Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 8, Issue 2, 2020

The invisible hole of cybersecurity insurance services

Tal Pavel, The Academic College of Tel Aviv–Yaffo, Israel, talpv@mta.ac.il

Ruti Gafni, The Academic College of Tel Aviv Yaffo, Israel, rutigafn@mta.ac.il

Abstract

This study examines the cybersecurity insurance market in the United States (U.S.) in order to reveal if an "invisible hole" of services and information exists in this market. This is performed by mapping the cybersecurity insurance services, offered by insurance companies, to cope with cybersecurity risks, and finding in which way these services are exposed, visible and comprehensive, in the insurance companies' websites. The research questions examined the extent cybersecurity insurance services offered by the main U.S. insurance companies; the visibility of such services on their websites; and the types of services offered. The sample included 44 insurance companies based upon nine lists of the top U.S. insurance companies. The findings present that most companies (68%) offer cybersecurity insurance services, while only a few (26.92%) expose such information in a visible way. Moreover, on the one hand, the insurance companies use general terms for services, which may be blur and ambiguous, while on the other hand, there is a widespread of specific services, most of them (81%) provided only by few companies. These findings may derive due to insufficient understanding of cybersecurity insurance clients' needs and may reflect the lack of maturity of the cybersecurity insurance market, as matured marketplaces are mostly more standardized. This study demonstrates that there is a long way to advance until the insurance market for cybersecurity risks will be mature, customers (businesses and organizations) will understand the needs for such insurance, and insurance companies will develop and offer relevant insurance services.

Keywords: Cybersecurity, insurance, cybersecurity insurance, cyber insurance, cyber coverage, information security, cybersecurity policy.

Introduction

Technology develops at a very fast pace, which creates new business opportunities, but alongside, new, unknown risks and challenges rise. Among them cybersecurity risks, that meet conservative markets, in this case, the insurance market. The cybersecurity insurance market is immature, since it is relatively a new market, with ongoing and developing features. This market face unique challenges, such as the ability to estimate the costs and losses due to an unknown cyber-attack, and to classify cybersecurity risks and attacks (Helms, 2019; Marotta et al., 2017; Marotta et al., 2015). This is an immature market both from the customers' perspective, who face new and unknown risks and threats and from the perspective of the insurance companies, who need to estimate a new world of risks, costs, losses, and their implications.

One of the main problems in cybersecurity insurance is to identify and cover the types of cybersecurity losses as well as events that affect the firms. There can be different types of losses, which some of them can be difficult to predict, such as reputational, regulatory and liability losses, and even some of the operational losses (Pooser et al., 2018). Therefore, cybersecurity insurance markets suffer from lack of data, analysis, research, and literature (Pooser et al., 2018). Thus, there is a need to provide formalization and standardization of terms, concepts, and regulatory guidelines in the area of cybersecurity insurance. Alongside with the knowledge problem, and mainly the knowledge gap among the organizations as well as the insurance companies, there is a gap of expectations between the customers and suppliers of cybersecurity insurance. One of the problems is the lack of incentive of the customers to manage their cybersecurity risk using cybersecurity insurance services. Moreover, the information needed, to cope with cybersecurity and being prepared for cyber-attacks, including the possibilities of relevant insurance, are not approachable to Small and Medium Businesses (SMBs), which are the majority of businesses (Gafni & Pavel, 2019). Neither the customers nor the suppliers of cybersecurity services are much experienced in estimating the costs and probabilities of cybersecurity risks. Customers underestimate the probability of cyber-attacks to their business, leading to underestimation of the possible risks (Rohn et al., 2016). Suppliers of cybersecurity insurance services do not have enough experience and historical data, to identify, assess and evaluate the risks and the premium needed (Tøndel et al., 2016). Another aspect is the role of the insurance companies in consulting and risk assessments, as private governance mechanism in improving the organizations' cyber readiness (Talesh, 2018). All these raise the level of uncertainties among the relevant players, customers and insurance companies, as well as keep this market immature.

This study aims to map the cybersecurity insurance market in the U.S. based upon the cybersecurity insurance services offered by the top U.S. insurance companies, as appear on their websites. The research questions examined were:

RQ1. To what extent do the main U.S. insurance companies offer cybersecurity insurance services?

RQ2. What is the visibility of the cybersecurity insurance services at those insurance companies' websites?

RQ3. What are the main cybersecurity insurance services offered by those insurance companies?

The sample included 44 insurance companies based upon nine lists of the top U.S. insurance companies, as explained in the methodology section. The findings present that 68% of those, do offer cybersecurity insurance services, while only 26.92% of them expose the information in a visible and easy way.

This study's importance is in portraying the cybersecurity insurance market from the insurance companies' perspective. Further research may illustrate this market based upon the customer's needs, bought policies, as well as policies claims. This study demonstrates that there is a long way to advance until the insurance market for cybersecurity risks will be mature, customers (businesses & organizations) will understand the needs for such insurance, and insurance companies will develop and offer relevant insurance services. The rest of this paper includes a literature review

enlightens the problems in cybersecurity insurance, a methodology section explaining the way this research was performed, a results section with the findings, as well as discussion and conclusion sections analyzing the findings.

Literature Review

The reviewed literature covered several aspects of the cybersecurity insurance market, its characteristics and challenges: some researches portray the picture of cybersecurity insurance as a tool to manage and mitigate cybersecurity risks and the importance of regulatory mechanisms to achieve the desired effects in some situations (Biener et al., 2015; Franke, 2017; Peters et al., 2018). Others focus on one of two sides of the cybersecurity insurance coin: Some research examine the organizations (i.e. the customers of cybersecurity insurance services) inclination and readiness to adopt cybersecurity insurance services (Bandyopadhyay, 2012; Bandyopadhyay et al., 2009; De Smidt & Botzen, 2018; Franke & Meland, 2019). Others deal with the cybersecurity insurance companies (i.e. the suppliers of cybersecurity insurance services), mainly in the context of assessing cybersecurity risks (Eling & Schnell, 2016; Meland et al., 2017; Tøndel et al., 2016).

The Cybersecurity Insurance Market

Eling and Schnell (2016) pointed that the research on cybersecurity risk is limited while emphasizing the immense difficulties to insure cybersecurity risk, mainly due to lack of data and modelling approaches, mentioning that availability of data on cybersecurity risk is rather scarce. Therefore, they tried to establish a database on studies, articles, and working papers on cybersecurity risk as well as cybersecurity risk insurance, with a focus on business and economics literature, providing definition and categorizations of cybersecurity risk. For that purpose, they scanned 209 papers, finding definitions of cybersecurity risks, ways to find data and to model cybersecurity risks. Eling and Schnell (2016) asserted that estimating the costs caused by cybersecurity risk is difficult and that some types of cyber-crime might even generate no costs at all or that the costs cannot be quantified. Moreover, they argued that in some cases, cybersecurity risk poses a threat to the global economy and society, and thus, they increase the challenges to cybersecurity insurance markets. The immature stage of the cybersecurity insurance market is a consequence of the evolution of cybersecurity threats in the last decade. The cybersecurity insurance market is not a regular insurance market, where the insurance companies have lots of experience and historic cases but is a unique and new challenge that must be examined as well as investigated (Marotta et al., 2015; Marotta et al., 2017). There is a need to standardize the cybersecurity risks regulation guidance since it poses an obstacle for organizations operating across different markets (Peters et al., 2018). Moreover, there is a need to examine different perspectives adopted by industry and regulators, to classify cyber-crime or cybersecurity risk loss processes, the emerging market of cybersecurity risk insurance and the challenges resulting from the diversity of insurance coverage, lack of homogeneity in service design, coverage, and uncertainty relating to potential exposures as well as vulnerabilities associated with this risk class. A conservatism in pricing exists in cybersecurity insurance instruments (Bandyopadhyay et al., 2009) which can explain the limited growth of the cybersecurity insurance market. Meland et al. (2017) examined the cybersecurity insurance market in Norway, especially the issue of uncertainties, raising the need to minimize the uncertainty among the organizations to elevate the

so-called immature cybersecurity insurance market. That includes, among others, security and coverage gaps. Biener et al. (2015) intended to "close" the research gap in the risk and insurance economics literature. For that purpose, their research examined 994 cases of cybersecurity losses (4.5 % of the total from total 22,075 incidents of operational loss that were reported between March 1971 & September 2009). They concluded that cybersecurity threats and risks have a unique nature compared to other operational risks, which affect the development of the cybersecurity insurance market as one of the possibilities for managing cybersecurity risk exposures. They indicated the importance of consulting and risk assessment by insurance companies and mention that there is a great need for more research on cybersecurity insurance.

The Cybersecurity Insurance Customers

Bandyopadhyay (2012) examined the inclination and the involved factors of cybersecurity insurance adoption by organizations, as part of the set of tools to manage their cybersecurity risks. A model that can explain the forces of organizational adoption of cybersecurity insurance, which integrates technology, organizational and environmental factors was developed. Franke and Meland (2019) shed the light on the expectations that early and prospective customers have towards cybersecurity insurance, especially the gap between what customers expect and what insurers offer, as exist in companies in Norway and Sweden. Aspects of cybersecurity risks asserting cybersecurity insurance could behave differently from other traditional insurances, from the very basic nature of cybersecurity events, emphasizing that the optimal purchase decision depends on the mixture of the types of cybersecurity breaches that a firm face (Bandyopadhyay & Mookerjee, 2019). Moreover, they elaborate how organizations behave in cases of cybersecurity events regarding claiming cybersecurity insurance, because of the complexity involved in the post-breach decision of whether and how a firm should optimally plan to claim indemnity in the event of a cybersecurity breach. Mukhopadhyay et al. (2013) advocated using cybersecurity insurance services to minimize the financial losses from security breaches. They proposed models to help the organizations to decide on the right cybersecurity insurance service, using expected loss computation, and even calculated the premium that a cybersecurity risk insurer can charge to indemnify cybersecurity losses. More and more companies begin to adopt cybersecurity-risk insurance services, thus, the trust of customers for these services will increase, positively impacting the top lines of a company too (Mukhopadhyay et al., 2013). This will help induce insurers to create more attractive cybersecurity services for firms, as well. Cybersecurity insurance companies are important as private governance mechanisms in improving the organizations' cybersecurity readiness and security (Woods & Moore, 2019). This is achieved by assessing organizational security postures, creating rules and enforcement mechanisms, prescribing security procedures and controls, and providing post-incident services. All these might influence the customers' security decisions to reduce cybersecurity losses. Nevertheless, currently, cybersecurity insurance appears to be a weak form of governance, since they focus more on organizational procedures than technical controls. Although cybersecurity risk poses major threats to organizations, most of them do not have enough protection to cope with cybersecurity risks and their implications (Talesh, 2018). Cybersecurity insurance can help the customers mitigate the cybersecurity threats, by motivating them to take proactive activities to manage cyber-attacks. This includes investing in improving their cybersecurity, assess their current insurance coverage, estimate and analyze their cybersecurity risk exposure and deciding whether to invest in

cybersecurity insurance to mitigate cybersecurity risks, providing a motive of self-protection (Biener et al., 2015; Shackelford, 2012). De Smidt and Botzen (2018) analyzed the human factor behind cybersecurity insurance and especially the decision-making process. Their research examined corporate professionals related to cybersecurity risks and revealed the importance of behavioral factors in influencing the perceived probability and impacts of cyberattacks. They revealed that the awareness of cyberattacks and risks may be high, but the impacts, especially financials, are underestimated. Therefore, organizations might be reluctant to insure cybersecurity risks. Indeed, only 18% of the surveyed organizations had purchased cybersecurity insurance, perhaps due to limited coverage conditions, high costs relative to perceived risks, and low uptake of cybersecurity insurance. The posture towards cybersecurity insurance is changing and growing, maybe because of the accumulating information of known and reported cyberattacks.

The Cybersecurity Insurance Suppliers

Other research examined the insurance market in different geographical zones, as well as the decision process of insurance companies relating to cybersecurity insurance and risk handling. Tøndel et al. (2016) emphasized the supplier, the cybersecurity insurance companies, mainly in the Nordic market, and examined their challenges in assessing cybersecurity risk. They found that the abilities of insurance companies to evaluate risk assessment is highly impacted by limited experience with cybersecurity insurance services and little historical data to rely on. Therefore, to be able to assess cybersecurity risks, the study underlines the need for improved approaches. According to Pooser et al. (2018) who examined the characteristics of early adopter firms of cybersecurity risk identification (smaller, more leveraged firms with greater profitability), in 2006, roughly 28% of insurance companies identified cybersecurity risk, while by 2013, 98% of insurance companies identified cybersecurity risk as a material risk. Franke (2017) referred to the cybersecurity insurance market in Sweden, mentioning that empirical investigations of cybersecurity insurance are rarely reported in the literature. The research asserts that the role of cybersecurity insurance is as not only an instrument to risk transferring, like any other insurance, but it also contains aspects of preparedness, avoidance and mitigation. They also emphasized the role of insurance companies as assisting in complying with privacy and dealing with cyberattacks, since their insurance services influence the ways organizations to comply with cybersecurity laws (Talesh, 2018). Eling and Schnell (2016) proposed that cybersecurity insurance firms can use the information collected about their customers, to provide standards and best practices for cybersecurity risks management and disseminate it to their customers.

Methodology

The main target of this study was to examine whether insurance companies offer cybersecurity insurance services to cope with cybersecurity risks. To understand and portray the cybersecurity insurance market, its main characteristics and features, and due to the immaturity of this market, the study focuses on one of the largest markets globally - the U.S. insurance market. From the same reason, the study covers the top U.S. insurance companies, with the intention that mapping the cybersecurity insurance service offered by the top U.S. insurance companies will enable a broad vision of the cybersecurity insurance market. The collection of data was performed by the authors of this paper, during December 2019 and January 2020.

The first research question (RQ1) - In what extent do the main U.S. insurance companies offer cybersecurity insurance services? - is covered by steps 1-4, which define the relevant insurance companies to be sampled:

1. Search the Internet (using Google search) for lists of top U.S. insurance companies
2. Create a unified list of all the companies out of the lists of top U.S. insurance companies
3. Count the number of appearances of each company in the unified list and sort the list by the number of appearances
4. Create a final list of top companies

The second research question (RQ2) - What is the visibility of the cybersecurity insurance services at those insurance companies' websites? - is covered by steps 5-7, which explore whether the insurance companies offer cybersecurity insurance services:

5. Retrieve the website address for each of the companies
6. Search for cybersecurity insurances for businesses in each insurance company website
7. If the cybersecurity insurance option is not visible, search the term 'Cyber' in each website, to verify the existence of cybersecurity insurance, not explicitly exposed

The third research question (RQ3) - What are the main cybersecurity insurance services offered by those insurance companies? - is covered by step number 8, which explores the types of cybersecurity services offered by those insurance companies offering cybersecurity insurance services:

8. For each company offering cybersecurity insurance, the features of the insurance were examined and annotated

Remark: in order to avoid exposure, promotion or marketing of the insurance companies, their name was omitted and change to an enumeration: IC1 (Insurance Company 1), IC2, IC3 and so on.

Findings

The search of the Internet for lists of top U.S. insurance companies (step 1 of the methodology), resulted in nine lists, as presented in Table 1. According to the nine lists of top insurance companies, a unified list of insurance companies was created (without duplicates), as defined in step 2 of the methodology. This list encompasses 315 different insurance companies. This list was sorted, according to the number of mentions of each insurance companies in the list (step 3 of the methodology), as shown in Table 2.

The sample of insurance companies to be examined was defined using the most mentioned companies in the lists (step 4 in the methodology). Obviously, a company mentioned in all nine lists is one of the top and has to be included in the sample. The final generated sample included the companies mentioned in four or more of the nine lists. The assumption was that companies mentioned in only a third of the lists, could not be counted as top companies. As can be seen in Table 2, the number of companies included in three lists is significantly higher comparing to those in four lists or more, confirming this assumption. Therefore, companies with three or less mentions were not selected. The list of selected companies is presented in Table 3. This final list was composed of 44 insurance companies.

Table 1. Top Lists of Insurance Companies in the U.S.

List Name	List Title	Number of Companies in the List
Wikipedia	List of United States insurance companies (n.d.)	203
Alphabetizer	Alphabetical List of Insurance Companies (n.d.)	177
Insurance-companies.co	List of All Insurance Companies in USA (n.d.)	173
Reinsurance news	The largest P&C insurers in the United States (2018)	101
The Balance Small Business	Top 25 U.S. Property/Casualty Insurers (Bonner, 2019)	25
Insurance Business America	These are the top 25 property/casualty insurance companies in the US (Moorcraft, 2016)	25
Disfold	Top 20 largest US insurance companies (2019)	20
Insurance Information Institute	Top 10 Life And Nonlife Insurance Companies, United States (Insurance Information Institute, 2017)	10
Business Insurance	Largest US insurers (2019)	10

Table 2. Number of Mentions of Insurance Companies in the Nine Lists

Number of Insurance companies	Number of appearances in lists
4	9
5	8
1	7
7	6
4	5
23	4
92	3
50	2
129	1

Each company's website was further investigated, to find if the specific insurance company offers business and commercial insurance and specific cybersecurity insurance services (according to steps 5-6 in the methodology). These findings are shown in the third and fourth column of Table 3, where "Y" defines that the insurance company offers this kind of service, "N" – no such service and "NA" – not applicable – the website of the insurance company is not available, and no information can be found online.

As can be seen, out of the 44 top U.S. insurance companies, only 26 offer services of cybersecurity insurance, which constitutes 59.09% of the companies. Four companies do not have websites, so it is not possible to find whether this kind of service is offered, and two companies do not offer business insurance, so it is obvious that they do neither offer cybersecurity insurance. Omitting these six companies, the percent of companies offering cybersecurity insurance is 68% (26 out of 38).

Table 3. Top U.S. Insurance Companies with Business and Cybersecurity Services

Insurance Company	Number of appearances in lists	Business and Commercial Insurance	Has Cybersecurity insurance services
IC1	9	Y	N
IC2	9	Y	Y
IC3	9	Y	Y
IC4	9	Y	Y
IC5	8	Y	Y
IC6	8	Y	Y
IC7	8	Y	Y
IC8	8	Y	Y
IC9	8	Y	Y
IC10	7	Y	Y
IC11	6	Y	Y
IC12	6	Y	Y
IC13	6	Y	Y
IC14	6	NA	NA
IC15	6	Y	Y
IC16	6	Y	N
IC17	6	Y	Y
IC18	5	Y	Y
IC19	5	Y	N
IC20	5	Y	N
IC21	5	Y	N
IC22	4	Y	Y
IC23	4	Y	N
IC24	4	Y	N
IC25	4	Y	N
IC26	4	Y	N
IC27	4	Y	Y
IC28	4	Y	N
IC29	4	NA	NA
IC30	4	Y	Y
IC31	4	Y	Y
IC32	4	Y	Y
IC33	4	N	N
IC34	4	Y	Y
IC35	4	NA	NA
IC36	4	Y	Y
IC37	4	N	N
IC38	4	Y	Y
IC39	4	Y	Y
IC40	4	Y	Y
IC41	4	NA	NA
IC42	4	Y	N
IC43	4	Y	Y
IC44	4	Y	N
Total	44	38	26

Table 4. Visibility and Ease to Find Cybersecurity Services

Insurance Company	Cybersecurity Insurance Visibility		
	Easy to find	**Relatively easy to find**	**Hard to find**
IC5	Part of the website homepage		
IC13	Part of the website homepage		
IC11			Unfriendly. Needs to search the term 'Cyber' in the search engine, not appear on Sitemap
IC2	Part of the website categories		
IC3	Part of the website categories		
IC4	Part of the website categories		
IC6			Unfriendly, dead link
IC7			Unfriendly
IC8		"Types of business coverage"	
IC9			Unfriendly. Needs to search the term 'Cyber' in the search engine, not appear on Sitemap
IC10			Unfriendly. Needs to search the term 'Cyber 'in the search engine, not appear on Sitemap
IC12			Unfriendly. Needs to search the term 'Cyber' in the search engine, not appear on Sitemap
IC15	Part of the website homepage		
IC17			Unfriendly. Needs to search the term 'Cyber' in the search engine, not appear on Sitemap
IC18	Part of the website homepage		
IC22		Business->All Business coverages->Data breach insurance	
IC27			Unfriendly. Products and Services->Protect your business->What we protect - our products->Cyber security and privacy
IC30			Unfriendly. Needs to search the term 'Cyber' in the search engine, not appear on Sitemap
IC31		Products->Specialized Coverages	
IC32		Products->Cyber Resilience Solutions	
IC34		Insurance->Business->Learn more->Grange Cyber Coverage	
IC36			Unfriendly. Needs to search the term 'Cyber' in the search engine, not appear on Sitemap
IC38		Business Insurance->Management & Professional Insurance->Cyber Liability Insurance	
IC39			Unfriendly. Our insurance->Business Insurance->Business Insurance Coverages
IC40			Unfriendly Our insurance->What we offer->Insurance products->Shared insurance products->Cyber and data breach
IC43			Unfriendly. Needs to search the term 'Cyber' in the search engine, not appear on Sitemap
Total	7	6	13

The visibility and ease of finding these services were examined (according to steps 6-7 of the methodology). The criteria to define visibility and ease to find consisted on finding a specific tab in the main menu, a specific button or a link in the main parts of the website. The results are summarized in Table 4. Out of the 26 companies offering cybersecurity insurance, only 7 (26.92%) of them expose the information in a visible and easy to find. 6 (23.08%) of them are relatively easy to find, but not obvious, and 13 (50%) are hard to find and very unfriendly. Further, the cybersecurity insurance services offered by each of these 26 insurance companies was examined according to each website, to discover the types of cybersecurity insurance coverage proposed (step 8 of the methodology). Table 5 exposes the insurance companies and the types of insurance coverage they propose.

Companies IC12 and IC17 offer, according to their website, only information about risks, how to manage them, but no cybersecurity insurance coverage for these risks. Thus, they were omitted from the table, leaving only 24 companies. The bottom row of the table shows the number of different cybersecurity insurance services offered by each insurance company.

The right column of the table shows the number of companies offering specific types of coverage, which are presented graphically in Figure 1.

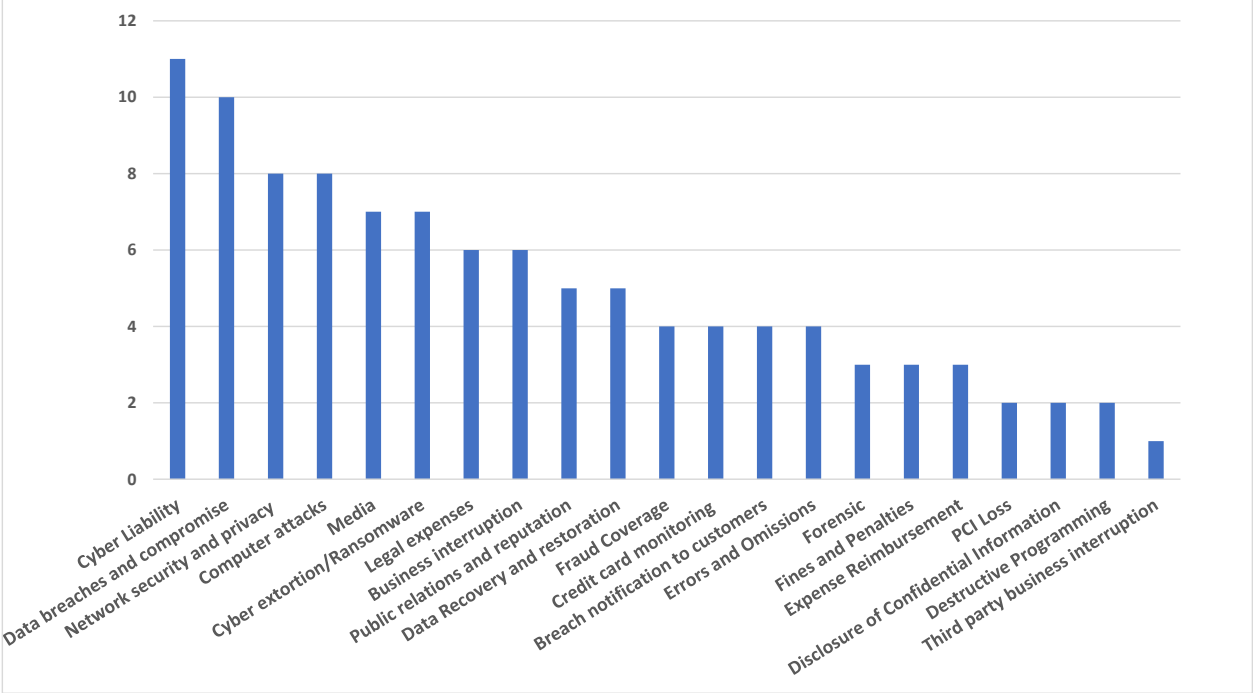

Figure 1. Number of Companies Offering Each Type of Cybersecurity Coverage

Table 5. Types of Cybersecurity Coverage Offered by Each Insurance Company

Types of Cybersecurity Coverage	Insurance Company																										Total
	IC2	IC3	IC 4	IC5	IC6	IC7	IC 8	IC 9	IC 10	IC 11	IC 12	IC 13	IC 15	IC 17	IC 18	IC 22	IC 27	IC 30	IC 31	IC 32	IC 34	IC 36	IC 38	IC 39	IC 40	IC 43	
Errors and Omissions	1		1										1											1			4
Destructive Programming	1																			1							2
Data Breaches and Data compromise	1	1			1		1			1		1			1	1		1						1			10
Computer attacks		1					1	1		1			1		1									1		1	8
Cyber extortion/ Ransomware		1						1				1	1		1						1					1	7
Disclosure of Confidential Information	1				1																						2
Data Recovery and restoration		1					1	1							1											1	5
Cyber Liability	1			1		1			1			1				1			1			1	1	1	1		11
Network security and privacy		1	1									1	1		1		1			1	1						8
Business interruption		1		1								1	1		1					1							6
Media		1	1										1		1		1				1			1			7
Legal expenses			1				1					1	1		1		1										6
Expense Reimbursement			1					1					1														3
Fines and Penalties			1												1		1										3
Breach notification to customers			1				1										1				1						4
PCI Loss												1	1														2
Credit card monitoring			1				1										1							1			4
Public relations and reputation	1		1										1		1		1										5
Forensic			1										1				1										3
Fraud Coverage					1			1					1													1	4
Third party business interruption																				1							1
Total	6	7	10	2	3	1	6	5	1	2	0	7	12	0	10	2	8	1	1	4	4	1	1	6	1	4	105

Discussion

This study aims to map the cybersecurity insurance market in the U.S. based upon the cybersecurity insurance services offered by the top U.S. insurance companies, as appear on their websites. According to the findings, the three research questions presented can be addressed.

The first research question deals with the cybersecurity insurance U.S. market size, according to the number of insurance companies offering these types of services. As presented in Table 3 ("Top U.S. Insurance Companies with Business and Cybersecurity Services") 68% (26 out of 38) of the top U.S. insurance companies discussed in this research, offer cybersecurity insurance services. Most of the reviewed literature (Eling & Schnell, 2016; Marotta et al., 2015; Marotta et al., 2017; Meland et al., 2017; Peters et al., 2018) emphasized the immaturity of the cybersecurity insurance market and the absence of these types of services. However, the fact, found in this research, that the majority of the top insurance companies offer cybersecurity services, could indicate that those firms understand the need for these services, as far as it concerns to the top U.S. insurance companies, and offering cybersecurity insurance services may be seen as the first steps towards cybersecurity insurance market maturity.

The second research question deals with the visibility of the cybersecurity insurance services at those insurance companies' websites. The level of exposure of those services on the insurance companies' websites reflects another aspect of the maturity of the cybersecurity insurance market. The research reveals (Table 4 – "Visibility and Ease to Find Cybersecurity Services") that in 50% of the reviewed U.S. insurance companies (13 out of 26) the cybersecurity insurance services were "Hard to find" (in 7 - the services were "Easy to find" and in 6 - "Relatively easy to find"). Thus, although from the first research question it can be understood that the insurance companies understand the need for cybersecurity insurance services, half of them do not proceed with the next step to make those services accessible, easy to find and user-friendly for current and potential customers. This may suggest that the covered U.S. insurance companies until now do not see the importance, uniqueness and relevance of cybersecurity insurance services. Moreover, the lack of exposure and visibility may be a sign of immaturity, because the insurance companies may be waiting for their customers to make the first step and ask for services, and then to tailor a specific solution, instead of offering publicly and promoting services designed beforehand.

The third research question deals with the main cybersecurity insurance services offered by the insurance companies. Immaturity of the U.S. cybersecurity insurance market may be revealed also when analyzing the cybersecurity insurance services offered by the reviewed insurance companies in this research. Table 5 ("Types of Cybersecurity Coverage Offered by Each Insurance Company") outline the type of cybersecurity insurance services and coverages offered by each of the 24 reviewed insurance companies, based upon the information available in each insurance company's website. This research categorized 21 types of cybersecurity coverages found in the insurance companies' websites and presented the wide diversity in the offered coverages. The findings indicate two trends that may indicate the U.S. cybersecurity insurance market lack of maturity:

1. A common use of general terms. As shown in Figure 1, the very general and obscure, but most popular, term of "cyber liability" is offered by 11 insurance companies (46%), the coverage "data breaches and data compromise" is offered by 10 insurance companies (42%). In the third place of popularity, the research found two services: "computer attacks" and "network security and privacy", with eight instances each (33%). This generality may serve the insurance companies to maintain some vagueness, blurriness and ambiguity, without defining the services specifically, or may derive due to insufficient understanding of cybersecurity insurance clients' needs.

2. The research indicated widespread diverse cybersecurity insurance services, while most of them (81%) are being provided only by only few companies. Most of the cybersecurity insurance services (17 out of 21 services, 81%) are offered by 1 to 7 insurance companies, out of 24 companies. This also may indicate the diversity of the offered cybersecurity coverage services and lack of consistency. As mentioned before, two companies offer only information, but no coverage at all. The results may reflect the early-discussed lack of maturity of the cybersecurity insurance market, as matured marketplaces are mostly more standardized.

Conclusions

The cybersecurity insurance market is developing and progressing, however, it is still immature. The reality forces the market to change and progress: The increasing number of cyberattacks and their significance to the organizations attacked leads to awareness of cybersecurity insurance services. This market will continue growing in the following years, as more incidents occur and more historical data and understanding of the consequences will be accumulated. Moreover, the needs for diverse needs will be understood, and therefore appropriate solutions and services will be developed. With the development of the cybersecurity market, the needs and services will be standardized. Consequently, the information about these services will be more visible and insurance companies will intensify their marketing efforts to these services. Moreover, the essence of the cybersecurity insurance coverage needs to be specified, detailed and categorized, to understand in-depth each service nature and the manner these offers can be compared by the customers, to choose the most relevant cybersecurity insurance services for their needs. All these will increase the competition, and leverage the market. However, until then, there will still be an invisible hole of information about cybersecurity insurance services.

Limitations and Future Research

The current research examined only the top insurance companies in the U.S. Moreover, to maintain the insurance companies' anonymity, this paper does not provide any details about the companies. Consequently, the results cannot be generalized as is for all kinds of insurance companies or other countries. Further research may examine the existence of cybersecurity insurance services by the second level of the U.S. insurance companies and by much cybersecurity niche insurance companies or by other countries' insurance companies. Furthermore, due to the findings of the reviewed literature about the immaturity of the cybersecurity insurance market, future research soon may point any progress of the market in the discussed parameters. Moreover, the aim of this paper, as explained and broadened in the introduction section, does not include the identification of risk scores or definition of customers' premium. Therefore, these issues, which are indeed very important, and insurance companies struggle to define properly, are not part of the scope of this research. Further research, with different methodology and research questions, will try to identify and define these issues.

References

Alphabetical List of Insurance Companies (n.d.). https://alphabetizer.flap.tv/lists/list-of-general-insurance-companies.php

Bandyopadhyay, T. (2012). Organizational adoption of cyber insurance instruments in IT security risk management: A modeling approach. *Proceedings of SAIS (Southern Association for Information Systems) Conference, Atlanta, GA, USA* 2012. 5.

Bandyopadhyay, T., & Mookerjee, V. (2019). A model to analyze the challenge of using cyber insurance. *Information Systems Frontiers*, *21*, 301–325. https://doi.org/10.1007/s10796-017-9737-3

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM-Scratch Programming for All*, *52*(11), 68-73.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131-158.

Bonner, M. (2019). Top 25 U.S. Property/casualty insurers. *The Balance Small Business*. https://www.thebalancesmb.com/top-u-s-property-casualty-insurers-462505

De Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 239-274. https://doi.org/10.1057/s41288-018-0082-7

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474-491.

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security*, *68*, 130-144.

Franke, U., & Meland, P. H. (2019). Demand side expectations of cyber insurance. In *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)* (pp. 1-8). IEEE.

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM), 7(1)*, 14-26.

Helms, J. (2019). Information systems security policy management: A literature review. http://jultika.oulu.fi/files/nbnfioulu-201906212604.pdf

Insurance Information Institute (2017). Top 10 life and nonlife insurance companies, United States. https://www.iii.org/table-archive/219750

Largest US insurers (2019). Business insurance. https://www.businessinsurance.com/article/20190103/NEWS06/912325916/Business-Insurance-2018-Data-Rankings-Largest-US-insurers

List of All Insurance Companies in USA (n.d.). Insurance-companies.co. http://insurance-companies.co/list-insurance-companies/#A%20summarized%20list

List of United States Insurance Companies. (n.d.). Wikipedia. https://en.wikipedia.org/wiki/List_of_United_States_insurance_companies

Marotta, A., Martinelli, F., Nanni, S., & Yautsiukhin, A. (2015). A survey on cyber-insurance. *Technical Rep. IIT TR-17/2015. Istituto di Informatica e Telematica, Consiglio Nazionale delle Richerce, Pisa*.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35-61.

Meland, P. H., Tøndel, I. A., Moe, M., & Seehusen, F. (2017). Facing uncertainty in cyber insurance policies. In *Livraga, G., Mitchell, Ch., eds., Security and trust management, Springer.* https://doi.org/10.1007/978-3-319-68063-7

Moorcraft, B. (2016). These are the top 25 property/casualty insurance companies in the US Insurance. *Business America.* https://www.insurancebusinessmag.com/us/news/breaking-news/these-are-the-top-25-propertycasualty-insurance-companies-in-the-us-32630.aspx

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11-26.

Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance. *In Fintech, Growth and Deregulation, Maurice, D., Freund, J., and Fairman, D. (eds), Chapter 12. Risk Books, London.*

Pooser, D. M., Browne, M. J., & Arkhangelska, O. (2018). Growth in the perception of cyber risk: evidence from US P&C insurers. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 208-223.

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business infosec posture using social theories. *Information & Computer Security, 24(5),* 534-556.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4), 349-356.

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, *43*(2), 417-440.

The largest P&C insurers in the United States (2018). Reinsurance news. https://www.reinsurancene.ws/top-100-u-s-property-casualty-insurance-companies/

Tøndel, I. A., Seehusen, F., Gjære, E. A., & Moe, M. E. G. (2016). Differentiating cyber risk of insurance customers: The insurance company perspective. In *International Conference on Availability, Reliability, and Security* (pp. 175-190). Springer, Cham.

Top 20 largest US insurance companies 2019 (2019). Disfold. https://disfold.com/top-us-insurance-companies/

Woods, D., & Moore, T. (2019). Does insurance have a future in governing cybersecurity? *IEEE Security and Privacy Magazine*, *18*(1), 21-27.

Authors Biographies

Tal Pavel is the Head of Cybersecurity Studies in the Information Systems Program, at The Academic College of Tel Aviv Yaffo. He specializes in cybersecurity threats and policies, holds a Ph.D. in Middle Eastern Studies from Bar-Ilan University, Israel (Dissertation: "Changes in Governmental Restrictions over the Use of Internet in Syria, Egypt, Saudi Arabia and the United Arab Emirates between the Years 2002 – 2005"). He served as a keynote speaker at international conferences. He has been interviewed as a cyber expert commentator on all major Israeli media outlets.

Ruti Gafni is the Head of the Information Systems BSc program at The Academic College of Tel Aviv Yaffo. She holds a PhD from Bar-Ilan University, Israel (in the Business Administration School), focusing on Information Systems, an M.Sc. from Tel Aviv University and a BA (Cum Laude) in Economics and Computer Science from Bar-Ilan University. She has more than 40 years of practical experience as Project Manager and Analyst of information systems.