International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:14, No:1, 2020

CybeRisk Management in Banks: An Italian Case Study

E. Cenderelli, E. Bruno, G. Iacoviello, A. Lazzini

***Abstract*—**The financial sector is exposed to the risk of cyber-attacks like any other industrial sector. Furthermore, the topic of CybeRisk (cyber risk) has become particularly relevant given that Information Technology (IT) attacks have increased drastically in recent years, and cannot be stopped by single organizations requiring a response at international and national level. IT risk is never a matter purely for the IT manager, although he clearly plays a key role. A bank's risk management function requires a thorough understanding of the evolving risks as well as the tools and practical techniques available to address them. Upon the request of European and national legislation regarding CybeRisk in the financial system, banks are therefore called upon to strengthen the operational model for CybeRisk management. This will require an important change with a more intense collaboration with the structures that deal with information security for the development of an ad hoc system for the evaluation and control of this type of risk. The aim of the work is to propose a framework for the management and control of CybeRisk that will bridge the gap in the literature regarding the understanding and consideration of CybeRisk as an integral part of business management. The IT function has a strong relevance in the management of CybeRisk, which is perceived mainly as operational risk, but with a positive tendency on the part of risk management to the identification of CybeRisk assessment methods that are increasingly complete, quantitative and able to better describe the possible impacts on the business. The paper provides answers to the research questions: Is it possible to define a CybeRisk governance structure able to support the comparison between risk and security? How can the relationships between IT assets be integrated into a cyberisk assessment framework to guarantee a system of protection and risks control? From a methodological point of view, this research uses a case study approach. The choice of "Monte dei Paschi di Siena" was determined by the specific features of one of Italy's biggest lenders. It is chosen to use an intensive research strategy: an in-depth study of reality. The case study methodology is an empirical approach to explore a complex and current phenomenon that develops over time. The use of cases has also the advantage of allowing the deepening of aspects concerning the "how" and "why" of contemporary events, on which the scholar has little control. The research bases on quantitative data and qualitative information obtained through semi-structured interviews of an open-ended nature and questionnaires to directors, members of the audit committee, risk, IT and compliance managers, and those responsible for internal audit function and anti-money laundering. The added value of the paper can be seen in the development of a framework based on a mapping of IT assets from which it is possible to identify their relationships for purposes of a more effective management and control of cyber risk.**

E. Cenderelli is with Department of Economics and Management, University of Pisa, Italy and with Monte dei Paschi di Siena, Italy (e-mail: elena.cenderelli@unipi.it).

E. Bruno and G. Iacoviello are with Department of Economics and Management, University of Pisa, Italy (e-mail: elena.bruno@unipi.it, giuseppina.iacoviello@unipi.it).

A. Lazzini is with Department of Communication & Economics, University of Modena and Reggio Emilia, Italy (e-mail: arianna.lazzini@unimore.it).

***Keywords*—**Bank, CybeRisk, information technology, risk management.

I. Introduction

WITH the rapid evolution of information and communication technologies, information systems have assumed a central importance in the organizational and functional structure of all kinds of business. In this context, the implementation of information systems capable of managing a plurality of information types coming from various information sources as well as the adoption of effective policies of information security assumes a crucial importance.

Over the years, studies and research have focused [1]-[3] on the role of information systems (IS) in terms of services offered by banks. Special attention was dedicated to what is called the Banking Information System (BIS) and on its capacity to provide services such as online banking, on-line credit card management, and automated teller machines (ATM) services. Studies conducted indicate that 2016-2017 was characterized by a significant increase in the level of cyber-insecurity and the World Economic classified the risks deriving from cyber-attacks in third place among major global risks in terms of probability and sixth place for impact generated [1].

The cyber-attacks have undergone a significant increase globally over the years increasing from 873 cases in 2014 to 1127 in 2017, an increase of 22.5% with a constant and significant upward trend, see Fig. 1 [1].

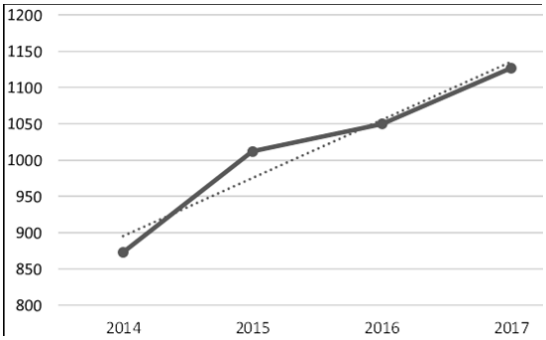

Fig. 1 Serious cyber-attacks 2014-2017 [1]

An analysis of the type of attacks in the four-year period 2014-2017, see Fig. 2, shows a steady growth in the number of episodes of cyber-crime which increased from 526 cases in 2014 to 857 in 2017 (+38.6%). At the same time there has been a significant decrease in cases of Hacktivism and

decrease, albeit milder, in cases of information warfare. The cases of espionage and sabotage, on the other hand, show a significant increase of 46.5% over a four-year period (2014-2017) and of 31.8% over the period 2016 to 2017 [1].

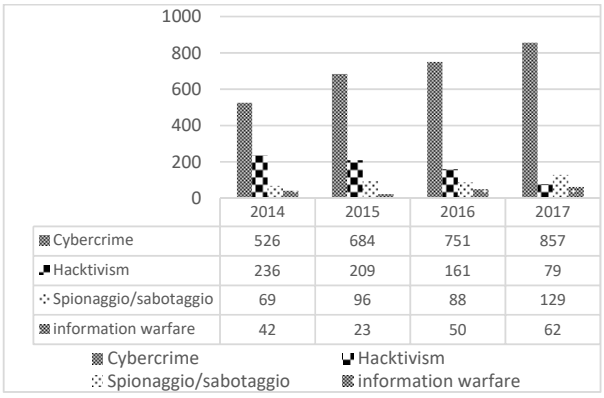

Fig. 2 Types of attack [1]

Studies conducted [1] show that compared to 2016, in 2017 the greatest percentage growth of serious attacks is observed with respect to mixed categories (Multiple Targets) where the observed increase is +353%. This is followed by the education sector (+29%) and Software/Hardware vendors (+21%), followed by the Banking/Finance category which underwent an 11% increase over the last year.

As in Fig. 3 the analysis of serious cyber-attacks that are involved the banking-financial sector in the four-year period 2014-2017 shows a growing trend with a variation of approximately +134% between 2014 and 2017. The total number of cyber-attacks in the banking sector in 2017 was 373 [1].

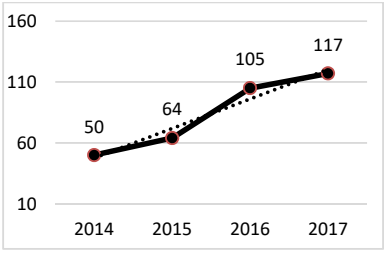

Fig. 3 Serious computer attacks in the financial sector [1]

Analysis of the main reports made in the four-year period 2014-2017 show a constant occurrence of criminal attacks against banks.

In 2005 the biggest cyber-robbery was carried out against over 100 banking institutions in more than 30 countries in the world, including the Italy, with an estimated damage of at least $1 billion. The operation, called Carbanak, began at the end of 2013, was only discovered in 2015 and is still continuing in other sectors. Cyber criminals succeeded in penetrating, through phishing techniques, the information systems of various banks infecting them with malware. They have stolen huge amounts of money simulating, after carefully studying internal flows, apparently lawful and authorized operations.

In 2016, the biggest cyber-robbery was carried out against the Bank of Bangladesh, and the one that, if not for a mistake by the attackers, would have been the biggest of all time. The hackers, after undermining some of the bank's systems, introduced fraudulent transactions into the SWIFT system, ordering the transfer of funds for a total of 1 billion dollars, of which only the first trance was successful with an estimated damage of 81 million dollars.

Again in 2016 about 20,000 customers of the British Tesco Bank were robbed by cyber criminals who over the course of a weekend forced the bank to block online accounts and credit/ debit cards for victims for a few days.

II. Literature Review

The notion of risk in economic-business context can be defined as the possibility that an adverse event will materialize, causing damage to a company [2]-[4]. The advent and development of IT have given rise to new types of risk, among which IT risk appears today to be particularly significant [5], [6].

In literature, cyber risk is considered as a specific case of IT risk and can be defined as the risk connected to adverse electronic events that can cause extremely serious problems, both strategic and operational, and can generate huge monetary losses [7], [8]. The International Organization of Market Supervisory Authorities (IOSCO) and the Committee on Payments and Market Infrastructures (CPMI) define "cyber risk" as the combination of the probability that an event will occur in the context of information and IT resources of an organization and the consequences of this event for the organization itself [9].

Cyber-attacks that can penetrate company databases stealing sensitive customer data and information (credit card number, debit card pin, etc.) can originate within the organization, through the complicity of employees, or as occurs more frequently, from the outside by groups of so-called "hackers" [10].

In recent years, information security has assumed a central role within the broader field of risk management studies [11]–[21], constituting a component of primary importance in the definition and measurement of the risk to which a company as a whole is exposed, a risk that can be defined by the well-known formula: Risk = probability of the event × Consequent impact. Specifically, IT risk is a function of three main variables: the scenario of the event occurring, the probability that this scenario will materialize, the impact of the consequences deriving from the occurrence of the event [22].

The problem of IT risk requires a labor analysis by adopting a business economic perspective in order to identify and evaluate, by means of risk management techniques, the procedures, activities and processes that the company can put in place to make its own operations safer, assess the level of adequacy of a given security system, the necessary investments to counter possible "attacks" on the system itself [23].

In general, companies are required to take action to protect the wealth of information available to them, whose value appears tendentially to be growing, also due to the possibilities and trends now offered by IT, through a prior identification and evaluation of the consequences, including economic ones, that a violation by third parties could determine [24]. Banks are trusted with a lot of data and information regarding their clients (individuals and businesses); the amount is potentially enormous: it includes personal data, credit history and merit, income, type and size of payments, risk appetite, consumption habits, type and entity of investments, etc. This information requires particular protection and has to be kept safely, also considering the value that it possesses. Emblematic in understanding the potential of this information heritage is the case of China where starting from 2020 each citizen and business will be assigned a "social credit rating" that will influence different aspects of the life of the community beginning with the possibility and costs of access to the banking system [25].

Valid support in the implementation of an effective integrated IT security management system can be found in the UNI EN ISO IEC 20000-1 standards "information technologies - service management -, in the UNI CEI ISO IEC 27001 standard" information technology for information security - information security management systems - requirements» and, in the ISO 22301 standard «societal security - business continuity management systems - requirements». The adoption of these standards represents an effective step in the development of more solid, resilient and above all effective management systems for the management of possible external attacks.

IT risk has its own particularities which, if analyzed in a traditional risk management system, make it necessary to make adjustments to the more general management framework of the forms traditionally assumed by operational risk.

The first characteristic of the IT risk that distinguishes is attributable to the source and the nature of the risk. It arises by virtue of increasingly sophisticated external attacks, carried out by highly motivated hackers able to infiltrate information systems, often silently, with different methods and techniques. This makes it very difficult both to identify the cyber-attack, and to determine a priori the potential damage.

Secondly, IT risk is characterized by the many ways in which the cyber-attack can affect the information systems of the bank and the speed with which it can spread, once it has managed to penetrate the defensive barriers.

The third characteristic of a cyber-attack is the fact that it can use procedures implemented to limit possible damage caused by other malicious events, of a physical origin, such as data replication and information procedures (backup) on external servers designed to protect them in the event of malicious events that may affect the main servers.

III. Methodology

This work can be considered the first step of a broader research project aimed at assessing whether IT security in banking organizations can be overseen and managed within the risk management system. As highlighted in the literature [1], [26], to date, within the strategic cyber security plans of the banks new areas seem to be emerging, such as Measurement and reporting, Advanced Threat Management, Threat intelligence and security analytics, highlighting how national banks intend to undertake the right development actions, also in relation to the need for management of cyber security of a more managerial nature.

The various aspects of cyber security are gradually becoming part of the life of a company, even if, however, the "implicit" component appears to be poorly traced and visible.

The research questions are as follows:

- QR1: How can a financial institution monitor and manage cyber risk?
- QR2: Is it possible to specifically monitor this type of risk within the integrated information risk management system for the control and management of crime attacks?

The answers to these questions make use of a theoretical framework which, on the basis of the taxonomy of the management processes activated in the Risk Management function, is able to favor the assessment of the relation between risk and IT security in the bank.

From a methodological point of view, the analysis is conducted on the basis of an epistemological study which corresponds more to a reflective-academic analysis [27]; so that by means of the inductive method we will verify the validity of the hypotheses formulated.

The sources used for the definition of the framework are of a primary and a secondary type. The former refers to the most recent normative documents expressing supra-national and national positions on cyber security while secondary sources refer to the contents of international and national literature. [28]-[36].

The paper relates to the themes regarding cyber risk and security in the financial system. The EBA considers cyber risk to be the greatest risk to the stability of the European banking system [30], [37] as stated in the Risk Dash Board: "aimed elevated cyber risk, improvements of IT systems are critical to support the implementation of banks' digitalisation strategies" [30].

The innovative aspects of the research compared to the existing literature refer to the construction of the theoretical framework of cyber risk management which must:

1. Consider cyber risk as a strategic risk, an integral part of the risk management system;
2. Define and outline processes, roles, responsibilities and persons responsible for monitoring and managing cyber risks;
3. Define the key indicators that guarantee prompt interventions by the competent bodies to protect the principles of preservation and the creation of value

IV. Definition of the Theoretical Framework: Particularities and Important Aspects

In defining the theoretical framework, particular attention is paid to ensuring that it is compliant with the national and supranational regulatory reference framework. In particular:

- Bank of Italy - Circular no. 263 27 December 2006, 15th update of 2 July 2013;
- Recommendations for the security of Internet payments - European Central Bank - in January 2013.
- Provisions contained in the applicable privacy legislation (Legislative Decree 196/2003 "Code regarding the protection of personal data" and subsequent measures dated 10.1.2008 and 11.27.2008);
- "Guidelines for the definition of an IT risk analysis methodology and an IT risk management process" - Supports the adaptation of the project to the 15th update of 263/06 - new information technologies and business continuity - September 2014;
- Risk analysis methodology "IT risk analysis methodology" - Project to adapt the project to the 15th update of 263/06 - new information technologies and business continuity - in January 2014;

Furthermore, the IT function, as a whole, must follow international best practices, such as: ISACA Cobit 5 for risk; ISO/IEC 27001: 2005 Information Technology - Security Techniques - Information Security Management Systems - Requirements; ISO/IEC 27005: 2011 Information technology - Security techniques - Risk management for information security; and ISO 31000 Risk Management - Principles and Guidelines.

The Cyber Risk framework makes use of the information gathered, among others from national and international literature on cyber risk issues, with the aim of providing a representation of the elements and relationships between management processes defined on the basis of sector operations.

Fig. 4 shows the components and the main management processes in the definition of the theoretical framework. The model shown in the figure is formalized through a regulatory system composed of policies, regulations and organizational procedures, overseen by the main players involved in the management of financial risks.

1 step: Potential Risk Identification of existing IT assets/services in banks expressed in quantitative terms; Classification of It service identified according to the information security standard (ISO/IEC 270021); Threat catalogue and threat modelling activities; Measurement of potential risk
2 step: Definition of strategic controls and controls Definition of the "Residual risk" matrix to highlight the Potentia risk - effectiveness of processes relation; Definition of the residual risk from the qualitative standpoint, using data from the "Residual risk" matrix; Acceptance of residual risk by identifying the risk tolerance threshold defined by the Board of Directors.
3 step: Evaluation of cyber risk Classification of cyber incidents recorded; Evaluation of the accidents identified during the reference period Determination of the "scoring incident" matrix;
4 step: Evaluation of residual risk Assessment of the compliance of IT assets with reference to the minimum safeguards defined in the guidelines document for the classification of information and IT resources; Mapping of scenarios for the identification and evaluation of IT assets considered to be of a “critical nature”; Determination of the risk measurement of IT assets deemed to be “critical in nature”
5 step: Reporting Activities of reporting to Top Management; Activities of reporting to the Board of Directors

Fig. 4 Cyber Risk Management Process

The relationships between individuals and processes involved in the control and management of cyber risks are shown in Fig. 5.

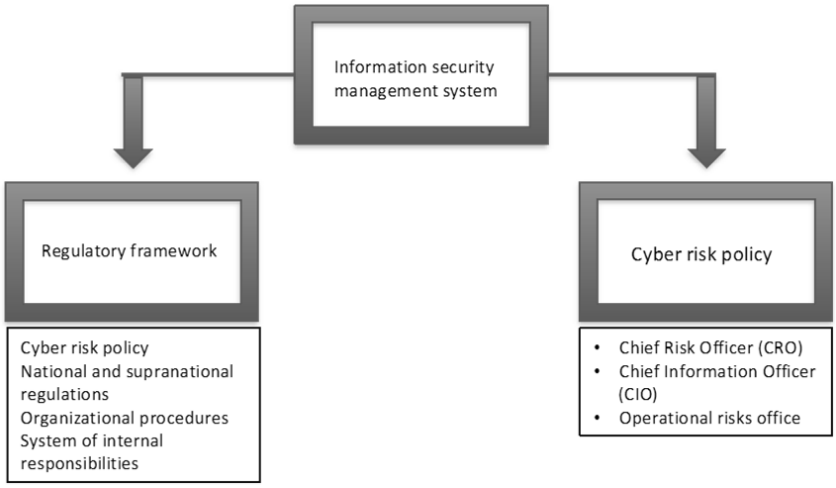

Fig. 5 The system of relations in the cyber risk management function

The guiding principles for the construction of the proposed theoretical framework presuppose a precise identification of the IT assets and the risk factors to which the organization is exposed. It is divided into a sequence of phases, each of which is subdivided into processes: identification of the main IT assets (risk factors) and their possible relationship and business processes; identification of IT risk scenarios and threats; evaluation of the probability of risk manifestation and

the definition of risk appetite and risk tolerance thresholds. Obviously, at the end of the risk management cycle, there is also the activity of reporting to the top management bodies. In particular, among IT assets it is important to identify all those IT applications whose vulnerability could represent a threat to data integrity and, consequently, to business continuity; the relationships between IT resources and the ways in which banks integrate IT risk with corporate risks, above all reputational and strategic.

The particular characteristic of the proposed framework is therefore that of highlighting a mapping of the "nodal" key elements and of the scenarios that characterize the technological chain, considered in any case in a general context of Risk management. In particular, aspects such as the following should emerge:

1. Potential Risk, through Identification of IT Assets

The IT elements that must be analyzed and evaluated within the model, using an approach that is proportional to the size of the bank, are:

- IT services consisting of one or more IT applications, whose purpose is to support the provision of the functionalities required by business processes to achieve its strategic and operational objectives;
- IT applications: a set of components supporting one or more IT services;
- IT processes: management and governance of the IT operational machine common to all IT applications;
- Infrastructures: elements of the model made up of the technological and infrastructural components that support the functioning of the other IT element.

2. Catalogue of Threats and of Threat Modelling Activities

The IT threat is any event or circumstance that can have negative consequences on information systems. Any threat can be characterized in terms of the vulnerabilities of the components of the information system, exposure of the components to the threat and types of consequences, while some threats can be realized according to different modalities.

These are presented according to a hierarchical structure (Threats of I, Level II, Level III ...) depending on the intrinsic granularity in them. Each banking institution supports the implementation of cyber risk analysis at different levels of detail, depending on the availability and quality of the information available on the elements to be analyzed.

3. Definition of Business Process Controls

They are a component of the cyber risk model as they contribute both to the assessment of the impacts associated with the risk scenarios relating to the components of the information system that support them and to the identification of the critical components of the information system.

4. Scenario Mapping for the Identification, Assessment and Management of Cyber Risk

The cyber risk scenario could be defined as a homogeneous set of IT threats that can cause damage to the company. A harmful event can be assessed qualitatively or quantitatively and includes economic damage, operating costs, violations of regulatory compliance.

The main features of the scenario are:

- Identification of the probable consequences of the manifestation of the risk for business continuity, in terms of strategic and reputational damage;
- Association, through the different levels of threats, with one or more elements of the IT model; examples of this may be the total unavailability of information systems, the deterioration of service quality and the violation of data privacy, the impairment of data integrity and the loss of data quality. The association between each IT Risk scenario and IT threats will then be reported in a specially designed "IT Threats Library"
- Definition of the metrics for the assessment of the probability of occurrence of one or more IT threats; the evaluation of the probability is represented using a qualitative scale of increasing probability evaluation levels: "Very Low", "Low", "Medium", "High", "Critical". It is defined as follows: a) Very low: probability of an event occurring once every three years; b) Low: probability that an event will occurring once in a year; c) Average: probability of an event occurring once every 6 months; d) High: probability of an occurring once in 3 months; e) Critical: probability of an event occurring once a month;
- Definition of the metrics for the impact assessment with reference to its various aspects: economic, deriving from the contraction or absence of profits through the normal course of business processes, due to destruction or damage of IT resources; of the operating costs relating to the use of human resources in the resolution of adverse events occurring in IT procedures; of the compliance risk for compliance violations following the occurrence of adverse events; of reputational and strategic damages arising from the manifestation of the negative event;
- Identification of security measures to mitigate risk. In this regard, it should be stressed that the objective of the security measure is to reduce the risk of threats, which is incident on IT assets and acts in relation to the different degree of damage caused. The set of security measures, called "IT Security Measures Library", is defined by identifying those measures that incorporate the requirements for mitigating the impact of a threat or the probability of its occurrence. In identifying security measures, risk policies, procedures, regulations and guidelines should be considered in order to facilitate their identification.

5. Evaluation of Residual Risk

In this phase, the bank defines the correlation between cyber risk and operational risk, as well as the appetite and tolerance risk thresholds, as highlighted in the Risk Appetite Framework (RAF).

6. Definition of the IT Risk Calculation Model

This phase concludes the cyber risk management cycle with

the production of a summary annual report on the IT risk situation. Closer deadlines may occur following the adoption of innovative IT projects, infrastructure projects capable of altering the previously assessed risk level; and again, in the presence of serious incidents or deficiencies in the checks carried out, of new threats or dissemination of news regarding the manifestation of new vulnerabilities in IT applications, new legal provisions, regulations, standards and industrial standards imposed contractually, of events or threats that raise doubts about the effectiveness of measures and safeguards regarding the quality and governance of data and information.

V. Discussion of the Results and Conclusions

The aim of the research was to develop a theoretical framework for the management and control of cyber risk in banking institutions. The model presented could make it possible to achieve the objective proposed by virtue of its particularities, recognizable in the opportunity to manage qualitative and quantitative processes and variables, with recourse to modular approaches and, in subsequent phases, to be able to provide also an evaluation of the quality of IT risk control under observation. It is clear that cybersecurity is no more than a combination of human resources, processes and technologies that involves the bank as a whole, of which the function of IT is one component. The implementation of information security measures must therefore encompass IT services, IT applications, processes, policies, procedures, networks and information, and not be limited to the IT function alone. However, it is a pilot model that needs further refinements on the basis of empirical analyzes that can be generalized to the entire banking system.

Regarding the first research question, we have observed that most of the studies on IT risk tend to consider cyber risk as an integral part of the information risk management system; indeed, it is hoped over time that the perimeter of the cybersecurity will be extended to the company organization as a whole. Therefore, the hope is that soon banks can provide themselves with an effective governance structure for determining the institution's propensity to cyber risk.

Regarding the second question, in 2015, CIS Sapienza in collaboration with the CINI consortium - Cyber Security National Laboratory National Interuniversity Consortium for Informatics -, adapted the NIST framework to the Italian context, highlighting the differences and company specifications in the implementation of the framework [38].

The principles that guided the definition of the methodology of technological risk analysis were the consideration of the impacts of IT components on the risks of business operations; the desired level of granularity for analysis; compliance with general principles such as repeatability of the methodology, compliance and consistency with regulation and feasibility. These important changes require adequate supervision over time and therefore the definition of governance models that include, necessarily, the issues of cybersecurity and the implementation of strategies aimed at managing cyber risk. For this purpose, condicio sine qua is not only the development of the professionalism and skills of the operational staff but also an improvement of the IT skills of the executive and the members of the company boards, without however neglecting those required by the supervisory bodies (e.g. Control and Risk Committee).

This model has some limits like all management and control models that deal with processes based on IT skills. In effect, it must be able to manage any methodological problem deriving from the quantification of quali-quantitative outputs. Furthermore the model has to deal with any difficulty encountered both in identifying in the technological chain the "nodal" devices that are more subject to vulnerability and in the manifestation of behaviors of human resources that do not conform to the rules and practices of safety. At last we should underline the necessary characteristic of universality of application, which, as is known, is dependent on the comparability of the data present in company reports.

There are possible future developments. The framework is a pilot model that needs further adjustments *in itinere*, based on rigorous empirical tests conducted to confer on it the characteristics of universal applicability in the banking context. Although presenting highly flexible features, lending itself to subsequent improvements, additions and processing to ensure greater adaptability to individual banks, the model, structured on the information derived from primary and secondary sources, may not respond to needs of a general nature or to the international banking.

References

[1] Clusit - Associazione Italiana per la Sicurezza Informatica, Rapporto Clusit 2018 sulla sicurezza ICT in Italia, 2018
[2] J. G. March, and Z. Shapira, “Managerial perspectives on risk and risk taking,” Management science, Vol. 33, no 11, pp. 1404-1418, 1987.
[3] K.J Arrow, Aspects of the Theory of Risk Bearing. Helsinki: Yrjo Jahnssonis Saatio, 1965.
[4] J. W. Pratt, “Risk Aversion in the Small and in the Large,” Econometrica, Vol. 32, pp. 122-136, 1964.
[5] G. Bansal, “Distinguishing between Privacy and Security Concerns: An Empirical Examination and Scale Validation,” Journal of Computer Information Systems, Vol. 57, pp. 330-343, 2017.
[6] D. L. Goodhue, and D. W. Straub, “Security concerns of system users: a study of perceptions of the adequacy of security,” Information & Management, Vol. 20, no. 1, pp. 13-27, 1991.
[7] A. Mukhopadhyay, D. Saha, B. B. Chakrabarti, A. Mahanti, and A. Podder, “Insurance for Cyber-risk: A Utility Model Decision,” Decision Support Systems , Vol. 32, no. 1, pp. 153-169, 2005.
[8] H. Öğüt, S. Raghunathan, N. Menon, “Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection,” Risk Analysis, Vol. 31, no. 3, pp. 497–512, 2010.
[9] CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures. Bank for International Settlements and International Organization of Securities Commissions, 2015.
[10] N. S. Safa, R. Von Solms, and S. Furnell, “Information security policy compliance model in organizations,” Computers & Security, Vol. 56, pp. 70-82, 2016.
[11] C. Biener, M. Eling, and J.H. Wirfs, “Insurability of Cyber Risk: An Empirical Analysis,” Working Paper of Finance, University of St. Gallen, no. 3, 2015.
[12] Deloitte, Modelli di governance dei rischi cyber e raccomandazioni di sviluppo per le aziende. Milano 2016.
[13] J. L. Hieb, “Cyber security risk assessment for SCADA and DCS networks,” ISA Transactions, Vol. 46, pp. 583-594, 2007.
[14] A. Hoffmann, and H. Ramaj, “Interdependent risk networks: the threat of cyber attack,” International Journal of Management and Decision Making, Vol. 11, no. 5/6, pp. 312-323, 2011.
[15] K. S. Hong, Y. P Chi, L. R. Chao, J. H. Tang, “An integrated system

theory of information security management," Information Management & Computer Security, Vol. 11, no. 5, pp. 243-248, 2003.
[16] P. Ifinedo, D. Olsen, "An Empirical Research on the Impacts of organisational decisions' locus, tasks structure rules, knowledge, and IT function's value on ERP system success," International Journal of Production Research, Vol. 53, no. 8, pp. 2554-2568, 2015.
[17] R. Keyun, "Introducing cybernomics: A unifying economic framework for measuring cyber risk," Computers & Security, no. 65, pp. 77–89, 2017.
[18] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity. 2017. www.nist.gov/cyberframework
[19] J. F. V. Niekerk, R. V. Solms, "Information security culture: a management perspective," Computers & Security, Vol.17, pp. 476-486, 2010.
[20] PricewaterHouseCoopers, Enhancing business resilience: Transforming Cyber risk management through the role of the Cief Risk Officer (CRO). 2015. www.pwc.com/financialservices
[21] H. Stewart, J. Jürjens, "Information security management and the human aspect in organizations," Information & Computer Security, Vol. 25, no. 5, pp. 494-534, 2017.
[22] S. Kaplan, B. J. Garrick, "On the quantitative definition of risk," Risk Analysis, Vol. 1, no 1, pp. 11–27, 1981.
[23] S. Hoo, How much is enough? A risk-management approach to computer security. CA: Stanford University, 2000.
[24] NIST, Risk management guide for information technology systems.National Institute of Standards and Technology (NIST). 2002.
[25] Z. Ramadan, "The gamification of trust: the case of China's "social credit," Marketing Intelligence & Planning, Vol. 36, no. 1, pp. 93-107, 2018.
[26] M.C. Arcuri, M. Brogi, and G. Gandolfi, "Ciber risk in the financial industry, the market reactions," Bancaria, Vol. 4, pp. 35-49, 2017.
[27] A. Abbott, Methods of Discovery: Heuristics for the Social Sciences. New York: W.W. Norton, 2004.
[28] Commissione Europea, Resilienza, deterrenza e difesa: verso una ciber sicurezza forte per l'UE. Comunicazione congiunta al parlamento europeo e al consiglio, 13 dicembre 2017.
[29] EBA (a), Risk Dashboard data as of Q2 2017. European Banking Authority, 2017.
[30] EBA (b), Guidelines on ICT Risk Assessment under the Supervisory Review. European Banking Authority, 2017.
[31] G7 (a), Foundamental elements of cybersecurity for the financial sector. ottobre 2016
[32] G7 (b), Foundamental elements for effective assessment of cybersecurity for the financial sector. ottobre 2017.
[33] Banca d'Italia (d), Disposizioni di Vigilanza per le banche, to the 16th update of 285/13. Banca d'Italia , 2013.
[34] Banca d'Italia (b), Linee guida per la definizione di una metodologia di analisi del rischio informatico e di un processo di gestione del rischio informatico. Support Project adjustment to the 15th update of 263/06 - new information technology and business continuity – September 2014.
[35] Banca d'Italia (c), Policy di Metodologia di analisi del rischio Informatico, Risk Analysis methodology - Support Project adjustment to the 15th update of 263/06 - new information technology and business continuity - January 2014.
[36] Banca d'Italia (a), Nuove disposizioni di vigilanza prudenziale per le banche. Circolare n. 263 del 27 novembre 2016, www.bancaditalia.it
[37] EBA (c), Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2). European Banking Authority, 2017.
[38] CIS Sapienza and CINI, Italian Cyber Security Report. Un report nazionale per la cyber security. Roma 2015, www.cybersecurityreport.com