Cyberinsurance—The Challenge of Transferring Failure in a Digital, Globalized World

Jeimy J. Cano, Ph.D., COBIT Foundation, CFE, is a research member of the Information Technology, Telecommunications, Electronic Commerce Studies Group (GECTI) of the Law School and a distinguished professor at Universidad de los Andes, Colombia.

Disponible también en español *(www.isaca.org/currentissue)*

As organizations enter the international context and leverage their IT operations, their visibility increases, which, in turn, increases exposure to threats with a global scope. Since information is one of the most valuable assets of an interconnected and dynamic reality, it becomes necessary to understand the requirements and responsibilities that companies acquire when operating in a scenario in which the value-generation model, reputation and relationships with stakeholders are at risk.

In this situation, organizations, as part of their due diligence, progress in the exercise of their risk management and undertake it with the required seriousness. Risk management establishes the general framework for the activities and decisions enterprises make for progressing amid instabilities and troubled times in the business sector. A risk management strategy should take international implications into consideration, as these affect the prospects and projections of their boards of directors (BoDs).

Reports of information security breaches and unauthorized actions on organizations' IT infrastructures have increased. This demonstrates a trend of an increased number of people or groups acting with the goal of drawing attention to particular aspects of the reality of a country or region; these can be financially motivated as well. Unconventional breaches that stress and weaken organizations' technological facilities are used, revealing the need for greater attention to the security and control of operations.

With this understanding, the actions and strategies of companies to make their digital activity more resistant become visible to cyberattackers. Unauthorized third parties seek not only to create fear, uncertainty and doubt in business executives, but also to obtain control of key information, which may be used for commercial purposes, extortion, intelligence or military action. As a result, corporations become strategic targets of national and regional interests.

And, in turn, a new stage of strategic risk management within companies has begun—one in which the composition of a global, digital and political view outlines the reality of cyberrisk.

The term "cyber" requires understanding that organizations not only represent the interests of the company in a business community but are also incorporated in the dynamics of globalization, within which business interests are manifested. In a globalized world, organizations may be affected by countries that contribute to influencing and defining the geopolitical scenario of all nations. Enterprises also obtain a fluidity of movement due to the high interconnectivity and intensive use of information and communication technologies (ICTs) that allow transactions and relationships based on a digital economy that serves emerging communities around the world.

Cyberinsurance is a way to account for cyberrisk and considers the new possible business responsibilities arising from operating in an international context. Presenting cyberinsurance as a coverage option is not designed to compensate for organizations' negligence of fulfilling the duty of protecting their information and technological infrastructure.

BASIC CONCEPTS OF INSURANCE

Insurance generally operates as a compensation strategy for specific situations involving third-party interests. In this sense, a contract or agreement between the parties—the insurer and the insured—is established. Aspects such as insurable risk, the conditional obligation of the insurer and the premium are reviewed to establish the framework of action and the required guarantee, which is based on the principle of good faith that prevails in this relationship.

Insurable risk is "a fortuitous event, that due to being sudden and unforeseen, does not have, in its origin and its development, any relationship with conscious human action, whether the consequence is voluntary or not."[1] As can be seen, that which is insured is a condition of exception not subject to deliberate actions by individuals and protects the insured party against the consequences of such events.

It is important to note that there is uninsurable risk associated with fraud (i.e., a voluntary act, intentionally harmful conduct). Certain events (i.e., events that will certainly occur), impossible events (i.e., events that will certainly never occur), past events (i.e., events that occurred and were beyond the initially established scope), events of unique provision of the insured party, and events related to criminal sanctions of an economic nature are uninsurable. These events have no effect on the coverages or payments made, since they are not insured.

The insurable interest shall be understood from the point of view of damage insurance as an economic relationship that links the insured party with an object. While the insurable interest is the subject of insurance contracts, it is necessary to remember that "several insurable interests can converge on the same object on behalf of the same person or different persons...with the condition that the compensation, if the event does indeed occur, may not exceed the total value of the object at the time of the incident."[2]

The conditional obligation of the insurer is applicable when the incident occurs (i.e., when the required condition is fulfilled), at which time the beneficiary may proceed to exercise his/her right that the insurer pay the agreed-upon amount. Conditionality provides two key elements: enforceability and delay. Enforceability indicates when the obligation is no longer pending (the instant when the incident occurs), and this depends on the terms of the agreed compensation. In addition, delay (the preexistence of a formal claim in compliance with the basic evidentiary burdens, the existence of the incident and the amount) indicates that if the claim has not been answered by the insurer within one month, it enters default along with its purposes, interests or compensation for damages.[3]

Finally the premium, as an essential element of an insurance contract, is the onerous element that transfers the risk to the insurer. Technically, it is the result of a rate, expressed in percentage terms, on the insured value. The premium involves four key factors:[4]

- The actual cost of the transfer of risk (risk premium—statistical analysis of the probability of occurrence)
- The cost of administration (includes the cost of reinsurance)
- The cost of intermediation (payment of commission to intermediaries)
- The expected profit

These fundamental concepts of insurance are the basis for reviewing the new conditions of companies' responsibility in the context of cybersecurity.

ARISING RESPONSIBILITIES OF COMPANIES IN THE 21ST CENTURY

As enterprises compete in highly digitized scenarios and with greater involvement of third parties in their operations, the most valuable information of the enterprise depends on correct processing by users who have access to it. This calls for a series of security and control practices that must be validated and guaranteed by each of the parties in the application of the information life cycle.

> "The most valuable information of the enterprise depends on correct processing by users who have access to it."

If the preceding is correct, the risk of loss and/or leakage of information becomes a critical concern for organizations, given that the occurrence of this risk exposes organizations to possible loss of reputation, customers, competitive advantage and markets, in addition to fines, reparatory actions and regulatory sanctions. These entail costs and compensations that, without the proper preparation and prevention, may compromise the viability of the company in the short and long term.[5]

Information has become the new natural resource of the 21st century as it facilitates a world in constant movement, generally shared among different actors. It carries with it risk that must be identified and addressed for the purpose of driving preventive actions that anticipate potential negative impacts due to improper processing. This implies expressing

due diligence and guaranteeing a minimum standard, which should involve the duty of care of individuals, predictability in adverse situations in the processing of information, a standard of due care in information security and a set of reasonable precautions that demonstrate a proactive attitude toward damages that may arise.[6]

Many of the causes of information security breaches are unexpected; however, some of the most common ones identified in the normal operation of companies are:[7]

- Lost or stolen laptops or mobile devices
- Unauthorized transfer of data to universal serial bus (USB) devices
- Inappropriate categorization or classification of sensitive information
- Theft of data by employees or third parties
- Printing and copying of sensitive data by employees
- Insufficient response to intrusions or security breaches
- Unintentional transmission of sensitive data
- Use of weak and/or known passwords
- Conversations in public spaces regarding sensitive data
- Unauthorized monitoring of communications

Due to these causes, a new series of corporate responsibilities is necessary regarding the processing of information associated with computer processes and interactions (whether operated by the company or third parties) to mobilize the value-generation model of the company. This means understanding that in the race for cost efficiency, ICT will play a fundamental role, since by increasing the level of automation, enterprises will become more agile and efficient. However, this dependence will open organizations to previously identified vulnerabilities and security and control failures.

In risk management, there are different approaches to risk: accept, mitigate and transfer. Organizations understand the sensitivity of this subject relative to the protection of their interests and keep it in mind during relevant activities. Consequently, organizations define processing plans that include human, procedural and technological aspects that seek to close the possible identified breaches and reduce the analyzed exposure level. Enterprises also define insurance as a form of risk transfer that requires, from the insured party, systematic and effective practices regarding data protection.

Nevertheless, the impacts of information security incidents—some identified and others emerging—may not be included in the risk analysis. The consequences of these incidents may have onerous and compensatory implications that compromise the best predictions of companies in their strategies for mitigation or transfer of such risk. Therefore, the digital life of enterprises requires reviewing risk transfer proposals to build a more accurate view of this reality and to overcome traditional insurance conditions in this area, such as errors or omissions in the provision of technology services, violation of intellectual property rights, losses due to theft through transactional electronic systems, and computer crime.[8]

UNDERSTANDING CYBERINSURANCE

To date, insurance policies, defined as documents containing the insurance contract,[9] have multiple classifications and names for specifically establishing their scope and limitations. In the case of cyberinsurance, policies for identification of risk classify it as “all-risk” and “named-risk.” While the former is directed at covering the insurable interest of any risk other than those excluded by contract or those that are legally insured by express agreement (agreed with the insurer), the latter intends to cover the insurable interest of the defined risk.[10]

This traditional system, from the standpoint of the insured party, takes on the customary difficulties of understanding the contractual identification of risk associated with a basic definition of it and one or more exclusion clauses.[11] Exclusion clauses are defined as circumstances in which the risk, as it is defined, is not covered by option of the insurer. In this context, cyberinsurance is at a crossroads between the insurer, the proposed coverages and the defined exclusions, addressing the needs, demands and requirements of the insured party. This is because the complexity of cyberrisk involves an understanding of human procedural, technological and legal variables in which the interaction provides a scenario of consequences that depends on each particular case.

However, the coverage of cyberinsurance contains aspects similar to all-risk insurance policies such as:[12]

- Overall responsibility for crime through the Internet
- Property (data are not considered property)
- Errors and omissions
- Professional liability
- Liability of directors and officials
- Employment practices liability (actions of employees)
- Business interruption
- Extortion and kidnapping
- Personnel group liability (key personnel)

- Life coverage of key personnel
- Media liability coverage
- Fidelity and crime liability
- Network security coverage
- Intellectual property
- Patent insurance
- Workplace violence coverage

The coverages established by the main cyberinsurance brokers are associated with property and theft, as well as liability.[13] **Figure 1** provides a summary of typical coverage.

Figure 1—Coverages Offered By the Largest Cyberinsurance Brokers

	Coverage
Property and theft	Destruction of information or software
	Recovery from viruses or other malicious codes
	Business interruption
	Denial of service
	Information theft
	Cybernetic extortion
	Losses due to terrorist acts
Liability	Network security
	Harm to electronic media or contents
	Private confidentiality breach

Source: Garcia, K.; "Propuesta de póliza de seguro para el ciber-riesgo en Guatemala," undergraduate thesis, Universidad de San Carlos de Guatemala, 2009, p. 70, *http://biblioteca.usac.edu.gt/tesis/08/08_0420_CS.pdf*

Recent cyberinsurance studies reflect a substantial evolution of the analyzed coverages, which reflects a greater understanding of the complexity exhibited by cyberrisk. A recent study concludes that cyberattacks can be seen as one of the most serious economic and national security challenges faced by governments and organizations globally.[14] With this understanding, the study details the risk factors associated with this challenge:

- Legal liability
- Information security breaches
- Privacy breaches
- Cybertheft
- Cyberespionage
- Cyberextortion
- Cyberterrorism
- Loss of profit
- Recovery of costs
- Reputational damage
- Business continuity/supply chain disruptions
- Cyberthreats to the nation's critical infrastructure

Based on that risk, the study outlines some specific coverage, including aspects such as:

- Data privacy
- Breaches in regulations, fines and penalties
- Interruption of business networks
- Damage to data and cyberextortion
- Crisis management and response to identity theft (includes costs of forensic investigations)

In addition, research specialized in these matters indicates that the insurance market presents an asymmetry of information between the insured party and the insurer, particularly focusing on potential primary losses (e.g., direct loss of information or data, suspension of operations) and less on secondary losses (e.g., indirect loss, decrease of reputation, good name, consumer confidence, strategic strength, loss of customers). When incidents occur, the claims processes will be estimated by the economic valuations represented in the company's operating conditions (primary losses), leaving secondary losses to subjective valuations based on experiences and comparisons with equivalent processes. This creates an imbalance of protection that sometimes favors the insurer and other times the insured party.[15, 16]

> "Cyberinsurance is emerging to prevent the extent and spread of an incident and bear the payment for repair, replacement or reconstruction of the goods affected by the occurrence of the cyberrisk."

It can be concluded that cyberinsurance is emerging to prevent the extent and spread of an incident and bear the payment for repair, replacement or reconstruction of the goods affected by the occurrence of the cyberrisk.

The negotiation implicit to this type of policy is associated with exclusions. Exclusions are circumstances or events that are excluded from the insured coverage and are clearly stated in the insurance policy. These exceptions are usually associated with the previously presented noninsurable risk, including, for example, the obsolescence of the insured asset; inexcusable negligence or defective execution of the

maintenance necessary for the proper operation of the insured interest; and damages to the insured party or third parties as the result of a commercial, industrial or professional activity other than that stated in the policy.[17]

Exclusions respond to the requirement for management to guarantee the insured interest, which in the case of cyberrisk implies a systemic view of the risk in the context of the organization. That is, this view contains an understanding of the relationships of the organization from its business position, its relationships with communities and stakeholders, and the government and management of information technology, in order to understand the interconnectivity that arises in this practice.

Likewise, information security plays a fundamental role in cyberinsurance because the insurer demands an understanding of the information as a strategic asset that serves as the basis for the company's internal and external relationships, as well as the shared responsibility for its management and control with the involved third parties. Third parties also acquire the category of coresponsible parties in this scenario and must also commit to good practices, meaning they will cooperate in preventing cyberrisk by the contracting company.

CONCLUSIONS

The BoDs of organizations must include cyberrisk considerations in their review of the strategic risk of companies. To ignore this interpretation of the current business dynamics (the consequences of which are evident in multiple international cases such as those of Target, JPMorgan Chase, Sony and Office Depot, among others) is to anticipate crisis scenarios that are generally unknown and whose processing requires specialized and coordinated actions to mitigate their harmful effects.

In this practice, board members must not only become familiar with these new realities,[18] generally manifested in large failures and security breaches, but also understand the levels of preparation that the organization has regarding similar situations. It is necessary to establish the required preventive mechanisms and extended protection covering aspects that may be relevant and that current actions only cover partially.

Cyberinsurance appears as an option to consider every time security and control practices are required for companies to limit the effects of massive and coordinated attacks—some for extortionary purposes or cyberespionage—that can compromise the strategic information assets of the company, the identity of their personnel or business strategies, and that can even affect a nation's critical infrastructure operations. Along these lines, cyberinsurance comprises a critical interpretation of the intangible assets of the company in the scenario of an operation that is digitized and deeply integrated in its dynamics and has global visibility.

Cyberinsurance introduces an understanding of relationships in the digital ecosystem in order to comprehend the thresholds of permissible loss of value. This promotes consideration of the object that defines the maximum loss estimated by an organization, given a defined resilience profile that comprises a series of company activities.

The greater the understanding of the organizational culture of information security, the availability of recovery and continuity capabilities, the knowledge of emerging vulnerabilities of the business, and the characterization of the possible attackers, the better the company's preparation and response to cyberrisk will be.

The cyberinsurance world will continue to evolve according to the challenges and demands of the market and the results of introducing disruptive and nontraditional technologies. It is necessary to know the impacts of the inevitability of failure to understand the coverages and exclusions being proposed by insurance contracts, while insurance companies are beginning to accompany organizations, acting as vigilant entities for information technology, communications management and information processing.

ENDNOTES

1 Ordonez, A.; *Elementos esenciales, partes y carácter indemnizatorio del contrato*, Insurance law lesson no. 2, Universidad Externado de Colombia, Bogota, Colombia, 2002, p. 10

2 *Ibid*., p. 32-33

3 *Ibid*., p. 48-51

4 *Ibid*., p. 42

5 Ernst & Young, *Data Loss Prevention. Keep Your Sensitive Data Out of the Public Domain. Insights on Governance, Risk and Compliance*, October 2011, *www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf*

6 Triump, I.; "Confronting the Legal Liabilities of IT Systems," *EDPACS: The EDP Audit, Control, and Security Newsletter*, 46(2), 2012, p. 11-16

[7] *Op cit* Ernst & Young, p. 6

[8] Garcia, K.; "Propuesta de póliza de seguro para el ciber-riesgo en Guatemala," undergraduate thesis, Universidad de San Carlos de Guatemala, 2009, *http://biblioteca.usac.edu.gt/tesis/08/08_0420_CS.pdf*

[9] Ramirez, E.; Specialization in Insurance course, Universidad Externado de Colombia

[10] *Ibid*.

[11] Ordonez, A.; *Cuestiones generales y caracteres del contrato*, Insurance law lesson No. 1, Universidad Externado de Colombia, Bogota, Colombia, 2001

[12] Drouin, D.; "Cyber Risk Insurance: A Discourse and Preparatory Guide," GIAC Security Essentials Certification, 2004, *www.sans.org/reading-room/whitepapers/legal/cyber-risk-insurance-1412*

[13] *Op cit* Garcia

[14] Carpenter, Guy; *Ahead of the Curve: Understanding Emerging Risk*, 2014, *www.guycarp.com/content/dam/guycarp/en/documents/dynamic-content/AheadoftheCurve-UnderstandingEmergingRisks.pdf*

[15] Ordonez, A.; *Las obligaciones y cargas de las partes en el contrato de seguro y la inoperancia del contrato de seguro*, Insurance law lesson No. 3, Universidad Externado de Colombia, Bogota, Colombia, 2004

[16] Bandyopadhyay, T.; V. Mookerjee; R. Rao; "Why IT Managers Don't Go for Cyber-insurance Products," *Communications of ACM*, 52(11), November 2009, p. 68-73

[17] Generali Seguros; "Generali negocio seguro. Condiciones generales y condiciones generales específicas," *http://62.97.131.36/rep_documentos/phogar/GENERALI-CCGG-COMERCIOS.pdf*

[18] Rai, S.; *Cybersecurity: What the Board of Directors Needs to Ask*, ISACA-IIA, 2014, *www.theiia.org/bookstore/downloads/freetoall/5036.dl_GRC%20Cyber%20Security%20Research%20Report.pdf*