated into a deliverable payload using for example a backdoor or exploit.

Delivery

The third step is sending the created weapons to the victim.

Exploitation

The fourth step is the execution of the weapon.

Installation

The fifth step is installing the malware on the target system and therefore establishing persistent access.

Command and control

In the sixed step a channel is created where the attacker can remotely access the system.

Action on objectives

The attacker acts on the intended goals.

Risk analysis

Phishing attacks

Phishing has become a significant threat to Internet users. Phishing attacks typically use legitimate looking but fake emails and websites to deceive users into disclosing personal or financial information to the attacker. Users can also be tricked into downloading and installing hostile software, which searches the user's computer or monitors online activities to steal private information (Wu, Miller, & Garfinkel, 2006).

The personal information obtained by the attacker can be used to obtain access to the network. The attacker is then able to access private documents of the company. The attacker is then able to leak those documents to the public or anyone willing to read. This could potentially be business critical information or personal data of employees.

The credentials obtained could also be used to directly harm the company by interfering in the operational processes. A company potentially could be losing much money in lost revenues due to a successful phishing attack, set aside the legal costs afterwards.

Because of the range possibility the attacker has when it has obtained the credentials, the impact is High. However, the likelihood of actually succeeding in passing the spam filter and obtaining the credentials is low.

Employee device

The employee device could also be used to illegitimately enter the enterprise network. For example, Ransomware could be used to keep the laptop hostage. Ransomware is described by Malwarebytes as is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access (Ransomware, 2020). If the laptop of an employee is infected with ransomware, the laptop is been taken hostage by the software. the employee would not be able to perform the tasks at hand, before the ransom is paid. Because this only affects the efficiency of the employee, the impact is low. Also, the risks of actually getting infected by a ransomware virus is low, the virus must pass through different layers of security before it reaches the employee's laptop.

The laptop itself can also be hacked by utilizing a backdoor or exploit to gain access and for example install a keylogger. If the hacker has access to the laptop of an employee, it has a very brough amount of possibilities to harm to company just like a phishing attack. A Difference with the phishing attack is the scope of the attack, it is directly aimed at a device. Therefore, the impact is high, and the likelihood is medium.

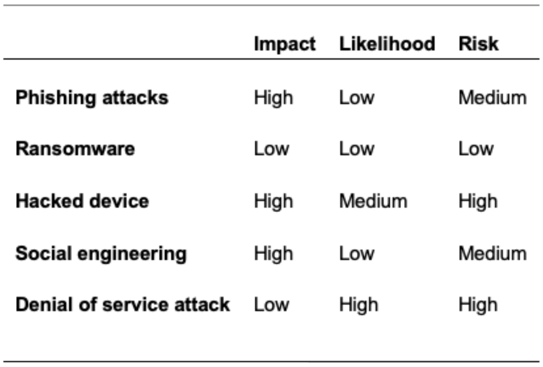
Social engineering

Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion (Krombholz, Hobel, & Huber, 2015). Social engineering aims at the weakest link in the security chain, the employees itself. If the attacker does gather enough information in the reconnaissance part, social engineering can be quite successful. Because of the wide amount of possibilities, the attacker has after the attack, the impact is high. The likelihood of an attack is low, lots of preparations have to be done before a social engineering attack can be carried out.

Denial of service attacks

Flooding-based distributed denial-of-service (DDoS) attack presents a very serious threat to the stability of the Internet. In a typical DDoS attack, a large number of compromised hosts are amassed to send useless packets to jam a victim, or its Internet connection, or both (Chang, 2002). This attack could disrupt the information flow within the company or supply chain. This kind of attack is quite easy to carry out in comparison with the other attacks; therefore, the likelihood is high.

The company network could be completely taken down by attackers, however this is not likely. The attack could disrupt the efficiency of a department; therefore, the impact is low.



	Impact	Likelihood	Risk
Phishing attacks	High	Low	Medium
Ransomware	Low	Low	Low
Hacked device	High	Medium	High
Social engineering	High	Low	Medium
Denial of service attack	Low	High	High

Table 2. Pre-Covid-19 risks

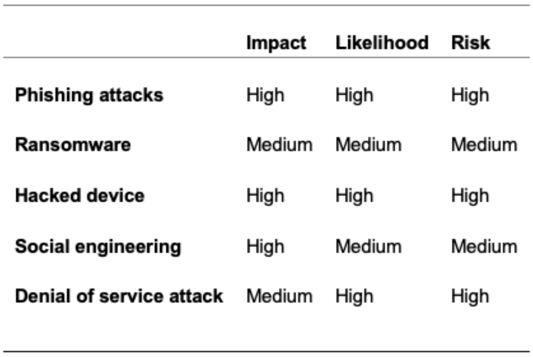
Risk evaluation

Covid-19 did have some influence on the risks stated before in this risk analyses. Due to Covid-19 many employees did have to start working remotely instead of on premise. This swift in way of working, enlarged the attack surface of the company by increasing the amount of access point to attack. Instead of attacking the enterprise network, every single laptop became an access point to the enterprise network. These swift increases the likelihood of an attack to be successfully carried out for phishing attacks, ransomware and hacked devices. In the cyber kill chain this would ease the intrusion state.

The ransomware attack is only influenced on its likelihood, but also the impact. Because the employee is not working in the office but remotely, he or she is dependent on the computer. Therefore, the impact of a ransomware attack is higher, the employee cannot work when the computer is taken hostage. The impact of the denial of service attacks is also increased due to corona.

Employees who are not working at the office, do not have direct contact with their colleagues. This makes it more difficult to ask for advice of help, they must make decisions on their own. This increases the likelihood of a successful social engineering and phishing attack. Employees cannot easily ask their collogues or IT department for help, and therefore are more easily tricked. This has effects on the state reconnaissance in the cyber kill chain, the attack can more easily gather information about the company and its employees.

Finally, the impact and the likelihood of a denial of service attack is increased. The likelihood of succeeding is increased because the attack surface is bigger. Moreover, are the home networks of employees less secure against this type of attack, then of a company. The impact of this type is bigger because employees rely on the information to conduct their work. When the services are unavailable, an employee cannot conduct its work anymore.



	Impact	Likelihood	Risk
Phishing attacks	High	High	High
Ransomware	Medium	Medium	Medium
Hacked device	High	High	High
Social engineering	High	Medium	Medium
Denial of service attack	Medium	High	High

Table 3. Unmitigated risks during Covid-19

Risk mitigation

Covid-19 has impacted the supply chain in many ways, increased the likelihood and impact. Volkswagen can implement different measures to mitigate the risks to an acceptable level and meet their risk appetite.

It is not possible to decrease the amount of access points when employees are still working remotely, however the likelihood of succeeding can be mitigated. The increased amount of access points eases the intrusion state of a cyber-attack. To mitigate this risk not only the computer and network should be secured, but he applications as well. In this case the attack would successfully intrude the device of an employee, however he or she cannot enter the enterprise applications even if there is an active connection with the enterprise network. For example, a second username and password pair are needed to view and/or alter the data within the enterprise's applications.

The risks of ransomware, phishing and social engineers can be mitigated by training and informing employees. They should be trained on recognizing phishing emails and know the correct procedures when receiving one. Also, the procedures and training around social engineering are important, employees should never share information with anybody who is not properly authenticated.

The likelihood of a denial of service attack cannot be lowed, however the impact can. Redundant servers should be operational to directly take over a service when it goes down. In this way the efficiency loss of a denial of service attack is lowered, however when an employee is directly targeted, they IT department should have a proper procedure to act.