CYBER-RISK INSURANCE — A BIG CHALLENGE FACING CONTEMPORARY ECONOMIES

Professor Leonardo Badea, Phd.[1)] și Lecturer Călin Mihai Rangu[2)]*

[1)] President, Authority of Financial Supervision, Bucharest, Romania
[2)] Director, Authority of Financial Supervision, Bucharest, Romania

Abstract

Cyber-security beyond the concept must be a product to be offered to modern society. We live in a complex world based on the digitization of products and services. Digitization also involves a complex system of associated risks. The road to the world of tomorrow goes through today's world and an analysis of the current situation in the contemporary economies about cyber risk insurance is only a first step that this article aims to achieve.

The study aims to substantiate the need to formulate and assume policies and to support the regulation of cyber risk coverage by ensuring the need to support sectoral strategies to increase the level of maturity of companies from the perspective of protection against cyber threats. There is also a need to set up a cyber-risk reporting system, at least for critical and important infrastructures, the development and use by insurers of advisory and evaluation models based on standards and certifications recognized at the level of including the development of necessary skills for insurers to engineer these risks.

Keywords: cyber risk, insurance, risk management, GDPR, underwriting, CISO, IT security, privacy, availability, data integrity, critical infrastructure, NIS, CERT

JEL Classification: D81, G22, H56, M15

* Corresponding author, **Călin RANGU** - Calin.RANGU@asfromania.ro

Introduction

Information and digital communication technology is present daily in our lives, both personal and professional, in services, in commerce, in supporting critical infrastructure, everywhere. If insurance is one of the main concepts of homogenization, by connecting everyone in a distributed network, through the Internet, we participate in a global, homogeneous network. Although this virtual network and its users are exposed to large and new risks, concrete threats that increasingly exploit the vulnerabilities of institutions, companies and individuals, the connection with the insurance has not yet been achieved and it is impetuous to achieve for the deployment a quiet digital life.

According to the Geneva Association[1] cyber risk is certainly the greatest challenge faced by modern economies. It can be defined as any risk arising from the use of information and communications technology including "deliberate attempt of some computer criminals who use the internet to use the networks of computers on which took control in order to change, to block or destroy computer systems, computer networks, data or programs stored times on them times transmitted by these"[2] . Cyber-attacks jeopardize the confidentiality, availability or integrity of any data or services. These lead to the interruption of business activities, of critical infrastructures (public services, energy, transportation, finance, etc.), affecting people and property.

The notion of cyber risk involves a multitude of risks that threaten the assets of companies, governments or individuals, losses generally including financial or non-financial assets, identities, disclosure of sensitive information, and disruption of business / operations.

Cyber risks result either from deliberate attacks (criminal, terrorist, backed by hostile states, activists, blackmail, or personal reasons), or accidental events (data deletions, service interruptions)[3].

1. Cyber threats are in a trend of growth, both in terms of the number and complexity.

According to CERT-RO report[4] on the development of cyber threats for the year 2017 cyber security alerts have increased by 25% by the year 2016, affecting 33.71% (2.89 million) unique IP addresses from Romania, of all IPs assigned to the RO. 10.32%

1 Understanding and Addressing Global Insurance Protection Gaps, Geneva Association, April 2018

2 https://wol.jw.org/ro/wol/d/r34/lp-m/102012171#h=1

3 Interview by Leonardo Badea, President of A.S.F.:
https://www.ziarulprofit.ro/index.php/semnal-de-alarma-tras-de-presedintele-asf-asigurarea-riscului-cibernetic-o-mare-provocare-cu-care-se-confrunta-economiile-moderne/

4 Raport privind evoluția amenințărilor cibernetice în 2017, CERT-RO, aprilie 2018,

(14.33 million) of processed alerts relate to computer systems compromised, meaning that they were either infected or have been operated[5] and used by attackers in different types of attacks.

Worldwide major attacks are on an accelerated growth according to Fig.1, in the first three months of 2019 thirteen major cyber-attacks were reported according to CSIS & Hackmageddon[6].

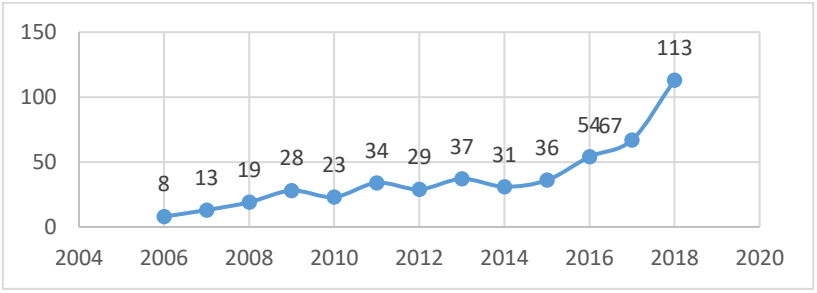

Figure no. 1. The annual evolution of the number of cyber-attacks between 2006 and 2018

Source: CSIS & Hackmageddon 2019 and its own processing

Based on the information available to the public according to the CSIS Technology Policy Program and hackmageddon.com, on cyber spying and cyberwar, excluding cybercrime, countries of origin and victims would be represented in Fig. 2. Long-term espionage campaigns have been treated as single events for the purpose of total incidents. Data is partial because some states hide incidents, while others fail to detect them.

5 Interview by Leonardo Badea, President of A.S.F.: https://www.ziarulprofit.ro/index.php/semnal-de-alarma-tras-de-presedintele-asf-asigurarea-riscului-cibernetic-o-mare-provocare-cu-care-se-confrunta-economiile-moderne/

6 https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

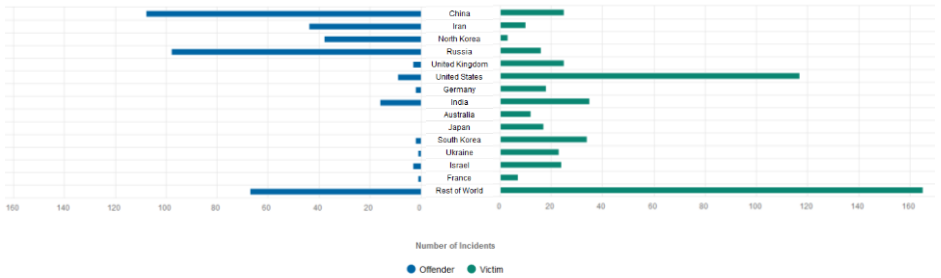

Figure no. 2. Graphic representation by country of the number of cyber-attacks and casualties, aggregated from 2006 to 2019

Source: CSIS & Hackmageddon, CSIS Technology Policy Program

Estimating the cost of cyber incidents is challenging companies avoiding to report losses. Worldwide it is estimated losses caused by cyber risks at almost 0.5 percent of world GDP and almost two times more than the average annual losses caused by natural disasters[7]. If apply it at the level of Romania shall have the same percentage of 0.5% of GDP would result in losses of about 9 billion euros.

The amount of financial losses generated by cyber risk is difficult to estimate, with a lack of information. Some cybercrime activities do not have a direct cost or cannot be quantified. The industry tries to estimate the total costs, costs per incident, and the cost of recording a data breach as shown in Table 16. Fig.3 and Fig. 4 presents estimates of the average annual cost of cybercrime per domain and major affected countries.

Table no. 1. Estimated costs of cybercrime

GLOBAL COSTS (IN BILLION USD, PER ANNUM)	
Symantec (2013)	113
McAfee (2014)	445 (375-575)
Kshetri (2010)	100-1'000

COSTS PER INCIDENT (IN MILLION USD)	
Ponemon Institute (2015)	3.8
Geschonnek *et al.* (2013)	2.1
Kaspersky Lab (2013)	2.4

COST PER RECORD (IN USD)	
Symantec (2013)	298
Ponemon Institute (2015)	217
NetDiligence (2014)	956

COSTS BY COUNTRY (IN % OF GDP; MCAFEE; 2014)	
U.S.	0.64
China	0.63
Japan	0.02
Germany	1.60

Source: Geneva Association, 2016

According to the estimates of the multinational company Accenture, in management consultancy, technology solutions and outsourcing, between 2015 and 2018, the greatest

7 Understanding and Addressing Global Insurance Protection Gaps, Geneva Association, April 2018

damage to cybercrime is recorded in the area of loss of electronically stored information (about $ 6 million in 2018), followed by business disruption (about 4 million USD in 2018), turnover losses and damage to equipment (Figure 3):

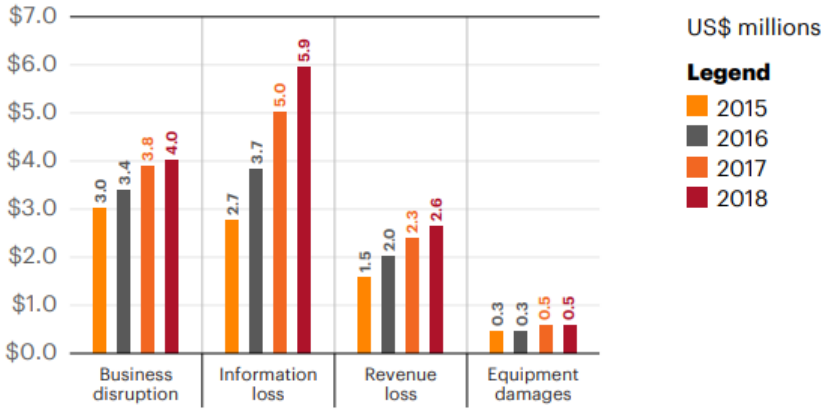

Figure no. 3. Average annual cost of cybercrime on the main loss areas

Source: Accenture, 2019

Below are the estimates of the same company, by developed countries, where the US holds the record with over 27 million USD in 2018, followed by Japan, Germany United Kingdom, etc. (Figure 4).

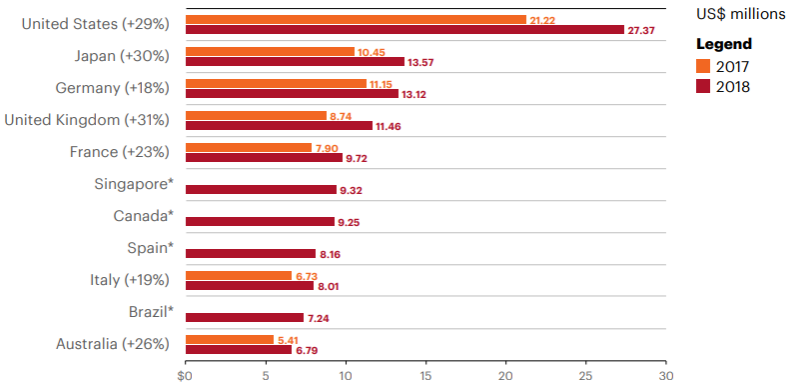

Figure no. 4. Annual average costs of cybercrime on major affected countries

Source: Accenture, 2019

Based on a risk barometer[8], conducted through interviews with 968 participants, at the level of 2019, the main causes of the cyber-related losses were established (Figure 5):

1. Business interruption
2. Loss of reputation
3. Liability claims after a data breach
4. Data restoration costs
5. Fines and penalties

Figure no. 5. The main causes of economic losses caused by cyber incidents

Source: Allianz Risk Barometer, 2019

As a result of the application of regulation costs further major GDPR, can be generated by damage to personal data.

2. The financial impact which can be covered by insurance against cyber risk[9]:

- theft of assets (financial)
- discontinuation of activities/business with revenue/turnover
- protection and compensation costs, additional costs with investigating losses, costs of communication (authorities, customers, injured) and repair.

With all these losses, the level of cyber-risk insurance is very low compared to the overall volume of the insurance market. Swiss Re expects that in 2025 (Figure 6) this volume will reach about 1% of the global insurance market.

8 Allianz Global Corporate & Specialty, Allianz Risk Barometer, 2019
9 https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

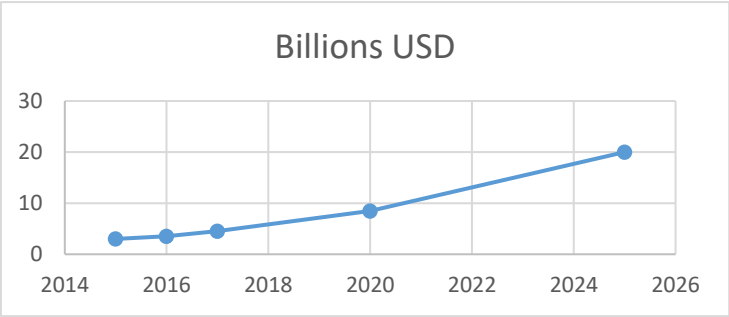

Figure no. 6. Evolution of premiums written for cyber-risk insurance

Source: Swiss Re, 2018

Similar forecasts[10] also provide statistics on world-wide subscribed cyber insurance premiums over the period 2014-2020, as shown in Fig. 7.

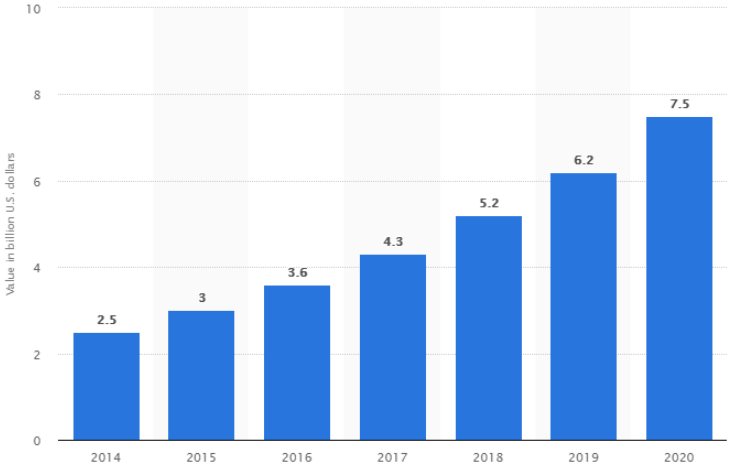

Figure no. 7. Estimated premiums for cyber-risk insurance 2014-2020 (USD billions)

Source: © Statista 2019

10 https://www.statista.com/markets/414/topic/461/insurance/

In accordance with the *Thematic analysis report relating to insurance risk cyberspace*[11] prepared by Romanian Financial Authority (A.S.F)., risks are the responsibility of the management of the institutions and companies, as well as the level of employment, insurance cybersecurity and may cover occupational hazards posed by cyber risks.

Most property insurance policies cover physical damage (even if the interruption of activity is constantly part of the commercial property) and generally excludes cyber risk. Worldwide, less than 10% of companies are considered to have purchased cyber insurance products today. We do not have information in Romania.

Insurance is a tool that complements (and does not replace) the risk management framework that each organization should have and is therefore relevant because[12]:

- Every day, organizations fight risk by focusing on the frequency (by avoiding an incident) through cyber prevention and security (CISO, CERT, etc.)
- If the attack is successful and the impact is ample, the financial consequences can be huge and political / social repercussions / political destabilization / military invasion is made easier if key infrastructures become inoperable (energy, telecommunications, banks, public administrations, transport, infrastructures etc.)
- Computer security exists to improve the resilience of organizations through financial support.

Accenture[13] in 2018 presented its own analysis of the average costs of cybercrime, noting that investments in computer security had a major positive impact (Figure 8) and the correlation between the annual cost of cybercrime and the organizational dimension of affected companies (Figure 9).

11 10 https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

13 Cost of cyber crime study, pag. 12, 17, Accenture, 2017

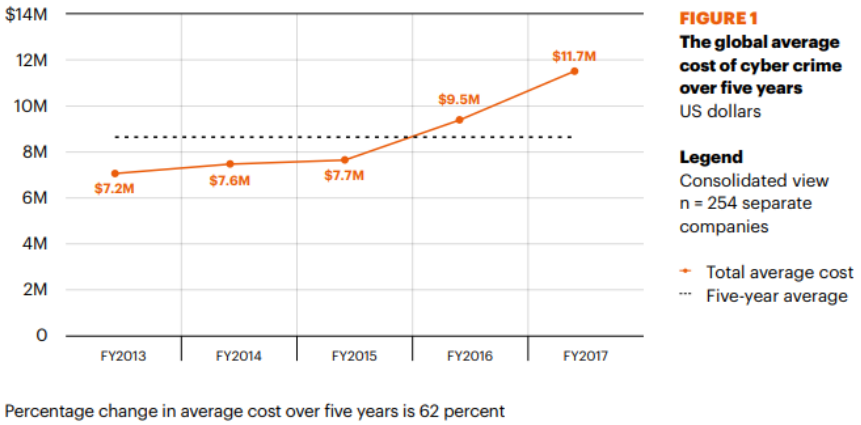

Figure no. 8. The global average cost of cybercrime over the period 2013-2017

Source: Accenture, 2018

In addition, Accenture presents in 2017 a year-on-year evolution of the annual cost of cybercrime, depending on the size of the affected US companies, with a loss of more than $ 75 million for large companies. The regression of these records indicates, on average, a peak of over USD 25 million for very large firms.

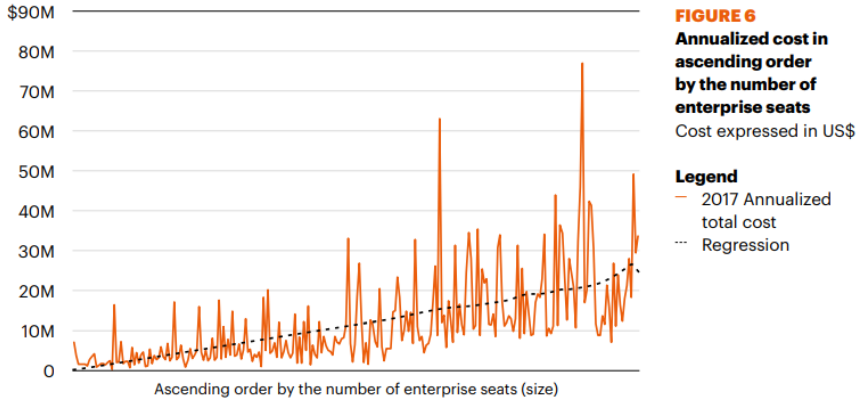

Figure no. 9. The correlation between the annual cost of cybercrime and the organizational dimension of the affected companies

Source: Accenture, 2018

3. Cyber security has three main challenges[14]:

- Lack of predictability of cyber losses. Exposures are largely unpredictable not only because of the lack of historical data in the past, but also because of the dynamics of cybercrime and the associated risks that complicate their assessment.

- Informational asymmetry. The adverse selection is almost inevitable, organizations that have taken cyber-risk insurance have experienced cyber-incidents before buying insurance. Lack of loss data affects the risk classification of policyholders.

- Coverage limits. Policies tend to cover only limited maximum losses (10-500 million USD, see Biener, Eling, Matt and Wirfs, 2015; Finkle, 2015), and contain more exclusions (eg self-loss, site access insecure or terrorism). Potential extreme scenarios (sometimes called "Cybergeddon") can not be covered by the insurance policy. In addition, the effects of cyber losses that can not be measured (for example, reputational losses and their impact on stock prices) could be indirectly not covered. Another problematic aspect of coverage is the complexity of the policy. Given the number of exclusions and the dynamic nature of cyber risk, there is uncertainty about what the cyber risk policy actually covers, uncertainty about agreed terminology, which makes insurance offers very difficult to compare.

Deloitte[15] presented the vicious circle of cyber-insurance (Figure 10) which emphasizes that the lack of historical data is probably the fundamental challenge and contributes to tightening coverage limits on cyber-insurance markets and the emergence of exclusions such as loss of access to unsafe sites or terrorism. Some indirect effects of cyber incidents cannot be measured and as a result are not covered (for example, reputational damage)[16].

14 Ten Key Questions on Cyber Risk and Cyber Risk Insurance**,** Geneva Association, nov 2016,
15 Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market, Deloitte, 2017
16 Understanding and Addressing Global Insurance Protection Gaps, Geneva Association, aprilie 2018,

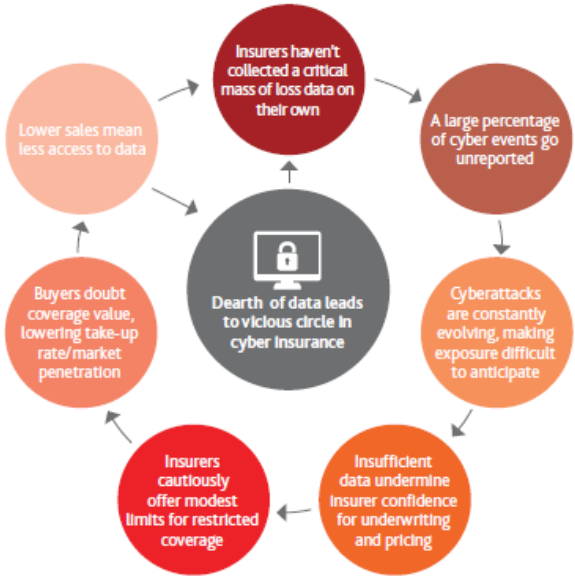

Figure no. 10. The vicious circle of cyber-insurance

Source: Deloitte, 2017

Despite all these shortcomings, global cyber-insurance products are already available globally and adapted to the client's risk profile. They allow companies to benefit from full protection against cybercrime and other cyber-incidents, indirect or external, malicious or accidental.

4. Five most important global approaches for such products would be:

1. addressing customer support with cyber insurance needs, providing loss prevention tools and services geared toward regaining stability as a result of cyber-attacks.

2. an extensive approach in the particular cases of human failure or negligence of employees, so it's not just cyber insurance business insurance, but individually. Some key areas of this coverage include damage by hackers, cyber-theft, social engineering, cyber extortion and responsibility for media online.

3. analysis of the extent to which approach a customer managing risk. This quantitative evaluation using statistical models which are then applied to the subscription

process. Recognizing a theme of organizations that focuses entirely on avoidance of violations, in general, it follows an approach that businesses want, customized according to the largest Cyber risks experiencing a specific target building a policy accordingly.

4. integrated approach with technology management clarifies that technology and, more precisely, cyber-space have created an entirely new insurance. Recognizing how technology now permeates the society, is the high level of risk that you bring this up. The approach was made to look beyond the financial protection, providing also an advisory capacity in the cyberspace. In fact, the support of experts in this field can help clients to improve safety. There are platforms that offer access to dozens of cyber risk insurers. Using this armada of assistance, are proposed also cyber insurance policies tailored to individual clients and their own risk profile.

5. the approach from the perspective of complexity of cyber threats. Protection of privacy is a central area of interest, providing coverage of repute, a crucial area due to the increase in the frequency and severity of the violations policy. Are taken into account factors such as forensic costs and costs for monitoring appropriations and expenditures.

Despite the many cyber-risk challenges, these examples prove that there are ongoing risk models and relevant datasets. New players will increase market capacity and competition will increase.

Swiss Re expects to suddenly increase global cyber-risk insurance to $ 18 billion by 2025; however, it would still be less than 1% of the global non-life insurance market. 99% of the damage caused by cyber incidents remains uninsured.

Last but not least, the fundamental issue of cyber-security can be addressed by public-private partnerships to develop a robust trade partnership from a cyber-risk perspective.

5. Ensuring cyber-related risks is an important subject for the authorities for at least the following six reasons[17]:

1. It is an element of economic, social and political stability, both for critical, governmental and commercial and personal infrastructures, including the financial sector, and should be used in assessing financial soundness / health and supporting business by recovering rapid loss and continuation of business[18]

2. Can be an element of national security (to support the activity of the specialized institutions)

17 Navigating through Cyber Risk, Thomas MARCADET, mai 2018, prezentare Marsh
18 https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

3. It is beneficial for society, as data privacy claims (ie loss of customer data by a telecom operator, healthcare system, social protection, banking and non-banking system, etc.) will have an impact on the lives of all citizens. Rapid compensation, with the financial support of an insurer, is a guarantee that these crisis-generating crises will not generate some disorder among the population for months.

4. Cyber risks cannot be eliminated as much as investing, the attackers being ahead of technical remedies. It can be financially covered by the insurance system, only a major residual risk for avoiding financial liability of institutions / companies (which may even lead to inability to pay), as well as personal, social, or even criminal.

5. Technology trends and interdependencies will bring new major cyber risks through interconnection of homes, current life through intelligent systems (IoT), artificial intelligence, robotics, etc

6. Currently rating agencies[19] and authorities demand concrete measures to eliminate cyber-related risks by requiring the application of regulations, standards, and audits that naturally complement insurance with areas where vulnerabilities cannot be technically covered. One of the most important legislative acts adopted in the field of cyber-security at European level is the European Parliament's "Network Safety and Information Systems Directive" (NIS Directive 2016/1148)[20], which sets out measures to achieve a high common level network and information security within the Union so as to improve the functioning of the internal market. This directive calls for concrete measures at the level of critical infrastructure but not only, and the rules assign responsibility to accountability and institutions / companies.

***The timing of the implementation of the directive is the following NIS*:**

August 2016	-	The entry into force of the directive
February 2017	6 months	Cooperative group commences its activities
August 2017	12 months	European Commission adopts acts implementing security and notification requirements for digital service providers
February 2018	18 months	Cooperative group work programme lays down

19 Cyber Risk And Corporate Credit – June 9, 2015, WWW.STANDARDANDPOORS.COM/RATINGSDIRECT
20 https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1479977104870&uri=CELEX:32016L1148

9 may 2018	21 months	Transposition of the directive into national law the NIS
November 2018	27 months	Member States will identify essential services operators
May 2019	33 months (1 year after transposition)	The Report Of The European Commission
May 2021	57 months (3 years from transposition)	Review by the European Commission

The evolution of cyber threats will increase in frequency and sophistication. Institutions/companies need a comprehensive cyber risk management strategy - a strategy based on economic risk modeling, optimized cyber security, robust cyber security programs and effective response capabilities that respond in a timely and effective manner, while maintaining breaks to a minimum, and returning to normal operations as quickly as possible, with the lowest costs[21].

Generally, cyber-related risks are discussed technically, with IT concepts but this topic already transcends this area and is transposed into business, social economy, mathematical and statistical modeling, data management, uncertainty theories, risk management (for example, Maillart and Sornette 2010; Biener, Eling and Wirfs, 2015). These concepts concern the field of complexity and dependency risk structures (eg, Hofmann and Ramaj, 2011; Ögüt, Raghunathan and Menon, 2011) or the field of adverse selection and moral hazard issues (eg Gordon, Loeb and Sohail, 2003), Infrastructure Critical Infrastructure (eg Economic Forum, 2010, Ruffle et al., 2014, Lloyd's, 2015b, Long Finance, 2015). Existing studies confirm challenges in risk management and cyber risk[22] .

According to the Geneva Association, through *Ten Key Questions on Cyber Risk and Cyber Risk Insurance*[23], it was found that:

- *A global fall of the Internet is unlikely, but regional bottlenecks have already occurred; given the global connection between the economy and society, we identify massive potential consequences of extreme scenarios on companies and individuals. The same is true of other cyber scenarios, such as, for example, blocking energy systems. For*

21 WannaCry: Lessons learned following ransomware attack, Jean Bayon de La Tour, Marsh
22 https://www.stiripesurse.ro/asigurarea-riscului-cibernetic-o-mare-provocare-cu-care-se-confrunta-economiile-moderne_1270359.html
23 Ten Key Questions on Cyber Risk and Cyber Risk Insurance**,** Geneva Association, may 2016

insurers, such scenarios represent an accumulation risk that may inhibit overall insurance if hybrid analysis methods are not applied.

- *The Cyber Insurance market is currently low compared to other business lines, but is expected to grow significantly in the coming years. The United States is ahead of Europe and Asia, for example, with regard to reporting requirements. The main problems of extending these insurances are lack of data, risk of change, accumulation risk and potential problems caused by moral hazard.*

- *Data on cyber risk is very low, as victims are reluctant to report such events. Most empirical cyber risk papers are based on data loss data (not loss of information), but recently the first loss-making databases (NetDiligence (2014) in the USA, Biener et al. (2015) global level).*

- *The insurance industry should: develop common standards, taxonomies and good practices; to develop scenario analyzes; initiate and / or intensify dialogue with stakeholders; (cloud computing, Internet of Things, blockchain, etc.), to increase their own analytical skills (digital forensics) and to make their own IT more resilient, to specifically support cyber-security either by developing anonymous databases) ensuring and developing new policies, either by setting up new models and approaches based on advice and evaluation*

- *Modeling the frequency and severity of cyber risk can be done by applying the extreme values theory and approaching the peaks above the limit. Distributions, power law or log-normal distribution for severity and negative binomial distribution for frequency were proposed. Aggregation of cyber risk must take into account nonlinear dependence. Scenario analysis is a popular tool in such situations.*

- *In order to prevent cyber-related risks, the fight against cybercrime needs to be stepped up by international collaboration, to initiate global dialogues and conventions aimed at limiting cyber warfare, stimulate the resilience of IT systems, introduce reporting requirements, support the development of databases with cyber incidents and the development of minimum standards for risk mitigation.*

- *To support cyber-security, it is recommended to establish public-private partnerships with the government as the ultimate insurer (government assurance for extreme scenarios); to stimulate the development of anonymized databases, to stimulate the development of traditional and alternative risk transfer mechanisms*

However, Maillart and Sornette (2010) investigated violations of personal data such as credit cards, social security numbers, bank accounts, or medical records. They find an exponential increase in the frequency of these incidents (the rate of events) for the period 2001-2006 (Figure 11). Regarding the distribution function illustrated in Figure 11, the violet points are the remarks before 2006, and the blue points observations after that date.

While violations of personal data are just a type of cyber risk, the authors argue that these findings are representative of other types of cyber-related risks come from the Internet[24].

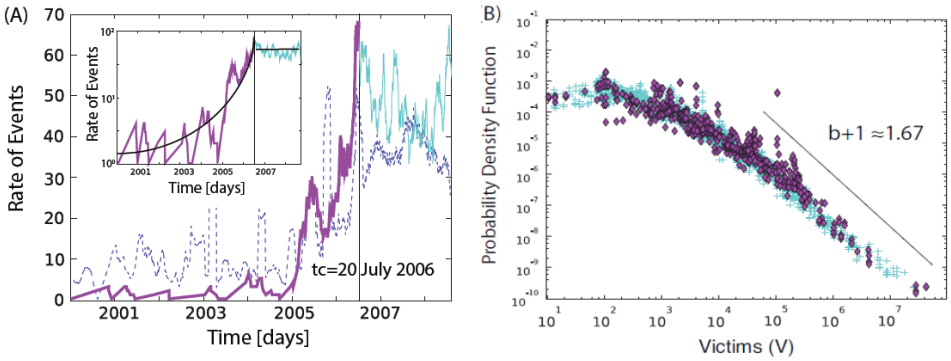

Figure no. 11. Distribution of severity and frequency

Source: Maillart and Sornette, 2010

Research into cyber-risk insurance includes two aspects according to the Geneva Association[25]:

- Micro perspective: demand-side research (eg risk perception, fatalism); analyzing the assurance and ways to improve the assurance (in particular empirical research, eg data generation, data analysis); the analysis of the optimal risk management (mitigation vs insurance) and the need for the capital needed to cover the cyber risks.

- Macro Perspective: scenario analyzes for measuring and managing the accumulation risk, if insurance companies can record a systemic risk with cyber risk, the actors involved become part of the global dialogue. In the absence of data, analyzes should be made more technically than statistical.

Especially for insurance purposes, a simple number of violations is not sufficient for the calculation of premiums, capital or capital reserves. Instead, a price indicator corresponding to the potential claim must be allocated to each breach of security.

24 National Vulnerability Database (by NIST)- Collects software vulnerabilities for the U.S., used by Maillart and Sornette; 2010

25 Understanding and Addressing Global Insurance Protection Gaps, Geneva Association, April 2018

Finally, classical risk measures based on mean and variance are not applicable and the merits of diversification may disappear due to infinite moments that characterize cyber risks (see Chavez-Demoulin et al., 2006).

6. Cyber-risk must be managed from several perspectives.

The classic risk management process consists of five steps:

1. defining objectives,
2. identification of risks,
3. evaluation / analysis,
4. effective risk management (avoidance, attenuation, transfer, retention)
5. risk monitoring.

The NIST agency of the US proposes the work framework described in Figure 12.

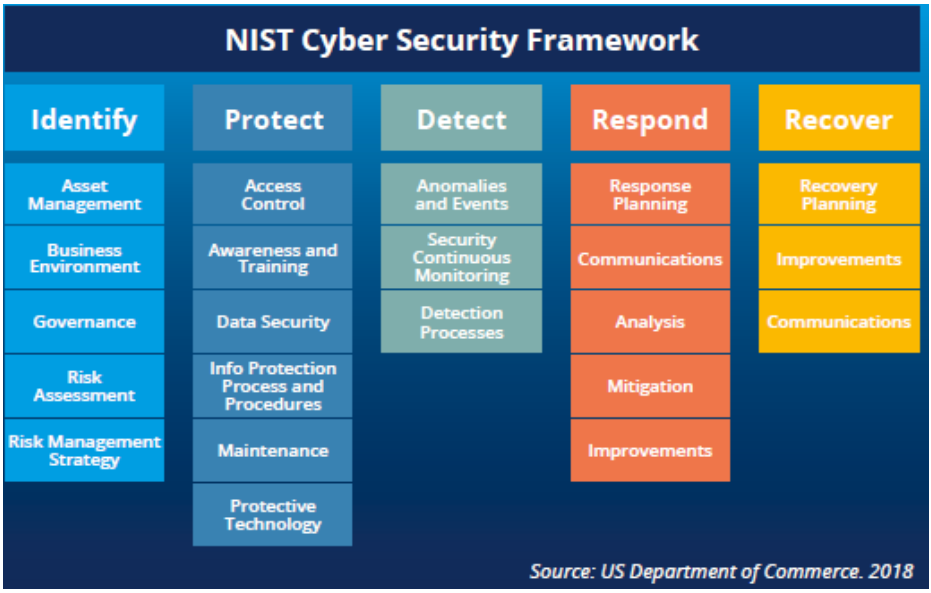

Figure no. 12. The framework of cyber security

Source: US Department of Commerce, 2018

At each stage of the classical risk management process, cyber risks have special features, for example, cyber-risk management is not the responsibility of the IT department, but there is a need for a company-wide dialogue on this risk (eg awareness, training, etc.).

The subject should also be embedded in the top-level C level leadership responsibilities[26].

Already institutional commitment - demonstrated by designating a person responsible for information security - is essential for successful risk management. For example, companies that already have a computer security officer (CISO) or a similar position have a lower average of events when the risk occurs, with a loss of $ 157 / record vs. $ 236 / record for firms without this position (see Shackelford, 2012).

Accenture[27] (2019) establishes a hierarchy of the main four cyber-defense activities (Figure 13).

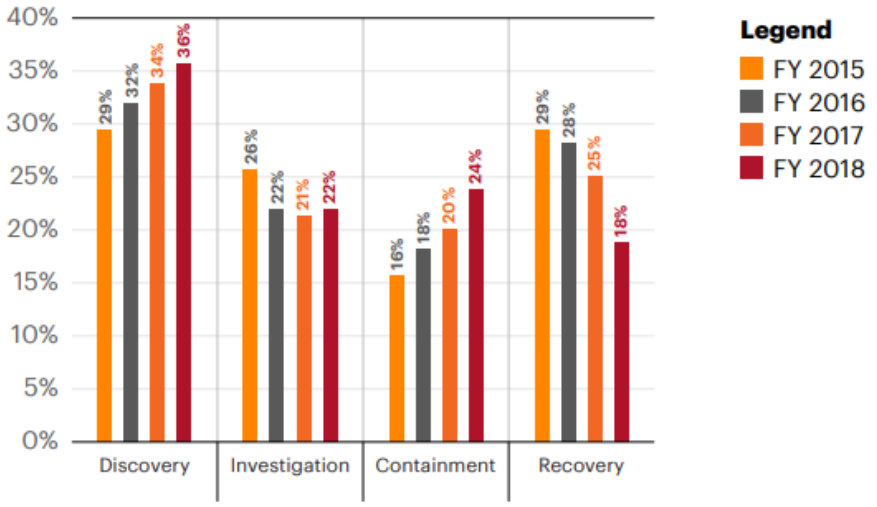

Figure no. 13. The share of four defense against cyber risks

Source: Accenture, 2019

The first step in the risk management process is to define the initial situation and objectives of cyber risk management. Until now, there are a number of standards,

26 The step down of Target's CEO following a massive data breach in 2014 exemplifies that the top management might be held accountable for cyber incidents (http://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-andcanadian- debacle/#799cf7283f56).
27 Cost of cyber crime study, pag. 30, Accenture, 2017

especially in the field of information technology, which can serve as cyber-risk management templates, for example the ISO / IEC 2700x family, BSI-IT-Grundschutz (BSI, 2008) or Cyber Security Best Practices (Allianz, 2011). There is also the possibility to certify compliance with these standards. For example, U.K.'s Department for Business, Innovation & Skills and Office (2014) defines an IT security standard and certification of its implementation in the so-called Cyber Essentials.

Business partners and customers are increasingly asking companies to verify that they meet certain minimum IT security standards. For cyber insurance, insurers should rely on similar assessments. Companies requiring cyber-cover would need to have such certificates and the insurer should carry out a similar risk assessment[28]. Insurers will have to enter the pre-assessment consulting area to estimate cyber risks and policy issuance.

To this end, for risk identification:

- Business processes that are relevant to cyber risk with their assets and their value must be established. After that, the potential threats, their type and sources must be determined. A detailed list of current threats can be found in ISO / IEC 27005.

- We need to collect data on weaknesses, always in connection with existing assets, threats and protection methods. A first potential indicator for risk identification can be provided by cyber-risk self-assessment; for example, methods proposed by companies specializing in the distribution of such insurance[29]. These tools can help determine exposure to risk and awareness of company risk and provide guidance on unidentified risks. Another aspect would be how a cyber-attack can be detected as soon as possible from when it happened. An instrument for analyzing the consequences on operations is Business Impact Analysis (BIA).

There are four options for effective risk management:

a) avoiding risks,
b) risk mitigation / attenuation,
c) risk transfer
d) self-insurance.

Avoiding risks would mean that electronic storage of information and restriction of the use of information systems. In today's world, this is hard to imagine. Risk reduction and attenuation are more effective. These are tools to reduce the likelihood of occurrence (eg anti-virus software, firewalls, etc.) or to reduce the size of losses (eg disaster recovery plans).

In general, the risk transfer is possible by purchasing an insurance contract. However, the cyber insurance market is growing, the product range will grow and sufficient coverage

28 ACGS (2014) analyses cyber risk management with the Business Model Canvas and the House of IT Quality.
29 http://www.marsh-stresstest.eu/.

will become viable. The combination of mitigation / mitigation and risk transfer is particularly important. An insurer will issue the policy if adequate measures are in place to mitigate / mitigate risks and the insurer has been able to verify the effectiveness of these instruments in their initial assessments. Therefore, advance assessments and interviews, or advice given directly by the insurer, are necessary before signing an insurance contract. These assessments will also contribute to raising cyber risk awareness.

In the case of self-insurance, the company decides to pay the losses on its own. In this case, the company's capital must serve as a buffer and must be allocated in advance. In addition to capital accumulation, emergency plans and crisis management must be established.

We can get the following cyber risk management guidelines by companies (see also Biener, Eling, Matt and Wirfs, 2015): institutional commitment, effective crisis management, risk dialogue with all employees, customer risk dialogue, and suppliers, certification, continuous monitoring, risk transfer by insurance as the only effective means of transferring cyber risk.

7. The risks identified must be covered by cyber-insurance coverage or not by explicit exclusions.

In general, the risks covered by the insurance of companies registered in Romania, according to the A.S.F.[30] on cyber risk insurance are:

- Liability for leakage of information, including loss of personal data collected;
- Leakage related costs including forensic notification and forensic analysis costs;
- Responsibility for network security for compromised systems, including DOS attacks;
- Media responsibility for digital publications;
- Business interruption caused by a computer incident;
- Costs of restoring data and applications resulting from an incident likely to affect the business operation;
- Crisis communication to reduce reputational risk;
- Liability for electronic payments, including fines and penalties;
- The losses generated by the theft of intellectual property.

The main exclusions from insurance are generally:

- Self-inflicted losses;
- Acts of terrorism;

30 https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

- Others: Violation of professional obligations; Deficiencies of service providers; Patent or commercial secret; Hacking committed by executives or partners Destruction of property; Personal Injury; Seizure and confiscation; War, terrorism and nuclear risks; Defamatory statements; Insolvency; Pre-existing problems; Abusive and criminal acts; Irresponsible conduct; Claims for employee liability accountability; Fines, penalties and penalties; Claims for damages outside the competent courts.

In the case of an insured event, the response rate of the insurance company may be 4 hours from the event notification.

Table no. 2 show different examples of international cyber-risk coverage in response to the different stages of cyber-attack or data losses, from FERMA (Federation of European Risk Management Association) perspectives[31].

Table no. 2 Coverage of cyber-risk insurance for attacks and data loss

Possible actions following a cyber attack or data loss	Examples of cyber coverage components
Investigate what happened	These issues likely require the specialised assistance of forensic investigators. Cyber policies may include coverage for forensic investigation costs following a cyber-attack or data loss.
Deploy technical measures to contain the loss and repair the IT system	
Assess legal/regulatory obligations	Legal services/assistance can be covered by cyber policies for breaches where it is reasonably suspected that confidential information has been compromised, generally in two forms: (i) post incident discovery and assistance in managing a breach (ii) defence costs following a claim alleging a breach of information
Execute a plan to comply with your obligations	
Assess the complaints/legal challenges you receive	
Implement the emergency plan to continue servicing clients	Cyber policies may include coverage for costs incurred as a result of a cybersecurity breach to maintain or restore operations and for income that is lost during the outage period.
Assess the cost of the cyber-attack, including possible loss of turnover	
If you are facing extortion: - Hire a response/threat consultant - Pay ransom, if legally allowed	Cyber policies may include services and costs to investigate and manage an extortion threat, including forensic experts and threat consultants.
If you are facing a regulatory investigation or a legal suit from third parties: - Hire legal advisers; prepare defence strategy - Pay damages	Cyber policies may include coverage for defence costs and damages that are agreed and/or assessed.

Source: FERMA 2018

31 Preparing for Cyber insurance, FERMA, Octombrie 2018

Conclusions

The thematic analysis of A.S.F.[32] related to cyber-risk insurance, have observed:

- Cyber-related risks are the responsibility of institution, company management, and employees, cyber-insurance can also cover the professional risks generated by cyber-related risks.
- Institutions / companies need a comprehensive cyber risk management strategy ensuring return to normal operations as soon as possible with the lowest possible cost.
- Cyber-risk insurance can play a key role in taking over / transferring the risks to which companies are exposed. It can be a tool that complements (and does not replace) the risk management framework that each organization should have and should be an element of economic and social stability for both critical, governmental and governmental infrastructures commercial and personal, including the financial sector.
- Cyber-risk insurance should be used in assessing financial solidity / health and sustaining activity by rapidly recovering losses and continuing to work.

In view of the above, in order to achieve the coverage and the risks posed by the digital society, the following conclusions can be drawn:

- To support the protection of critical infrastructures, public sector activities, the good functioning of the economy and the protection of national and individual assets, with a major exposure to risks in the context of the current digital world, it is essential to formulate and adopt policies and support regulation of cyber- insurance, with the relocation of financial responsibility to those who can pay very large damages by reducing the political, social and economic impact. These policies will have beneficial effects both at the level of demand[33] and supply.
- In order to ensure the necessary data series for insurers' actuarial activity on a long-term basis, it is necessary to establish a system for reporting the losses caused by cyber risks, at least for critical and important infrastructures,
- In order to ensure the development of specific insurance products in the short-medium term, it is necessary to develop and use by the insurers models of consulting and evaluation for clients wishing to assure against cyber threats based on recognized standards and certifications in the world, and the development of the necessary skills at the level of insurers regarding the engineering of these risks.
- Cyber-related risks call for a common front of beneficiaries, technology companies and insurers to increase cyber maturity and cyber security, apply risk management principles, implement joint mechanisms to fight cybercrime and develop products customer-specific insurance.

32 https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

33 Interview by Leonardo Badea, President of A.S.F.:
https://www.ziarulprofit.ro/index.php/semnal-de-alarma-tras-de-presedintele-asf-asigurarea-riscului-cibernetic-o-mare-provocare-cu-care-se-confrunta-economiile-moderne/

Bibliography:

[1] Geneva Association - Understanding and Addressing Global Insurance Protection Gaps, aprilie 2018;

[2] CERT-RO - Raport privind evoluția amenințărilor cibernetice în 2017, aprilie 2018;

[3] Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market, Deloitte, 2017

[4] WannaCry: Lessons learned following ransomware attack, Jean Bayon de La Tour, Marsh;

[5] Thomas MARCADET - Navigating through Cyber Risk, , mai 2018, prezentare Marsh;

[6] www.standardandpoors.com - Cyber Risk And Corporate Credit – June 9, 2015,;

[7] ACGS (2014)- Analyses cyber risk management with the Business Model Canvas and the House of IT Quality;

[8] Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, nov 2016,

[9] Navigating through Cyber Risk, Thomas MARCADET, mai 2018, prezentare Marsh

[10] Cyber Risk And Corporate Credit – June 9, 2015, WWW.STANDARDANDPOORS.COM/RATINGSDIRECT

[11] The step down of Target's CEO following a massive data breach in 2014 exemplifies that the top management might be held accountable for cyber incidents (http://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-andcanadian-debacle/#799cf7283f56).

[12] ACGS (2014) analyses cyber risk management with the Business Model Canvas and the House of IT Quality.

[13] http://www.marsh-stresstest.eu/.

[14] CIS (2016) or ASD (2014) for guidance on how IT security measures, such as access control, authorisation of devices and software, malware defense, and network configuration, should be used.

[15] National Vulnerability Database (by NIST), USA- Collects software vulnerabilities for the U.S., used by Maillart and Sornette; 2010

[16] Cost of cyber crime study, pag. 12, 17, 30, Accenture, 2017

[17] Preparing for Cyber insurance(ppt), FERMA, Octombrie 2018

[18] https://wol.jw.org/ro/wol/d/r34/lp-m/102012171#h=1

[19] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf

[20] Interview by Leonardo Badea, President of A.S.F.: https://www.ziarulprofit.ro/index.php/semnal-de-alarma-tras-de-presedintele-asf-asigurarea-riscului-cibernetic-o-mare-provocare-cu-care-se-confrunta-economiile-moderne/

[21] https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1479977104870&uri=CELEX:32016L1148

[22] https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

[23] https://www.statista.com/markets/414/topic/461/insurance/