IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

MARKET CONDUCT SUPERVISION DIRECTORATE
PRODUCT SUPERVISION DIVISION

Survey on policies against cyber risk

October 2023

1. Foreword and *executive summary*

IVASS carried out a survey to investigate insurance policies against cyber risk, referred to as "cyber policies", offered by insurance companies to protect individuals/households (retail customers) and Small and Medium-sized Enterprises (SMEs).

The survey draws on the increasing exposure to cyber risk due to several factors, including: the spread of new technologies and increasing digital interconnection between things, people, processes and data; the use of the internet for social relations purposes or for online purchases and sales or to use home banking services; the increase in cyber attacks, including as a result of geopolitical tensions linked to the conflict in Ukraine. These factors make users - households, businesses and public authorities - increasingly vulnerable in terms of cyber security.

The survey was based on the analysis of contracts and does not enter into the assessment of the goodness or convenience of the policies and disregards their commercial success and of the level of premium income associated with them. The reference to policies or commercial initiatives mentioned in this Report does not imply an approval by IVASS.

Cyber risk is the combination of the probability of cyber incidents occurring and their impact, whereby a cyber incident is defined as a breach of the computer security of an IT system or of the information that the system processes, stores or transmits, irrespective of whether it is the result of malicious or unintentional activity[1].

In particular, cyber risk may arise from incidents involving the breach, loss or dissemination of sensitive data, of a personal but also financial nature, fraud and extortion, cyberbullying/cyberstalking, identity theft, damage to image or reputation, fraud on e-commerce purchases or sales, credit and debit card cloning, and so forth.

For companies, cyber risk can in turn generate operational and legal risks for business interruption, regulatory violations, extortion demands (ransomware), etc.

The main evidence from the survey suggests the growing popularity of cyber policies, particularly for SMEs and, to a lesser extent at present, for individuals and households.

[1] Definitions from the **Cyber** *Lexicon FSB:* https://www.fsb.org/wp-content/uploads/P130423-3.pdf

The covers for SMEs are quite articulated, with guarantees that aim to cover companies against damage caused by cyber attacks, as well as damage caused to third parties as a result of the attacks, and legal costs. Several policies offer ancillary services before the occurrence of a cyber attack (identification of vulnerabilities, implementation of protective measures) and in post-event management (restoration of IT operations, management of reputational damage, etc.).

The covers are currently mostly standardised: in the future they could benefit from greater flexibility, so as to better calibrate and customise guarantees according to the specific operations and coverage needs of companies.

The policies for individuals and households cover losses resulting from theft or cloning of credit or debit cards and prepaid cards, digital identity theft, and fraudulent online purchases. Often, telephone and digital assistance is provided to the individual and their household through an online monitoring service that, in the event of a suspected cyber attack on the insured's devices, allows the company to contact a specialised technician to activate all analysis and recovery procedures. There is also cover in the form of psychological counselling following traumatic events related to cyber-attacks such as cyberbullying and cyberstalking, and assistance in case of fraud when booking a trip abroad online.

For both types, this is a market set to grow rapidly, in parallel with the strengthening of the IT security culture among companies and individuals. The assistance of professional insurance intermediaries, who are well versed in cyber risks and the very technical aspects of these policies, is crucial for the further development of the offer.

The analysis also showed that:

- some companies require specific operating conditions of the person or company to be insured, as prerequisites or conditions to make the risk insurable and, consequently, the cover effectively operational (see Section 3.1.2 and Section 3.2.6);
- there are sometimes exclusions and deductibles that reduce their scope and applicability, even with margins of ambiguity. For example, the exclusion clause in the event of “war”, which is present in most of the contracts examined, does not make explicit whether the term “war” also includes “cyber war”, which is particularly topical, given that

today's wars also take place through cyber attacks (see, in particular, Section 3.1.4 and Section 3.1.5);

- glossaries have room for improvement in terms of comprehensiveness and unambiguousness of the terms used (see Chapter 4);

2. Scope of the analysis

The analysis looked at **50 insurance policies** for cyber risk protection for individuals, households and SMEs offered on the market on 30 July 2023 of the following types:

- **stand-alone**, i.e. policies specifically designed to cover cyber risk;
- **modular**, i.e. policies offering a wide range of guarantees for the customer, covering the person or property, organised in modules that can be variously combined and that have optional cyber covers, to be purchased in conjunction with other guarantees.

To perform the analysis, the information sets of contracts with cyber coverage on the companies' websites were examined.

The sample analysed consists in particular of:

a) 26 policies aimed at SMEs:

- **14** stand alone policies;
- **12** modular policies;

b) 24 policies aimed at individuals and households:

- **6** stand alone policies;
- **18** modular policies.

3. Type of cyber policies

3.1 Stand alone cyber policies for SMEs

The stand-alone cyber policies for SMEs aim to protect the assets of the insured (entrepreneur, legal entity, professional or trader) against the expenses and damages directly suffered or caused to third parties as a result of an attack on the company's computer system.

These policies provide cover for the expenses and work required to restore data and the computer system, as well as compensation claimed from the insured by third parties to whom it has caused damage and legal protection for disputes arising from the cyber attack.

The **14** policies examined are standardised, providing basic cover to which optional covers can often be added. These can be purchased separately and offer increasing protection depending on the number of covers added to the basic cover.

Most stand-alone policies are aimed at small and medium-sized enterprises carrying out production activities (including craft activities) in the manufacturing or services sector (including IT services), commercial establishments, professional offices, and accommodation facilities. The policy premium is often related to turnover.

There are only five policies dedicated to large companies.

3.1.1 Coverages (with specific exclusions and limitations of the guarantee)

All benefits presuppose the occurrence of a cyber attack on the insured company's computer system. The main guarantees are set out in more detail below, also highlighting the specific exclusions and limitations of the individual guarantee.

3.1.1.1 *Financial loss*

Guarantees for **financial losses** compensate direct losses incurred by the insured for the restoration of data and computer systems following a cyber attack and the costs incurred for interruption to business resulting from the same events.

These basic guarantees **are often supplemented by covers relating to**: investigation costs to ascertain the causes and modalities of the attack; costs of notifying third parties of the consequences of a cyber attack, e.g. the compromise of systems followed by the disclosure of sensitive data of third parties in the custody of the insured (data breach); costs incurred in re-issuing credit/debit or prepaid cards (PCI-DSS certifications - *Payment Card Industry Data Security Standard*[2]); recognition of a daily allowance for each day of forced inactivity; costs for expert advice in dealing with cyber attacks suffered.

Two companies also insure damage to computer equipment used by the insured, eight companies insure damage resulting from cyber extortion or attempted cyber extortion by providing compensation for expenses incurred (data restoration, malware removal), while reimbursement of expenses incurred for ransom payments as a result of cyber extortion is generally excluded.

[2] The **PCI-DSS** (*Payment Card Industry Data Security Standard*) certification serves to ensure the protection of card holder data and specifies precise requirements for procedures, network architecture and software that companies handling credit card numbers must meet. Compliance with the PCI DSS is a requirement for all operators storing, processing or transmitting credit card data.

- *Specific Exclusions and Limitations of the Guarantee:*
  - absence of antivirus or updates for more than 6 months or exclusive use of freeware antiviruses;
  - wilful misconduct of the insured's employees;
  - use of default credentials not changed by the insured;
  - failure of external networks or power failures of public utilities;
  - acts of war and terrorism;
  - damage by explosion or emission of heat or radiation;
  - damage during attacks with chemical, biological, biochemical or electromagnetic weapons;
  - damage due to discharge/dispersal/infiltration/leakage of hazardous substances, contaminants or pollutants;
  - damages from theft, infringement or disclosure of intellectual property;
  - extortion of any kind (except for policies that also cover this event);
  - damage due to ransomware, demands for ransom (except for policies that also cover this event);
  - the costs of restoring/recovering/reinstalling or reconstituting electronic data or software or repairing/renting or replacing a computer system or one of its components.

3.1.1.2 *General liability*

With regard to **general liability** coverage, the guarantees offered by most companies cover compensation for damage caused to third parties by a cyber attack that causes a breach of privacy on confidential data and computer security in general.

Some companies **insure other cases**, such as liability for reputational damage to the third party concerned, violations of intellectual property, costs incurred for the intervention of experts aimed at containing or eliminating the damage, costs incurred by the third party for business interruption, sanctions/fines for non-compliance with administrative obligations and financial damage and damage to the image for failure to notify other interested parties of the cyber attack suffered by the insured, financial losses caused to third parties by

inadequate technical solutions adopted by the insured for the use of Advanced Electronic Signature (Firma Elettronica Avanzata - FEA) in institutional, corporate or commercial relations.

- *Specific Exclusions and Limitations of the Guarantee:*
  - damages arising from contractual liability;
  - damage resulting from publications on websites not controlled by the insured;
  - liability not resulting from the law;
  - damage resulting from failure to remove content from websites under the control of the insured, following a report or claim by a third party.

3.1.1.3 *Legal expenses*

With respect to the coverage of **legal expenses**, the insurance company reimburses legal expenses in connection with litigation involving the insured in the defence of its interests.

The covers offered mainly concern legal protection for non-contractual damages suffered due to the tortious acts of third parties and damages caused to third parties due to malicious, negligent or misdemeanour crimes related to the use of the web and social media in the course of business or professional activity.

In many cases, coverage of legal expenses in the relevant fora is also accompanied by legal advice by telephone from legal experts.

In some cases, the following guarantees are included: legal disputes with providers of IT services, such as e-mail, software, internet connection, website management, etc; fraudulent use by third parties of credit cards and the like belonging to the insured; recourse to the Banking and Financial Arbitrator, etc.

The survey showed that cover for legal expenses is less extensive and residual than that for financial losses and general liability, and often merely a few basic guarantees are provided to the insured, which only in some cases offer the client the possibility of supplementing them with ancillary guarantees. Moreover, in some cases, these types of cover are only offered on condition that the guarantees for financial loss and/or general liability are purchased.

It was also noted that claims are often outsourced to operations centres of insurance companies specialising in legal expenses insurance.

➢ Specific Exclusions and Limitations of the Guarantee:

- enforcement costs;
- costs of the mediation body, if mediation is not compulsory;
- legal fees not agreed with the company;
- damage caused by fraudulent use of the insured's digital identity;
- breach of contract by the insured;
- punitive damages;
- fines, penalties and tax charges.

3.1.1.4 Insurance cover for demands for ransom

The cyber threat landscape is witnessing an increasing spread of ransomware[3].

Ransomware spreads through a user's installation of an 'exe' file. In most cases, the installation of these files occurs inadvertently, through clickjacking[4] or as a consequence of a phishing attack[5]: once installed, this particular type of malware[6] prevents users from accessing data residing on the "infected" computer by encrypting its contents. Once inside the network, ransomware may also have the ability to spread to other vulnerable systems silently and autonomously. Following a ransomware attack, cybercriminals ask the victim to pay a ransom, by a certain date, usually using cryptocurrencies (such as Bitcoin), to decrypt data or prevent data deletion.

Ransomware can also be used to publicly disseminate confidential data on the network, such as personal information on individuals or the disclosure of trade secrets.

[3] *Ransomware:* malware used for the purpose of extortion by damaging or altering the system and/or the information contained in it (e.g. data encryption), thus enabling the attacker to demand a ransom to restore normal operation.
[4] *Clickjacking* is a fraudulent computer technique. During normal web browsing, the user clicks with a mouse pointer on an object (e.g. a link), but in reality this click is redirected, without the user's knowledge, to another object, which can lead to the most varied consequences, from simply sending spam, to downloading a file, to ordering products from e-commerce sites.
[5] *Phishing*: a digital form of social engineering performed through electronic communication (usually e-mail) and impersonating a trusted entity with the aim of acquiring personal or confidential information from the victim.
[6] *Malware*: any malicious software or code designed to gain unlawful access to and/or disrupt the operation of the computer system.

Two foreign companies operating in Italy cover the financial losses to the company resulting from ransom demands following a ransomware attack. A company offers a cyber policy with a guarantee against cyber-attacks for extortion purposes, with coverage for losses resulting from a threat that includes the sums paid by the insured as ransom to make the extortion cease, as well as compensation for expenses incurred in using specialised cyber extortion consultants. Cover is provided by the company on condition that the underwriting of the policy is kept confidential and that prompt notice is given to the authorities of the threat of extortion.

3.1.2 Insurability requirements

In order to be able to insure against cyber risk, insurance companies require minimum insurability requirements from companies and, in particular, that they have implemented preventive security measures. In this way, for various types of cyber attacks, the company is able to assess the possible reaction of the insured company on the basis of risk analysis, the technology adopted, the security safeguards and the digital training of security managers and employees.

Below are the main insurability requirements found in the policies:

- presence of appropriate IT safeguards to prevent/counter cyber attacks;
- installation and frequent updating of appropriate antivirus and firewall systems;
- performance of regular and frequent backups of computer systems;
- adequate internet connection to allow remote technical repairs;
- adequate organisational safeguards for the correct and conscious management of IT risks, such as procedures, existence of dedicated internal or external structures for the supervision of IT functions, continuous digital training of personnel, etc;
- the signing and maintenance of a technical assistance and maintenance contract for both hardware and software throughout the whole life of the policy.

3.1.3 Claims-made formula and retroactivity

The survey showed that in many cyber policies the guarantees operate on a “claims made” basis, i.e. the insurance cover applies to claims reported for the first time during the

policy period, even if they occurred earlier, or during the posthumous reporting period[7], if provided for in the contract.

It also emerged that in other cases, in addition to “basic” cover for claims occurring during the validity of the policy, the customer is offered the possibility of benefiting, as an ancillary guarantee (Top/Premium/Full), from a “retroactive” period of the policy's effectiveness, which also covers claims occurred before the policy was taken out. In such cases, cover is also valid for claims for compensation submitted to the insured for the first time during the policy period, provided that the insured's negligent conduct occurred during the policy period or not before the retroactive period specified in the policy. The date specified in the policy as the "retroactive date" represents the date before which an insured event is not covered by the insurance.

3.1.4 Exclusions common to all guarantees

The analysis shows that typical exclusions of insurance contracts are applied to a large extent, as well as **specific exclusions for cyber risk**, some of which have the effect of limiting guarantees, with reference in particular to:

- the general clause relating to wars, uprisings, insurrections, etc., bearing in mind that cyber attacks may increasingly arise from war or terrorist events. In some cases companies expressly exclude the applicability of cover in the event of “cyber war”, in other cases the provision refers generically to “war”. The glossary in the appendix to the contract does not always contain an explicit definition of what is meant by “war” or “cyber war";
- clause aimed at excluding business interruptions of electrical, IT, etc. infrastructure provided for in almost all the policies examined in respect of damages - not indemnifiable - arising from breakdowns, interruptions, unavailability of communication systems, internet service, electricity supply and other external infrastructure not under the control of the insured.

It also emerged that the conditions that for some companies constitute the impossibility of insuring cyber risk (see Section 3.1.2 on insurability conditions), for others represent causes of exclusion or limitation of guarantees. Examples include:

[7] In fact, some policies also provide for a posthumous claim reporting period, i.e. a period of grace, sometimes also referred to as a “posthumous guarantee”, which extends the time period within which a claim can be reported.

- failure to have adequate IT tools to prevent/counter any cyber attacks;
- failure to install adequate antivirus systems or to update them regularly;
- failure to install appropriate firewall systems;
- failure to perform regular and frequent backups of computer systems;
- the use of default credentials for access, not customised by users;
- the non-compensation of any ransom paid by the insured victim of a cyber extortion attempt, even when the main event (ransomware) is insured;
- in some cases, costs for damage to the hardware used are expressly excluded; however, damage to the business software(s) used is indemnifiable.

3.1.5 Territorial limits, deductibles, maximum amounts of cover and waiting periods

Certain territorial limits were noted depending on the guarantees provided. In particular:

- the guarantee "Financial loss due to damage to the company's computer system": it covers damage to the computer system located in Italy, the Republic of San Marino, and the Vatican City. Support services are provided remotely, by means of tele-connection throughout the EU; the possible physical intervention of an operator is guaranteed only in Italy;
- "General Liability" guarantee: some policies cover claims arising worldwide, while other policies provide coverage for claims arising from breaches of privacy and/or breaches of security committed by the insured in EU territories and/or brought before an Italian judicial authority and/or concerning decisions rendered by foreign judicial authorities and recognised in Italy;
- "Legal expenses" guarantee: It applies in all European states, in case of disputes for non-contractual damages and criminal proceedings; in the EU, Switzerland, Liechtenstein, Monaco, Norway, Andorra, Vatican City, Republic of San Marino, for disputes of a contractual nature; in Italy, the Vatican City, the Republic of San Marino, for administrative cases and for legal advice by telephone.

Cyber policies dedicated to SMEs have fixed deductibles, which are deducted from the indemnity, and time deductibles, which correspond to the number of days of business interruption established in the contract, after which the right to indemnity accrues.

Maximum amounts of cover are set per single claim or per maximum indemnifiable amount in the reference year.

Some cyber policy guarantees, such as Legal Protection or Business Interruption, have contractual waiting periods[8] of up to 90 days.

3.2 Stand-alone cyber policies for individuals and households

There were fewer stand-alone policies for retail customers, individuals and households than the corresponding policies for SMEs.

In the policies for individuals, whose cover can often be extended to the entire household, the most common guarantees concern, as for companies, **financial loss** (direct damage to the insured), **general third party liability**, **legal expenses** for disputes arising from the insured event, and personal **assistance**.

3.2.1 *Financial loss*

As regards the coverage relating to financial losses of individuals and households, it covers direct losses to the insured and, if applicable, his or her household, as a result of theft or cloning of credit/debit cards and prepaid cards, digital identity theft, and fraudulent online purchases.

3.2.2 *General liability*

With regard to liability cover, the guarantees offered concern the indemnification of the expenses that the insured is required to pay, by way of compensation, for financial and non-financial damage involuntarily caused to third parties as a result of a cyber attack.

In several cases, the basic guarantee may be supplemented with other covers, such as indemnification for damage resulting from the improper use of copyright and/or copyright-protected material, improper publication of content causing damage to the image of third parties, violation of privacy or dissemination of personal data of third parties, provided that this occurs through the use of electronic devices and computer networks.

3.2.3 *Legal expenses*

With regard to legal protection, the covers offered do not differ from those already examined for SME products.

[8] The initial period, starting from the validity date of the contract, during which the claim is not covered.

3.2.4 *Assistance*

In these policies, **psychological, telephone and digital assistance** is often provided to the individual and his or her family through an online monitoring service which, based on the prior registration of the insured on a digital platform, sends an alert in the event of a suspected cyber attack on his or her devices. In this way, the company's organisational structure is immediately informed and promptly contacts a specialised technician to activate all analysis and restoration procedures.

There are covers for personal assistance, including in the form of **psychological counselling** following traumatic events related to cyber attacks, such as **digital identity theft, cyberbullying and cyberstalking** (for more details, see Section 3.2.5), and the assistance provided in connection with fraud in the online booking of a trip abroad.

3.2.5 *Cyberbullying/cyberstalking*

Within policies aimed at retail customers, companies often offer specific cover to protect individuals and families in case they suffer **episodes of cyberbullying/cyberstalking; often the same cover also operates in cases of harassment and revenge porn.**

The cover is provided in the form of assistance to the person/family unit for the reimbursement of expenses incurred in obtaining psychological support due to the occurrence of situations of discomfort or psychophysical stress resulting from episodes of cyberbullying, cyberstalking, harassment through computer supports, etc.

In some cases, in addition to the reimbursement of medical expenses for psychological support, the insured is also offered IT support, in the form of assistance, from IT experts, to eliminate/reduce the effects of the attack suffered, e.g. by removing offensive or reputational content from the web, carrying out in-depth diagnoses of the manner and consequences of the attack suffered, etc.

In other cases, the insured is also offered coverage for the legal expenses incurred in filing an **application for the shutdown of websites/social media pages** in accordance with the law or to apply to the Personal Data Protection Authority.

In most cases, the various forms of assistance guaranteed to the insured are outsourced to specialised operators.

In the case of the most widespread cover, that relating to the reimbursement of medical expenses, the insured is always required to report the claim within a certain period of time from the occurrence of the attack and according to codified procedures. The insured person is at all times required to produce medical documentation proving the need for psychological support. In addition, maximum amounts of cover are always envisaged for the reimbursement of expenses incurred, per number of claims and/or per amount reimbursed. In some cases, companies expressly exclude from the scope of cover cases of pre-existing psychiatric conditions, alcohol abuse, psychotropic drugs, and non-therapeutic use of narcotics and hallucinogens.

3.2.6 Insurability requirements

Among the insurability requirements in products for retail customers, an internet connection (usually at least 2 Mbps download, 0.80 Mbps upload) is required, since most policies, in the event of the introduction of malware, provide for technical interventions to restore the computer system of the insured or his/her household through remote assistance.

Some companies stipulate that the operation of the guarantee is also conditional on the following requirements: a) that the equipment used by the insured person is exclusively notebook or desktop computers and is not used exclusively for professional/commercial/craft activities, thus excluding tablets/smartphones and external memories; b) that home or mobile digital devices are provided with open source software and a regular licence; c) that the equipment and devices no longer benefit from the manufacturer's warranty and that they are CE certified; d) that the insured carries out data backups, periodic checks for the presence of unauthorised programmes, has adopted programmes protecting against threats or malicious events, and has also updated the data recovery programme; e) that the computer operates in a Microsoft Windows, Apple MacOS or GNU/Linux environment.

3.3 Modular policies with cyber cover for SMEs, individuals and households

Several policies covering cyber risk, aimed at retail customers and SMEs, are offered to the public in the form of modules that can be added to other policies covering the person/company or assets (modular policies).

Generally speaking, these are policies in which cyber coverage is limited in scope.

Modular policies are mostly aimed at individuals but can be extended to the household, and contain optional cyber cover by purchasing Legal expenses, Assistance and Third Party Liability. These are flexible and customisable policies in which there are assistance services for the insured, such as telephone and psychological counselling following traumatic events related to cyber-attacks or following episodes of cyberbullying and cyberstalking. Recently, this cover has also been included in Land vehicle insurance.

With regard to e-commerce purchases, many policies expressly exclude claims arising from the purchase of a wide range of goods, which are usually listed in detail in cyber policies, and which, among others, include jewellery, precious goods, and art objects purchased through online auctions; money and financial instruments of various kinds, motor vehicles/craft, perishable goods such as food and drink, weapons or medicines; animals and plants.

In the policies aimed at SMEs, the most common cover relates to legal expenses for disputes relating to damage suffered due to the unlawful acts of third parties and to damage caused to third parties due to wilful, negligent or misdemeanour offences related to the use of the web and social media in the course of business, to disputes with IT service providers, and to disputes relating to the fraudulent use by third parties of credit cards and similar cards owned by the insured. Coverage is also provided in the form of assistance for the recovery of computer data and the restoration of computer systems damaged by the attack (whereas in the corresponding stand-alone policies, compensation for financial losses associated with the same event is also offered).

Some policies include third-party liability coverage, especially in the event of damage to third-party computer systems, theft, loss or unauthorised disclosure of third-party computer data, and reputational damage.

The survey also revealed that coverage for cyber events directly or indirectly related to the main insured event is also present within the scope of land vehicle policies: in particular, a modular policy covering damage to the vehicle has been found that also provides cover for cyber attacks, which, however, by virtue of the exclusions provided for[9], in fact covers only the recovery of car keys.

[9] Cyber cover only operates for cyberterrorism if the “Sociopolitical Events” module is expressly purchased.

Some foreign companies active in the global market are starting to develop customised modular cyber policies for SMEs. In one case a flexible modular policy is also offered in Italy that covers cyber risk only and gives the policyholder (SME) the possibility of choosing from the various policy modules the cover best suited to the company's protection needs.

3.4 Multi-risk policies with cyber cover for SMEs, individuals and households

The analysis showed that there are numerous multi-risk policies with optional sections, dedicated to retail customers and SMEs, that meet the needs of protecting the insured's (owner or tenant or SME) assets and property, where cyber cover is present in the Legal Protection and Assistance guarantees.

The features of these policies, both with regard to the cover offered and to exclusions and limitations, deductibles and maximum amounts of cover, do not differ from those illustrated for the other types of policies.

4. Glossaries

Checks on the Glossaries of cyber policies revealed a lack of consistency in the technical definitions of terms related to cyber risk.

By way of example, the term "**data**" in some glossaries is defined in detail as "any digital information, present in the insured's computer system and stored outside random access memory (RAM), regardless of the form or manner in which it is used or displayed (e.g. text, images, video, software)"; in another glossary, "data" is generically understood as "electronic data and software".

Even in the case of the term "**cyber attack**", differences were found in the definitions provided in the glossaries. In one case, for example, the *"cyber attack*" is briefly identified as a "*malicious act, malware, theft against the insured's computer system";* in another case, it is defined as "*an unlawful act committed deliberately by a person who, by using the system and/or network resources of the insured, causes consequences with regard to the confidentiality, availability or integrity of data and the computer system". Going into details: 1) unauthorised acquisition, access, disclosure or misappropriation of data and/or personal data that are in the charge, custody or control of the insured or third parties under a contract with the insured; 2) unauthorised access to or use of the insured's computer system, loss, alteration, corruption or damage to programmes, applications or data and/or personal data*

on the insured's computer systems; 3) infection and corruption of the insured's computer system through the use of malicious programmes; 4) transmission of harmful programmes from the insured's computer system to third parties; 5) DoS (Denial of Service) attack; 6) computer extortion".

In other cases, glossaries do not provide an exhaustive definition of certain terms (as in the case of the definition of the term “war”, which especially in a cyber policy should also include “cyber war”, or of “malware”, “ransomware” or “sensitive data”, “data theft”, or "phishing')[10].

5. Conclusions

A snapshot of the Italian insurance market of cyber policies that emerges from the analysis brings with it some considerations on the prospects of their evolution towards consumer centricity.

The refinement and granularity of the target market, an issue that is generally of primary importance for all insurance products, is also crucial for cyber policies, which are, at present, standardised.

Policies could be more flexible and tailored to the actual and specific needs of the customer/consumer, also paying more attention to profiling and the degree of exposure to cyber risk: for example, a small business that does not operate via e-commerce will have a different cyber risk profile than one that also sells products online.

Recognition of the customer's operations is important in order to be able to offer a policy in line with and appropriate to his or her “digital” profile, his or her specific operations in that world, and thus, his or her exposure to cyber risk.

These policies could also benefit from a revision of exclusions, which should also take into account the granularity and actual needs of the reference target market.

A single glossary for definitions should be adopted to ensure homogeneity and certainty: in this regard, companies could refer to the ***Cyber Lexicon FSB[11],*** which offers a set of established and accepted definitions in the digital community.

[10] See. par. 3.1.1.4

[11] https://www.fsb.org/wp-content/uploads/P130423-3.pdf

Adequate training and updating of the distribution network on cyber policies is also important, in view of the technical complexity that these policies can have and the insurability requirements involved.

On the corporate side, it is important that businesses assess their specific risks and consult with a professional insurance intermediary to determine the appropriate level of IT coverage needed. Factors such as the nature of the business, volume of sensitive data, dependence on technology and industry regulations should be taken into account when assessing the need for and extent of cyber insurance cover. It is also important to discuss and verify aspects of insurability requirements and exclusions.