COVID-19 in the Insurance Industry: Can IT/IS Management Incorporate Black-Swan Events?

Roza Amin
a.amin@tilburguniversity.edu

Tim van der Berg
t.p.a.vdnberg@tilburguniversity.edu

Hugo Biolchini
h.p.p.biolchini@tilburguniversity.edu

Georgette Doekes
g.c.c.doekes@tilburguniversity.edu

Des Spreeuwenberg
d.l.l.a.spreeuwenberg@tilburguniversity.edu

ABSTRACT

In this paper we describe the effects of COVID-19 on the Dutch insurance industry. More specifically insurance companies need to re-assess their prediction models as well as their digital transformation efforts. The question how insurance companies can best leverage IT to manage the uncertainty associated with the COVID-19 pandemic will be the central topic of this paper. What are the main tasks for the IT/IS management layer to tackle the challenges posed by COVID-19, who is responsible for the execution of these tasks and who is held accountable are questions that will be addressed in this paper. Our research consisted of a literature review where we relied heavily on reports by industry experts such as Deloiette and EY to provide data as the event covered in this paper is recent and ongoing which limits the academic literature that is presently available. We consider several scenarios that describe how insurance companies can react to COVID-19. We offer recommendations that are intended to increase organizational resilience in the case of a black-swan event occurring. For example, insurance companies need to implement continuous assessment of their digital operations in order to remain sensitive to emerging threats and opportunities. It should be noted that the research scope of this paper was limited, more research is necessary, especially research utilizing primary data. Nonetheless we hope this paper can help the insurance industry to develop a way forward by utilizing digital transformation which will help insurance companies thrive in a post COVID-19 world.

Keywords

COVID-19, insurance, digital transformation, business process integration, IT governance, cybersecurity.

INTRODUCTION

COVID-19 has had an impact on businesses in every sector. For the insurance sector this means that it can expect to see a dramatic increase in claims, be it health insurance, life insurance or non-life insurance related. The insurance industry needs to determine what strategies and technologies exist that can assist them dealing with the consequences of the pandemic. (KPMG: Insurers COVID-19 covered, 2020).

COVID-19 caught the world off-guard however it was not the first black-swan event to hit the industry. Another event similar in term of its global impact was the 2008 financial crisis.

During the financial crisis, banking and insurance businesses suffered greatly (Schich, 2009). The severity of the situation was part of the reason that the 2008 crisis led to the re-design of payment systems and processes and set the stage for disruptive industry forces such as fintech companies. Now, 12 years later COVID-19 will likely lead to another redesign within the insurance industry. This redesign will force insurance to shift even further from physical to digital channels and products by using end-to-end automation and AI optimization of business processes (KPMG: Fast track to technology,2020).

It is therefore crucial that research is done on how the insurance sector can take these disruptions and trends towards further digital transformation of their sector into account and ensure they are well equipped to deal with their future business environment.

By doing a critical review of the available secondary literature, we will assess if and how insurance companies should reevaluate their priorities when it comes to digital transformation initiatives. Moreover, we will incorporate lessons learned from the fields of IT governance, strategic

Sourcing, business process integration as well as cyber security and risk management. We will integrate these research subsections and provide recommendations for insurance companies to implement.

RESEARCH OBJECTIVE

Insurance companies use statistical models to calculate and put a price on uncertainty. Despite these advanced models it can been concluded from the literature that insurance companies are still unable to achieve levels of preparedness necessary to deal with low likelihood, high impact events, such as 9/11, hurricane Katrina or Covid-19 (*15 years after Katrina: Would we be prepared today?*, 2020). Of course, no one can exactly predict when these types of events will occur but it is certain that they will, and therefore contingency planning is possible. Events relating to terrorism, environmental hazards and societal unrest can have major economical and societal effects such as the loss of jobs and loss of money, for example, 40 billion USD had to be paid by insurers after 9/11, but the effects can also be organizational in nature as was the case with AIG, the insurance company thath AIG was one of the beneficiaries of the 2008 bailout of institutions that were deemed "too big to fail", AIG received 150 billion USD as part of a bailout package. (Makinen, 2002).

The key objective of this research is to develop an information management framework that can be used to mitigate the problems that arise when a insurance company is confronted with a black-swan event such as the COVID-19 pandemic. The research question is as follows:

How can IT/IS management assist the Dutch insurance industry in the managing of the effects of an unforeseen disruptive external event such as the COVID-19 pandemic?

RESEARCH APPROACH

The approach of the research will be theoretical. Papers and articles from other researchers and consultancy firms will be used to determine pre- and post-COVID-19 situations within the insurance industry. This will be analyzed and compared. During the analysis, the aim is to find out what aspects of the insurance industry are vulnerable to black swan events such as COVID-19. Secondly, a theoretical study will help to establish a vision for improving the decision making process of insurance firms being confronted by black swan events.

We will approach our research from 3 different perspectives, namely: IT Governance and Strategic Sourcing, Business Process Integration and Cybersecurity Risk Management.

The field of IT Governance will provide the tools needed to assess to what extent the management model and decision areas ought to change in order to align more with the digital transformation trends and ambitions of the industry as well as with the COVID-19 induced 'new-normal'.

Looking at the effects COVID-19 had on the insurance industry through the lens of business process integration will help us obtain insight into the business processes commonly used within this industry, and compare what has changed or what is likely to change through necessity or choice in post-COVID-19 world.

The cybersecurity and risk management perspective will enable us to identify the risks that are inherent within the digital transformation process currently underway in the insurance industry, we will also identify possible control measures to mitigate these risks.

In the next section, a brief overview of the insurance industry will be given. Followed by a description of the Dutch insurance industry which will be further examined in the following sections.

THE INSURANCE INDUSTRY

COVID-19 and the Insurance Sector

With the rapid spread of COVID-19 worldwide, one of the most pressing challenges facing the insurance business is how to achieve a large-scale transition to remote work (KPMG: Fast track to technology, 2020).

According to Deloitte (Deloitte Global, 2020), the insurance industry is generally well prepared for major damages, including pandemics, but the financial impact will take time and will depend on the company specifically. The potential long-term impact of COVID-19 on insurance companies may be:

- Interest rates may put pressure on the balance sheets of insurance companies and the profitability of life insurance products (Deloitte, 2020). According to the 'European Insurance and Occupational Pensions authority (2020)', with the current uncertainties (duration of lockdown and economic recovery), interest rates will remain low, this will lead to more uncertainty and insurers will be less inclined to take risks.
- Delay in reporting insurance claims to insurers, their assessment and payment. (Deloitte, 2020) According to Bryan Cave Leighton Paisner (2020), the Insurance Act states that the insurer must pay the amounts owed on the claim within

a reasonable time. Insurance companies can be taken to court if they do not pay on time and can be held liable for damages that occur while the claim has not been paid.

- An insurance company with a higher level of risk diversification will be best protected against losses resulting from COVID-19 it will also have lower economic and capital needs and can therefore offer lower prices to customers. By offering lower prices, new clients will be more likely to use its insurance services (OECD, 2020).

The Dutch Insurance Sector

Within the Dutch insurance sector, data analysis will be a strong driver for growth in 2020 and allow for increased automation of business processes such claim handling. This will enable insurance companies to focus manpower on customer interaction and satisfaction(Accenture (2020).

Within the Dutch insurance Industry there are several key players, the top four in terms of market share prior to the COVID-19 pandemic were Achmea, VGZ, CZ and Menzis(Vektis, 2019).

Before the COVID-19 pandemic, the premium paid by customers showed a slow but steady rise over the previous five years(Vektis, 2019). For the 2021 premium, it will be interesting to see the effects of the COVID-19 pandemic on the height of the premium.

Insurance Against Black-Swan Events

A black swan event is an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences (Nafday, 2009). The COVID-19 pandemic has affected all lives of all people to various degrees. It has shown that black-swan events make everything we undertake more uncertain, be it the conducting of business, work, travel, etc.

Due to this increase in uncertainty caused by a black-swan event, insurance companies could benefit from an increase in demand for insurance against future black-swan events, whether this is a feasible market opportunity will depend greatly on the risk appetite of individual insurers as well as their liquidity which might be under some stress because of an increase in COVID-19 related policy pay outs to customers.

ANALYSIS

IT Governance and Strategic Sourcing

The goal of this section is to compare and contrast the core IT governance aspects as well as the common practices followed by the insurance industry before and after the COVID-19 pandemic. The effects and implications of the pandemic are not fully understood yet, some reliance on assumptions will therefore be unavoidable, especially for the description and analysis of the post-COVID-19 situation.

Most if not all insurance companies operating in the Netherlands were already well on their way to becoming de facto digital entities(Boston Consulting Group, 2015). The reasons for this was that the insurance industry recognized early on the potential digital technologies held and how these technologies could help create value and increase competitiveness (Eling & Lehmann, 2017).

However, insurers did not view themselves as digital firms yet, this despite being confronted by a variety of disruptive forces ranging from changing customer needs and expectations to insurtech start-ups(Deloitte, 2017). Before COVID-19 traditional insurance firms viewed themselves fundamentally different from insurtech firms.(McKinsey, 2017).

Table 1 provides an overview of the IT Governance structure of a generalized insurance firm operating in the Netherlands, before and during the start of the COVID-19 pandemic (Deloitte Global, 2020).

Generally speaking, insurance firms face two major challenges due to the pandemic. The first being a potential liquidity crisis due to COVID-19 related payouts to customers, the second being an increased demand for digital services on the business side. The dilemma faced by the average insurance firm is therefore: do they invest in IT or do they postpone IT-investments and create a financial buffer to mitigate the risks associated with a liquidity crisis (Hay, 2020; Chakrabarty, 2020; Bainbridge, 2020; "General Insurance Article - Increased demand for private medical insurance after COVID19," 2020)

In case of a liquidity crisis, all focus will likely be on keeping the company from bankruptcy. In this scenario, the firm's IT leadership should play less of a role in the decision making process. The business leadership is assumed to be best equipped to deal with liquidity issues and will decide on priorities and funding. Consequently, the business monarchy governance archetype is likely to be the best option here. An additional advantage of the Business Monarchy is that it is cost-efficient, as little coordination is needed. However, solely for Business Application Needs a federal archetype is

assumed, due to the fact that local business units and senior management together are responsible for addressing the business application needs.

In case of the second scenario, insurance companies have to potentially divert resources in the business towards customer-oriented services. Therefore, it is suggested that the business leadership gets relieved and only decides on the IT-principles and IT-investment, the reason for this being that the company financials need to be kept in check especially during times of crisis. All remaining responsibilities, as they relate to IT, are placed on the IT department.

When an insurance company does not foresee any liquidity issues and trusts its ability to adequately respond to the COVID-19 pandemic, it should then possibly leverage its relative strong starting position to further increase its competitive advantage. In terms of IT governance, this means that the business strategy and IT strategy will be used as input for the IT principles section of the governance matrix and that the IT leadership will be able to decide on IT architecture and IT infrastructure strategies.

The addressing of business application needs will be the responsibility of local business units and business process owners which together with senior management and where needed, senior IT management will be held responsible and accountable for addressing the business application needs of the organization. Finally, decisions regarding IT investments should be in the hands of the IT leadership, in this way the traditional focus areas of the business-side leadership will not act as a barrier to IT-innovation.

Our last scenario, where the insurance company does not foresee any issues and can properly respond to COVID-19 pandemic, is the scenario which we will assume for the rest of our analysis.

Table 1. Pre- COVID-19

IT Activities (Input/Decision)	*IT Principles*		*IT Architecture*		*IT Infrastructure Strategies*		*Business Application Needs*		*IT Investment*	
Archetype	*I*	*D*	*I*	*D*	*I*	*D*	*I*	*D*	*I*	*D*
Business Monarchy	x	x					x	x		x
IT Monarchy			x	x		x			x	
Feudal					x					
Federal										
IT Duopoly										
Anarchy										

Note: I = Input; D = Decision

Table 2. Post-COVID-19: Scenario 1 Liquidity Crisis

IT Activities (Input/Decision)	*IT Principles*		*IT Architecture*		*IT Infrastructure Strategies*		*Business Application Needs*		*IT Investment*	
Archetype	*I*	*D*	*I*	*D*	*I*	*D*	*I*	*D*	*I*	*D*
Business Monarchy	x	x	x	x	x	x			x	x
IT Monarchy										
Feudal										
Federal							x	x		
IT Duopoly										
Anarchy										

Note: I = Input; D = Decision

Table 3. Post-COVID-19 Scenario 2 Customer-Oriented Services

IT Activities (Input/Decision)	*IT Principles*		*IT Architecture*		*IT Infrastructure Strategies*		*Business Application Needs*		*IT Investment*	
Archetype	*I*	*D*	*I*	*D*	*I*	*D*	*I*	*D*	*I*	*D*
Business Monarchy	x	x							x	x
IT Monarchy			x	x	x	x	x	x		
Feudal										
Federal										
IT Duopoly										
Anarchy										

Note: I = Input; D = Decision

Table 4. Post-COVID-19 Extend Competitive Power

IT Activities (Input/Decision)	*IT Principles*		*IT Architecture*		*IT Infrastructure Strategies*		*Business Application Needs*		*IT Investment*	
Archetype	*I*	*D*	*I*	*D*	*I*	*D*	*I*	*D*	*I*	*D*
Business Monarchy									x	x
IT Monarchy			x	x	x	x				
Feudal										
Federal							x	x		
IT Duopoly	x	x								
Anarchy										

Note: I = Input; D = Decision

Business Process Integration

In this section, we will adopt a business process integration perspective to analyze the implications of COVID-19 on the Dutch insurance sector.

Regulations implemented by the Dutch government to contain the spread of the virus has put a considerable strain on the livelihood of various types of businesses. For insurers, the chances of paying out policies have increased due to business closures, firings as well as physical and psychological health issues related to COVID-19 (Kocianski, 2020).The opportunities provided by the COVID-19 pandemic are also numerous, and mainly come in the form of the demand from potential clients to insure themselves against not only COVID-19, but also against its unforeseen consequences.

Both opportunities and threats are likely to lead to changes in the internal processes of a typical insurance firm. Most changes will be related to a greater focus on IT capabilities that enable smooth business operations, while the majority of people work from home as well as a satisfactory digital customer experience.

Remoteness both for the employees and well as the customers will determine the change in processes necessary for the insurance firm to thrive in the 'new normal'.

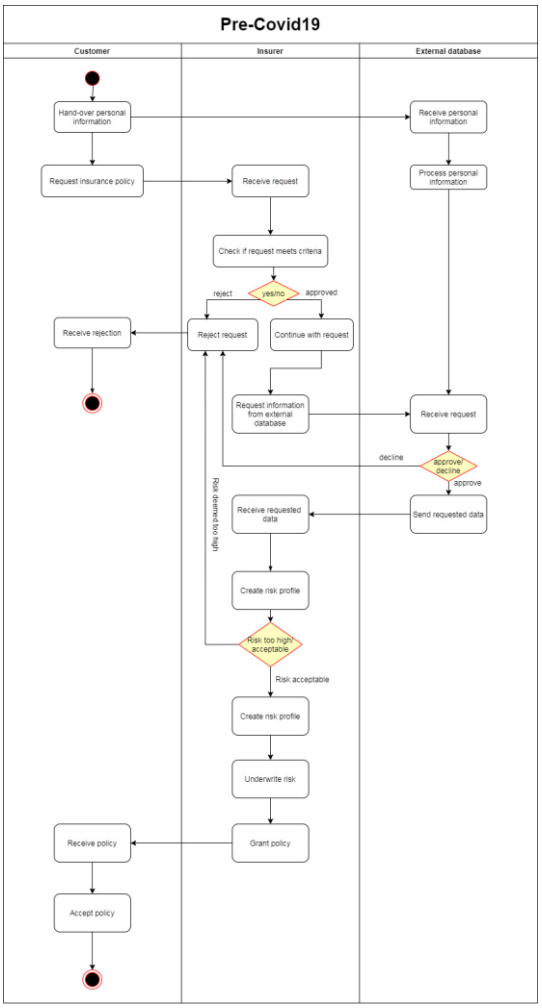

Figure 1. Pre-COVID-19 activity diagram

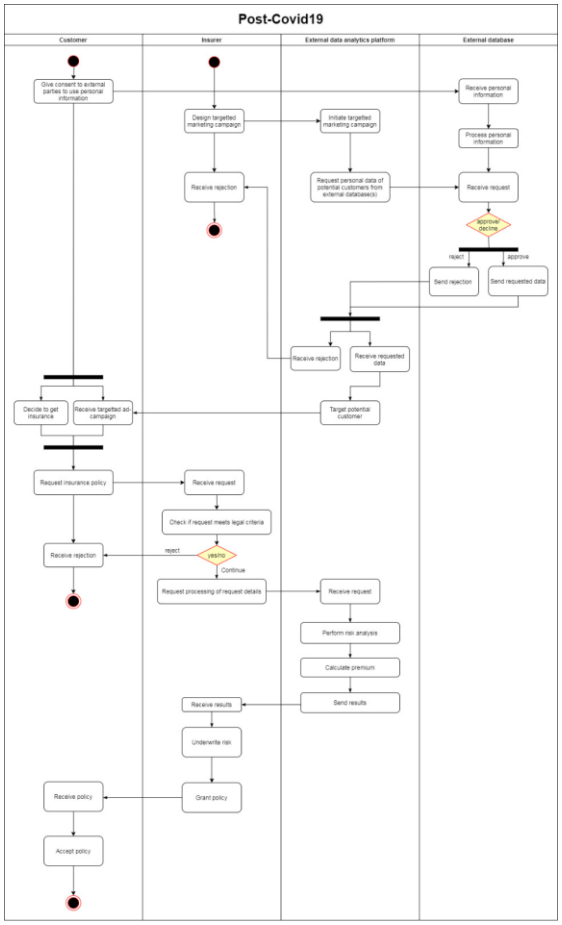

Figure 2. Post- COVID-19 activity diagram

To illustrate the differences between a traditional insurer and a more digitized one we use activity diagrams,

The two activity diagrams of figure 3 and figure 4 represent the flow from one insurance activity to another. An activity here can be described as an operation performed by an actor belonging to a particular system. In this case, the system consists of a customer, an insurer, an external database and an external analytics platform.

When comparing the two activity diagrams, it becomes clear that the main difference can be found in the reliance of the insurer on outsourced IT capabilities such as analytics and use of external databases, while most insurers were already doing this pre-COVID19, this diagram aims to illustrate the trends influencing the core differences between activities of a pre-COVID19 traditional insurer and a post-COVID19 digitized insurer.

Changes due to New Technologies

The pandemic has led to the acceleration of insurance business innovation and the shift from physical to digital channels and products, with end-to-end automation and optimization of processes (KPMG: Fast track to technology, 2020).

Pre-COVID, the insurance application process used by insurance companies was still heavily reliant on paper-based activities as well as face-to-face contact with their customers for handling their claims and premiums (InformationAge, 2020). In addition, the selling of products was done by simple cross-selling and upselling approaches (EY, 2017), these products were often standardized, meaning they were not catered to the needs of the individual customer (KPMG: Customer and digitization, 2020).

Post-COVID, A more intensive use of *Data Analytics* has enabled insurers greater predictive capabilities which are aimed at matching products to customers based on, but not limited to geographic and demographic attributes. Analytics "listen" to customer input, recognize patterns which can be used to identify opportunities and help calculate the correct premium based on more accurate risk profiles. Other new technologies that have potential to assist insurers in their business operations can be seen in table 5, some are already being implemented (EY insurance, 2017) (KMPG: customer and digitization, 2020).

	Cost reduction	Customer experience enhancement	Speed to market	Sales productivity	Underwriting efficiency	Claims efficiency
Omni-channel	✓	✓	✓	✓		✓
Big data analytics	✓	✓	✓	✓	✓	✓
Internet of Things (IoT)	✓	✓			✓	
Telematics		✓		✓	✓	✓
Voice biometrics and analysis	✓	✓				
Drones and satellites					✓	✓
Blockchain	✓	✓	✓	✓	✓	✓

Table 5. Digital Transformation Scorecard. Note. Reprinted from *Digital Transformation in Insurance, by EY insurance, October 1 2020, retrievedfrom: https://germanyfintech.org/wp-content/uploads/2017/12/EY-Digital-Transformation-in-Insurance.pdf*
Copyright 2017 by EY insurance.

Through Artificial Intelligence and Intelligent Automation with the use of Data Analytics and IoT, insurance companies can streamline and enhance their processes in areas such as pricing and underwriting. For pricing a more dynamic and real-time behavioral model can be created to more accurately calculate premiums for specific customers. Moreover, underwriting accuracy is also scaled up due to speeding up the data collection and risk assessment through newly embedded technologies (KMPG: Fast track to technology, 2020).

Key processes which need to change are the sharing of more information via images and videos to support claims or to assess processes (KPMG: Fast track to technology, 2020). The creation of end-to-end digital pathways for customers and integration of channels. Issues encountered are the reluctance of customers to share information in the past. Since COVID-19 there are signs that this behavior has started to change (KPMG: Customer and digitization, 2020). For instance, Australia, where 2 million Australians signed up for the government's tracking app, COVID Safe, within 48 hours after it was launched (Regan, 2020). Important to note here, is that in general Australia is quite reluctant to share their personal information on this type of application (Regan, 2020). The Netherlands and Australia have a similar attitude towards sharing data, a survey done by GFK shows (GfK, 2017). Taking this into account, COVID-19 can create great possibilities for more sharing of information in the insurance industry.

COVID-19 has led to changes in the internal processes within the insurance industry. IT capabilities are enhanced in order to improve smooth business operations, done entirely from home and online. With many insurance businesses already transitioning towards more digital insurance, COVID-19 has accelerated the digital processes for online insurance applications.

CYBERSECURITY RISK MANAGEMENT

As previously described, COVID-19 forces insurance companies to accelerate their digital transformation efforts (KPMG: Fast track to technology, 2020).

The switch of customers increasingly using online services, created a greater attraction for hackers (Mitic, 2020). This development is especially risky for those customers who are not yet fully adapted to the use of new technology. Therefore, cyber security needs to be a fully integrated consideration of the digital transformation process undertaken by insurance companies.

Digital Changes in the Insurance Industry

Before the pandemic, some insurance companies were already well on their way in terms of their digital transformation. However, many companies needed to make rapid changes to how they conduct their business in order to survive the pandemic. Luckily with technological advancements in AI and predictive analytics, claims are now being processed in minutes without any manual intervention (Clover Infotech, 2020). The AI technologies are supported by machine learning (ML), neural networks, natural language processing (NLP) and computer vision, bringing the industry from 'detect and repair' to 'predict and prevent' (The Friday Five, 2020).

Insurance companies need to change their approach from office-based to online, with a strong focus on *Customer Experience, AI & Data Analytics* as well as *Process Automation* (Clover Infotech, 2020).

First, a digital engagement model should be implemented. In the past three years the online application for insurance has quadrupled according to a well-known insurance provider (name not mentioned in source) (Clover infotech, 2020). Consequently, a more digitized business process can help insurers acquire more accurate data as well as enable them to process claims faster and minimize mismatching (Clover Infotech, 2020).

In addition, the tracking of pending claims and policy renewals is made easier and more dynamically integrated into the processes. This dynamic integration is made possible by implementing Robotic Process Automation or R.P.A.. R.P.A. tools are increasingly used within the insurance industry to help enable their digital transformation (Clover Infotech, 2020).

Risks Identified

In consideration of the digital transformation mentioned above, insurance companies are dealing with increasing cybersecurity risks due to COVID-19. Insurance companies are a potential target for cyber attackers, as they possess a large amount of confidential information about policyholders (Jones, 2016).

Having studied the available literature we have identified a number of risks that threaten companies active in the insurance industry. These risks will be discussed in the following section. In order to understand how we determine risk and construct a risk matrix; two definitions are important to note: likelihood and impact. Likelihood refers to the 'chance that something will occur', based on the frequency of the occurrence (Refsdal, 2015). Likelihood is classified as: Certain (5), Likely (4), Possible (3), Unlikely (2), Rare (1). Impact entails the 'effect of an incident on an asset in terms of harm or reduced assets value (Refsdal, 2105). Impact is classified as: Critical (5), High (4), Considerable (3), Low (2), Very Low (1). Lastly, in order to mitigate the risks, control measures are suggested. Control measures are 'measures implemented to prevent, or else to detect and correct a control risk (Hulstijn - Lecture 3, 2020).

Risk 1. Attacks via email. *Phishing email***,** this attack will typically direct the user to visit a website where they are asked to update personal information, such as password, credit card, social

security or bank account numbers, that the legitimate organization already has.(European Insurance and Occupational Pensions Authority, 2019) and *Business Email Compromise (BEC)* which are email schemes that target recipients to conduct wire transfers, typically by impersonating the CEO, CFO or other senior managers of the organization.

In 2016, consulting firm Accenture found that one out of three attacks on insurance companies resulted in a security breach (Accenture Security Report, 2016). Even though four out of five insurers believe that they are well protected against these attacks.

Phishing attacks overall have increased by 600% during COVID-19 (Enisa, 2020).

An example of a phishing attack that targeted the insurance industry was via a method known as *spear phishing*, where attackers focus on a particular company or branch. In May 2017, DocuSign, a legal service provider used by many insurance companies, was hacked via spear phishing. A list of email addresses in DocuSign's database were sent an email containing an attachment which was infected with malware. Even though this did not lead to any severe consequences it still showed how vulnerable third parties can expose insurance firms to certain risks. Considering the aforementioned, the likelihood of such an attack occurring is "high".

The impact of phishing attacks differs per organization. In 2014, the health insurer Anthem suffered from a phishing attack, where access to valuable customer data was obtained. The result was that 79 million customers had their personal information exposed and were therefore exposed to potential malicious intent (Berkowitz, 2019).

When a large insurance company becomes a victim of phishing email, it might lose part of its customer base because of negative exposure in the media. Also, customers who became victims of the attack could lose their trust in the company that was attacked.

It is worth nothing that an email attack is often only the first step in a more complex attack. For instance, an attacker would impersonate as a trusted entity and send a *phishing mail*. This mail would then include a malicious link. This could then lead to a *malware attack* or *ransomware attack*. These attacks are then the actual attack an attacker was aiming for. Therefore, the impact of a single phishing attack on the business continuity of an insurer "low".

Risk 2. Malware infection. A type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid (European Insurance and Occupational Pensions Authority, 2019).

Ransomware is one of the most common cyber security threats. According to Deloitte (2020), a group of large insurances and financial services companies (names not provided by source) were the victims of a group of cyber criminals who stole personal information of more than one million customers and sales prospects. Richardson and North (2017) describe that 79% of organizations in the UK in the year 2015/2016 suffered at least one ransomware attack and 22% over twenty attacks. They also describe financial services as one of the top four industries that are likely to become a victim of ransomware attacks.

During COVID-19 the risk of a successful ransomware attack has increased significantly (150%) (Bradshaw, 2020). This is due to weaker controls on home IT and higher likelihood of users clicking on such emails due to increased level of anxiety (KPMG; the rise of ransomware, 2020). Hence, the likelihood of this risk is "possible".

In another case, described by Deloitte (2020), the organizations that fell victim to a ransomware attack had to provide their customers with free credit monitoring for a year including reimbursement of all damages resulting from the breach. Next to that, there was substantial damage to the brand of the affected organizations as well as a general loss of trust. Other possible consequences of a ransomware attack can be business downtime, productivity loss, revenue loss and business disruption in the post-attack period (Richard and North, 2017). Therefore, the impact of a ransomware attack can be considered to be "high".

Risk 3. Data Exfiltration. The loss of confidential data from companies to unauthorized people that breach the privacy of their customers, employees, clients or counterparties (European Insurance and Occupational Pensions Authority, 2019).

Now that a lot of business processes are becoming more digital including those of insurers (KPMG, 2020), the increase in cyber security incidents and more specifically *Data Exfiltration*, has increased significantly due to COVID-19 (PWC, 2020) . Therefore, the likelihood of the risk will be classified as "possible".

One case described by Deloitte (2020) shows how a very large investment and insurance company (names not provided by source) can be affected critically by data exfiltration. The case notes that even if the attack affects only a small number of employees, the company still receives large amounts of negative media coverage that damages the company's reputation.

Therefore, the impact of this attack on insurance companies is "high" due to the same impacts that Ransomware also has such as loss of

availability and trust, reputation damage, etc. According to the BBC, in July 2016, a U.S. health insurance company called 'Banner Health' suffered an unusual cyber-attack that attacked two independent data systems and exposed confidential information of 3.7 million customers and healthcare providers. The attacker accessed personally identifiable information (for example, social security number, claims and health insurance information) and payment data, including the cardholder's name, card number, and expiration date. After this data breach, at least one class action lawsuit has been filed. (BBC, 2016)

Risk 4. DDOS - Distributed Denial of Services. Type of attack where multiple compromised systems, which are often infected with a Trojan, 'any malware which misleads users of its true intent', are used to target a single system causing a Denial of Services attack. (European Insurance and Occupational Pensions Authority, 2019).

45% of businesses have been targeted by DDOS attacks and 10% of businesses are being targeted every week (Exigent Networks, 2019). In the last couple of years, the Russian cybersecurity vendor Kaspersky noted that there was a decline in DDOS attacks. However, since COVID-19, the amount of detected DDOS attacks has increased with 30% from the first to the second quarter (Kaspersky Q2 2020 DDOS attacks). According to Kaspersky (2020) they have detected and blocked 217% more in the third quarter of 2020 in comparison to the same period a year ago. This indicates that even though the amount of attacks has increased, the amount detected and blocked as well. Thus, we consider the likelihood to be "possible".

The impact of such an attack is "critical" since it leads to software or hardware replacements in 52% of the cases, revenue loss in 51% of the cases as well as e reputational damage (Exigent Networks, 2019).

It is likely that more and more insurers will be targeted by such attacks leading to further disruptions of business activities as well as significant remediation costs combined with costs associated with customer compensation arrangements. (Insurance Business, 2019).

Risk 5. Breach in Outsourcing Agreements. IT services are mostly outsourced to service providers in order for insurance companies to focus on their core business. However, a possible risk can be a cyber-attack on the outsourced company, which again has repercussions for the insurance company.

In order to create leaner organizations by establishing a more agile digital processing network, insurance companies might shift the custody of their assets. Therefore, a loss of control over their assets can be the consequence (EY, 2017). Moreover, as a result of COVID-19, the outsourcing of digital operations has increased, thus creating a greater risk for data breaches due to a potential lack of security on the other parties' end. For instance, in 2018, the insurance company Aflac had been the target of an attack which occurred via the hack of the email accounts of independent contractors. This led to the exposure of customers' sensitive personal information. (Berkowitz, 2019)

With regards to outsourced IT services, the companies asked to manage a company's IT services hold a near-monopolistic position within the market for IT-outsourcing. It has increased the monopolistic position of tech giants even further (Dayen, 2020). Due to this position of IT service providers, they become a more attractive asset to attack. Thus, increasing the probability that they become a victim of an advanced attack. Consequently, the likelihood of a breach in outsourcing agreements becomes "possible".

If such a situation would occur the impact would be "high". There is no knowing what data might have been accessed or stolen and the control is almost entirely out of the hands of the outsourcing company. Nonetheless, since critical assets (i.e. assets linked to the core business of the company) are not likely to be outsourced, the impact is not considered to be critical.

All of these attacks result in loss of trust. Since insurance businesses revolve around trust, a breach can significantly damage an insurers brand name and market value (Deloitte, 2020).

Risk Analysis

Table 6. Risk Matrix

Table 6. Risk Assessment Matrix

		Rare (1)	*Unlikely (2)*	*Possible (3)*	*Likely (4)*	*Certain (5)*
Impact	*Critical (5)*	5	10	15 **Risk 4**	20	25
	High Impact (4)	4	8	12 **Risk 2, 3, 5**	16	20
	Considerable Impact (3)	3	6	9	12	18
	Low Impact (2)	2	4	6	8 **Risk 1**	10
	Very Low (1)	1	2	3	4	5

Note: Calculation risk = Likelihood * Impact

Table 7. Risks Prioritization

Prioritized Risks	*High*	*Medium*	*Low*
Risk 1 – Attacks via Email			✔
Risk 2 – Malware Infection		✔	
Risk 3 – Data Exfiltration		✔	
Risk 4 – DDOS		✔	
Risk 5 – Breach in Outsourcing Agreements		✔	

Note: High > 19, Medium 10 – 19, Low < 10

Note: Calculation = Likelihood * Impact

Mitigation of Risk: Control Measures

The above-mentioned risks can be mitigated by implementing the following control measures:

- *The Managing of Risk Appetite* Risk appetite is the risk an insurer is willing to take in order to conduct every business operation successfully (EY Insurance, 2017). What is important here is for insurance firms to have a thorough understanding of the assets under their control as well as the ability to ensure that only the information that is required for the adequate undertaking of outsourcing activities is shared. If this is done correctly, the risk of critical systems and sensitive information being compromised is contained. This is how *potential breaches in outsourcing agreements* (risk 5) can be controlled for.

- *Dynamic vulnerability assessment*
  Vulnerability assessments help to keep track of any new technological risk (risk 2, 3, 4), including real-time alerting to detect attacks and measure their impact (Brook, 2020). This is done before the product reaches the customer (De Groot, 2020).

- *Cloud security and compliance*
  Redundancy is obtained by using multiple cloud service providers (Brook, 2020). Moreover, this can monitor configuration drift and unauthorized manipulation (Zurich Commercial Insurance, 2020). In doing so, DDoS attacks can be observed and controlled (risk 4).

- *Internet Perimeter Protection*
  By ensuring properly configured firewalls and monitor firewall logging in, can help to mitigate the risk of DDoS attacks (risk 4) (Zurich Commercial Insurance, 2020) (Brook, 2020).

- *Re-evaluation of technologies and threats*
  Constantly re-evaluate new technologies and threats to maintain focus on the right cybersecurity priorities (EY, 2014). Using tests to ensure and monitor the 'health' of security systems and the prevention of any unexpected attacks. Malware Infection in the form of Ransomware (risk 2) is mostly mitigated using this control.

- *Anti-Virus & Anti-Malware programs*
  These programs can help to mitigate malware attacks (risk 2) (Jones Jr. & Muhammad, 2017).

- *Management of assets*
  Critical assets have to be prioritized and performed internally rather than being outsourced to BPOs or cloud (EY, 2014). Main responsibility here lies with management and board support from professional partners and suppliers. Moreover, data- and privacy agreements will contain the consequences whenever there is a breach by an outsourced party (risk 5).

- *Employee/user awareness training*
  Ensuring that information security is an integral part of the risk management function, and not assigned to an autonomous unit that does not involve the whole company in the process (EY, 2014). By continuously training and creating awareness amongst its employees the likelihood of a successful cyberattack is reduced. Additionally, employees should be informed about correct corporate processes and procedures in order to detect hacker attacks (Zurich Commercial Insurance, 2020). This will control the risk of phishing mails (risk 1).

- *Detection & Blocking of phishing mails and other links*
  Even though the above-mentioned control measure can prevent many phishing attacks. It is still possible for phishing attacks to succeed in their intent. Employees can forget their training, or simply be caught off-guard for a moment. However, a comprehensive DNS web filtering could offer a solution, it can help detect phishing campaigns, block fraudulent links, rogue antivirus downloads and forced redirection to malicious domains. (Defense Intelligence Blog, 2017) This control can help to almost entirely mitigate the risk of phishing attacks (risk 1) and also Data Exfiltration attacks (risk 3).

Table 8. Control Measures Assessment

	Attacks via Email	*Malware Infection*	*Data Exfiltration*	*DDOS*	*Breach of Outsourcing Agreements*
*Likelihood (1-5) * impact (1-5)*	4 * 2 = 8	3 * 4 = 12	3 * 4 = 12	3 * 5 = 15	3 * 4 = 12
New Controls	Employee/User Awareness training Detection & Blocking of phishing mails and other links	Dynamic Vulnerability Assessment Re-evaluation of technologies and threats Anti-Virus and Anti-Malware programs	Dynamic Vulnerability Assessment Detection & Blocking of phishing mails and other links	Dynamic Vulnerability Assessment Cloud Security and Compliance Internet Perimeter Protection	Manage Risk Appetite Management of Assets
*Likelihood (1-5) * Impact (1-5)*	1 * 4 = 4	2 * 4 = 8	2 * 4 = 8	2 * 5 = 10	2 * 4 = 8

Note: High > 19, Medium 10 – 19, Low < 10

Acceptance of the Risk

The digital transformation process brings with it numerous risks. Due to the fact that many processes will become exclusively online based cyber security risks will become an even larger driver of the overall vulnerability of insurance firms. Nonetheless, some measures and controls have been identified to mitigate these risks. As can be seen from the table above, risks can be reduced significantly. As a consequence of implementing these controls, companies will operate in a more risk-free online environment. All the risks are reduced to be (almost) below 10, which is an acceptable rate. However, we do want to stress that insurance companies ought to consider that these risks are not completely mitigated and that dynamic risk assessment is of crucial importance to address any possible (new) attacks.

DISCUSSION

In this section, the integration of the sub-topics (IT Governance, Business Process Integration, Cyber security and Risk Management) will be made. Also, it includes practical implications, limitations of the research and recommendations for future research and practical implementation.

Firstly, on a general level, it is clear that the environment in which insurance companies operate, has experienced a major shock from COVID-19. This has had an effect on how insurance companies operate: our research shows that governance mechanisms will need to change in order to become better prepared for the next black swan event. New technologies are beginning to play an even larger role and cyber security risks have increased significantly, all of this in turn raises the need for enhanced digital capabilities as well as risk controls.

These required changes can be integrated into a singular *Digital Transformation*(DT) strategy. In a way COVID-19 acted as a catalyst for DT: insurance companies were forced to speed up their digital transformation efforts. Traditionally insurance companies were slow moving behemoths, they could afford to lag behind in terms of technological adoption, this has changed, now they need to become agile, nimble and resilient as well as more technologically savvy. The framework of Figure 5 shows the most important pillars (BPI, CSRM and ITG) and aspects that need to be taken into account by insurers in order to achieve this.

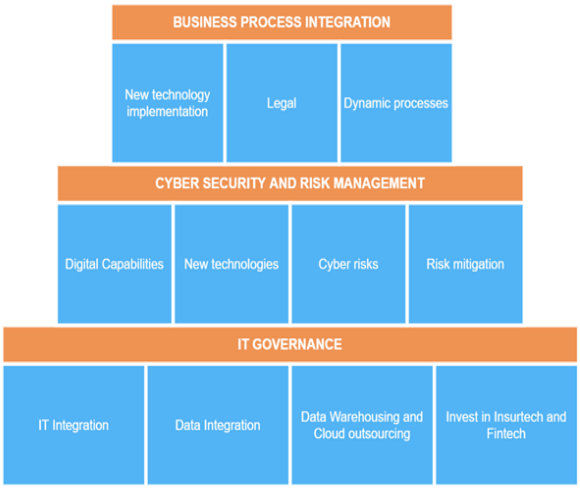

Figure 3. Integrated Framework

This research has multiple practical implications: first and foremost, the framework should prepare an organization for the unexpected by continuously improving and re-evaluating existing processes. We suggest creating a commission to periodically evaluate the overall preparedness of the organization.

This research is not without limitations. Firstly, the data used for the analysis is not without assumptions, because of the complete lack of documentation in some areas. Secondly, the study greatly relies on informal reports from consultancy firms, which do not need to adhere to academic rigor. This means this report does not have complete academic rigor either; as a consequence, the data analysis should not be treated as unshakable. Rather, we invite insurance companies to share their insights in order to make a contribution to the research question: "*How can IT/IS management assist the Dutch insurance industry in the managing of the effects of an unforeseen disruptive external event such as the COVID-19 pandemic?"*

For future research, we recommend gathering more primary data within the Dutch insurance sector about all three main topics (ITG, CSRM and BPI) during or after a black swan event such as COVID-19, 9/11 or Hurricane Katrina.

CONCLUSION

COVID-19 has had implications for businesses all over the world, including the Dutch insurance industry. In our paper we researched whether there are any long-term solutions to be incorporated in the models of the industry to respond to uncertain circumstances. Insurers sell security, which is more difficult to maintain when disruptive black-swan events occur. Considering this, we recommend a few main tasks in different departments for IT/IS management that insurance companies need to embed in their business in order to manage unforeseen disruptive external events.

For the IT governance of an insurance company we advise a stronger emphasis of IT within the adopted archetype. Insurance companies ought to reevaluate their IT architecture and change their strategic mindset to resemble those found in typical Insurtech firms.

COVID-19 has also brought forth an increased trend in cyber-attacks on businesses. With the expansion of technology needed for the insurance industry, it is evident that attention and investments need to be paid to mitigate the cybersecurity risks. Incorporating a dynamic risk assessment is crucial to detect and respond to new attacks.

Insurance companies should aim to become more resilient with respect to black-swan events. Despite COVID-19 still being amongst us it has already become clear that the way forward for insurers is the speeding up of their digital transformation efforts.

ACKNOWLEDGMENTS

We want to thank drs. ing. Kenny Meesters for setting up the structure for this research paper. Furthermore, we would like to thank dr. Andreas Alexiou, prof. dr. Carol Ou, dr. Joris Hulstijn, dr. ir. Francesco Lelli and dr. Emiel Caron.

REFERENCES

Accenture Security Report (2016). Key Insights for Insurance. | Accenture. Retrieved 2 October 2020, from http://ins.accenture.com/rs/897-EWH-515/images/Accenture-Security-Report-2016-Key-Insights-for-Insurance-POV.pdf

Accenture: Digital capabilities for insurance customers. (2020). Retrieved 2 October 2020, from https://www.accenture.com/nl-en/blogs/insights/what-digital-capabilities-matter-most-to-insurance-customers

Bainbridge, R. (2020). China records increase in demand for insurance among women during Covid-19. Retrieved 8 October 2020, from https://www.itij.com/latest/news/china-records-increase-demand-insurance-among-women-during-covid-19

Baraniuk, C. (2016) BBC: US health insurer warns 3.7m after cyber-attack. | BBC |. Retrieved 2 October 2020, from https://www.bbc.com/news/technology-36976701

Berkowitz, M. (2019). Cybersecurity for the Insurance Industry - Insurance Thought Leadership. Retrieved 2 October 2020, from

https://www.insurancethoughtleadership.com/cybersecurity-for-the-insurance-industry/

Boston Consulting Group, perspectives in insurance. (2015). Retrieved 22 September 2020, from https://image-src.bcg.com/Images/Perspectives_in_Insurance_Jan_2015_tcm9-79815.pdf

Bradshaw, S. (2020). Data breaches during COVID-19: Insights and best practice tips from the OAIC | Clayton Utz. Retrieved 7 October 2020, from https://www.claytonutz.com/knowledge/2020/august/data-breaches-during-covid-19-insights-and-best-practice-tips-from-the-oaic

Brook, C. (2020). How to Mitigate a DDoS Attack. Retrieved 2 October 2020, from https://digitalguardian.com/blog/how-mitigate-ddos-attack

Bryan Cave Leighton Paisner - Does "late payment" of Covid-19 BI claims create additional exposure for insurers and reinsurers?. (2020). Retrieved 8 October 2020, from https://www.bclplaw.com/en-GB/insights/does-late-payment-of-covid-19-bi-claims-create-additional-exposure-for-insurers-and-reinsurers.html

C. Jones, J. Muhammad. 2017. Ransomware and Its Impact on Modern Society. In *Proceedings of 2017 ADMI Symposium,* Virginia Beach, Virginia USA, March 23-26.

Chakrabarty, A. (2020). Insurance Trends During Covid-19: Health in high demand, Motor lags. Retrieved 10 October 2020, from https://www.financialexpress.com/money/insurance/insurance-trends-during-covid-19-health-in-high-demand-motor-lags/1996340/

Chappelow, J. (2020) Black Swan. | Investopedia| Retrieved 8 October 2020, from https://www.investopedia.com/terms/b/blackswan.asp

Cortis, 2019: Cortis D., Debattista J., Debono J., Farrell M. (2019) InsurTech. In: Lynn T., Mooney J., Rosati P., Cummins M. (eds) Disrupting Finance. Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Pivot, Cham. Retrieved 5 October 2020, from https://doi-org.tilburguniversity.idm.oclc.org/10.1007/978-3-030-02330-0_5

Dayen, D. (2020). America's Monopoly Problem Goes Way Beyond the Tech Giants. Retrieved 7 October 2020, from https://www.theatlantic.com/ideas/archive/2020/07/pandemic-making-monopolies-worse/614644/

De Groot, J. (2020). Top Security Considerations for Insurance Companies. Retrieved 2 October 2020, from https://digitalguardian.com/blog/top-security-considerations-insurance-companies

Defence Intelligence Blog - Phishing and its Impact on Businesses and Employees. (2017). Retrieved 2 October 2020, from https://defintel.com/blog/index.php/2017/02/phishing-and-its-impact-on-businesses-and-employees.html

Deloitte Global (2020). Understanding COVID-19's impact on the insurance sector | Retrieved 8 October 2020, from https://www2.deloitte.com/global/en/pages/about-deloitte/articles/covid-19/understanding-covid-19-s-impact-on-the-insurance-sector-.html

Deloitte, Sam Friedman: insurtechs are disrupting the insurance industry. (2017). retrieved 26 September 2020, from https://www2.deloitte.com/us/en/pages/financial-services/articles/insurtechs-disrupting-insurance-industry.html

Deloitte. Insurance - Cyber Executive Briefing | Deloitte | Analysis. (2020). Retrieved 2 October 2020, from https://www2.deloitte.com/be/en/pages/risk/articles/insurance.html#case-3

Digital Transformation in the Insurance Industry post COVID-19 | Clover Infotech. (2020). Retrieved 2 October 2020, from https://www.cloverinfotech.com/blog/digital-transformation-in-the-insurance-industry-post-covid-19/

Eiopa (2020). | Impact of Ultra Low Yields on the Insurance Sector, including First Effects of COVID-19 Crisis | Retrieved 8 October 2020, from https://www.eiopa.europa.eu/sites/default/files/financial_stability/impact-of-ultra-low-yields-on-the-insurance-sector-including-first-effects-of-covid-19.pdf

Eling, Martin & Lehmann, Martin. (2018). The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks. Geneva Papers on Risk and Insurance - Issues and Practice. 43. 359-396.

Enisa (2020) | Understanding and dealing with phishing during the covid-19 pandemic. Retrieved 7 October 2020, from https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic

European Insurance and Occupational Pensions Authority (2019). Cyber Risk for Insurers - Challenges and Opportunities. | EIOPA. Retrieved 2 October 2020, from https://www.eiopa.europa.eu/sites/default/files/

publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf

Exigent Networks. The Destructive Impact of DDoS Attacks – Infographic. (2019). Retrieved 2 October 2020, from http://www.exigentnetworks.ie/the-destructive-impact-of-ddos-attacks-infographic/

EY (2014). Mitigating Cyber Risk for Insurers | Insights into Cybersecurity and Risk Part 2. Retrieved 2 October 2020, from https://www.ey.com/Publication/vwLUAssets/EY_-_Insights_into_cybersecurity_and_risk_(Part_2)/$File/ey-mitigating-cyber-risk-for-insurers.pdf

EY insurance (2017). Digital transformation in insurance. Retrieved 1 October 2020, from https://germanyfintech.org/wp-content/uploads/2017/12/EY-Digital-Transformation-in-Insurance.pdf

General Insurance Article - Increased demand for private medical insurance after COVID19. (2020). Retrieved 8 October 2020, from http://www.actuarialpost.co.uk/article/increased-demand-for-private-medical-insurance-after-covid19-18468.htm

GfK (2017). Global GfK survey; willingness to share personal data in exchange for benefits or rewards. | GfK. Retrieved on 9 October 2020, from https://cdn2.hubspot.net/hubfs/2405078/cms-pdfs/fileadmin/user_upload/country_one_pager/nl/images/global-gfk_onderzoek_-_delen_van_persoonlijke_data.pdf

Hay, L. (2020). COVID-19: could liquidity challenges be on the way for insurers? Retrieved 11 October 2020, from https://home.kpmg/xx/en/home/insights/2020/05/covid-19-could-liquidity-challenges-be-on-the-way-for-insurers.html

Hulstijn, J. (2020) Lecture 3 Risk Management and Controls. | Tilburg University. Retrieved on 9 October 2020.

KPMG: Do Insurers have COVID-19 Covered? (2020). Retrieved on 1 October 2020, from https://home.kpmg/xx/en/home/insights/2020/03/do-insurers-have-covid-19-covered.html

InformationAge (2020). Digitization accelerated by Covid-19 will change the insurance industry. Retrieved 1 October 2020, from https://www.information-age.com/digitisation-accelerated-covid-19-change-insurance-industry-123490366/

Jones, T. (2016). Digital transformation exposes insurers to greater cyber-security risks - Accenture Insurance Blog. Retrieved 2 October 2020, from https://insuranceblog.accenture.com/digital-transformation-exposes-insurers-to-greater-cyber-security-risks

Kaspersky DDoS attacks in Q2 2020. (2020). Retrieved 7 October 2020, from https://securelist.com/ddos-attacks-in-q2-2020/98077/

KPMG: COVID-19 puts insurers on the fast-track to technology adoption. (2020). Retrieved 1 October 2020, from https://home.kpmg/xx/en/home/insights/2020/04/covid-19-puts-insurers-on-fast-track-to-technology-adoption.html

KPMG: COVID-19: customer and digitization in insurance. (2020). Retrieved 1 October 2020, from https://home.kpmg/xx/en/home/insights/2020/05/covid-19-customer-and-digitization-in-insurance.html

KPMG: Do Insurers have COVID-19 Covered? (2020). Retrieved on 1 October 2020, from https://home.kpmg/xx/en/home/insights/2020/03/do-insurers-have-covid-19-covered.html

Kocianski, S. (2020). The impact of Coronavirus on the insurance industry. Retrieved 2 October 2020, from https://11fs.com/blog/the-impact-of-coronavirus-on-the-insurance-industry

Makinen, G. (2002). The Economic Effects of 9/11: A Retrospective Assessment. Retrieved 9 October 2020, from https://www.researchgate.net/publication/235132312_The_Economic_Effects_of_911_A_Retrospective_Assessment .

McKinsey, Catlin, Tanguy & Lorenz, Johannes-Tobias. (2017). Insurtech the threat that inspires. Retrieved 28 September 2020, from https://www.mckinsey.com/industries/financial-services/our-insights/insurtecht-the-threat-that-inspires

Mitic, I. (2020). Everything You Need to Know about Online Banking: Statistics & Facts | Fortunly. Retrieved 7 October 2020, from https://fortunly.com/statistics/online-mobile-banking-statistics/#gref

Nafday, A., (2020). Strategies for Managing the Consequences of Black Swan Events. Leadership and Management in Engineering. Retrieved 9 October 2020, from https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%29LM.1943-5630.0000036

OECD (2020) Responding to the COVID-19 and pandemic protection gap in insurance. (2020). | Organisation for Economic Co-operation and Development | Retrieved 8 October 2020, from https://www.oecd.org/coronavirus/policy-responses/responding-to-the-covid-19-and-pandemic-protection-gap-in-insurance-35e74736/

Pedro Lima Ramos. (2017). Premium calculation in insurance activity, Journal of Statistics and Management Systems, 20:1, 39-65.

Pijl, T. (2017). A Framework to Forecast Insurance Claims. Erasmus University Rotterdam. Retrieved 2 October 2020, from https://thesis.eur.nl/pub/39731/Pijl.pdf

PWC (2020). Why has there been an increase in Cyber Security Incidents during COVID-19. | PWC UK Cyber Threat Intelligence. Retrieved on 9 October 2020, from https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html

Refsdal, A., Solhaug, B., & Stolen, K. (2015). Cyber-Risk Management: Springer. : https://www.springer.com/gp/book/9783319235691

Regan, H. (2020). 2 million Australians have downloaded a coronavirus contact tracing app. Retrieved 1 October 2020, from https://edition.cnn.com/2020/04/28/australia/covidsafe-coronavirus-tracing-app-australia-intl/index.html

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21.

Schich, S. (2009). Insurance Companies and the Financial Crisis. *OECD Journal: Financial Market Trends*. Vol 2009-2. Issue 2. Retrieved 5 October 2020, from https://www.oecd.org/pensions/insurance/44260382.pdf

The Friday Five: COVID-19 Impact on the Insurance Industry. | LexisNexis. 2020). Retrieved 2 October 2020, from https://blogs.lexisnexis.com/insurance-insights/2020/03/the-friday-five-coronavirus-impact-on-insurance-industry/

The rise of ransomware during COVID-19. (2020). Retrieved 7 October 2020, from https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html

Weill, Peter & Ross, Jeanne. (2004). IT Governance on One Page. SSRN Electronic Journal. 349.

Vektis (2019). Zorgthermometer: verzekerden in beeld 2019. (2019). Retrieved 20 September 2020, from https://www.vektis.nl/uploads/Publicaties/Zorgthermometer/Zorgthermometer%20Verzekerden%20in%20Beeld_2019.pdf

Zurich Commercial Insurance (2020). Risk Insights: The Cyberdimension of the Coronavirus. Retrieved 2 October 2020, from https://www.zurich.com/en/knowledge/topics/cyber-and-data-risks/the-cyber-dimension-of-covid-19

15 years after Katrina: Would we be prepared today? (2020). Retrieved 9 October 2020, from https://www.swissre.com/dam/jcr:a835acae-c433-4bdb-96d1-a154dd6b88ea/hurrican-katrina-brochure-usletter-web.pdf