CYBER RISK MANAGEMENT IN CREDIT COOPERATIVE BANKS: A CASE STUDY

CYBER RISK MANAGEMENT IN CREDIT COOPERATIVE BANKS: A CASE STUDY.

Abstract

This research explores the Italian banking sector. In particular it focuses on the analysis of the cyber risk management in Bene Banca, a Credit Cooperative Bank (BCC) in the North-West of Italy.

This study represents a case study that can help understand the context and the main characteristics of the methodology implied by Bene Banca in managing cyber risk. Data were collected through semi-structured interviews of an open-ended nature and questionnaires to directors, members of the audit committee, risk managers, compliance managers, internal audit function and anti-money laundering responsible.

The focus is on this small bank because of its size and its role on the local territory and because the cyber risk management is outsourced.

Furthermore the topic of cyber crime has become particularly relevant because IT attacks have increased drastically in recent years, both in terms of complexity and resources, and they cannot be stopped by single organizations, because they need a response at country level.

Consequently this paper has been motivated by the gaps in the understanding and in considering cyber risk and cyber risk management as an integral part of the business management.

Keywords: cyber risk management, credit cooperative bank, cybercrime, threats, IT, case study

Track n. 40: General Tracks

Introduction

Companies with the constant need to adapt to the needs of the surrounding environment have increasingly developed information and communication technologies (ICTs), leading companies to be heavily dependent on cyberspace.

In the banking system in particular, nowadays in order to be competitive, each bank must be increasingly connected to the technological world. However, cyberspace and its components are influenced by a high number of potential hazards. First of all, since they are complex and rapidly evolving systems, their vulnerability is always present. One or more of these

vulnerabilities can be exploited by hackers that illegally might have access to an organization's IT systems, allowing them to read, steal or delete critical information, or even take control of their IT or physical resources. These vulnerabilities make cyber risk very relevant from the point of view of both financial and reputational risks.

As regards the banking system and in particular credit cooperative banks in Italy, they find their origins in the last quarter of 1800. Since their inception these institutions were closely linked to the local communities in which they were established, in fact thanks to the deep knowledge and mutual members of the community, their family situation, their personal reputation were singled out to creditworthy people. Since then, Rural and Artisan banks have maintained a very close relationship with the territory of reference, weaving their own story with that of the communities, as to be “local banks call”. The rural banks were able to grow in number and spread over time, supporting the socio-economic development of their local areas.

In 1993, the Banking Act lays down a radical change since the naming ranging from "Rural and Artisan banks "to the current "mutual banks". By means of this decree are not operating limitations of BCCs that can offer so all the products and services of other banks.

The system of mutual banks in Italy today includes 364 banks for a total of over 4,400 branches throughout the Italian territory. The employees of the banks are over 37,000.

In total there are more than one million and two hundred thousand members of the mutual banks and mutual banks are more than 6 million customers.

In December 2016, total managed amounts on behalf of customers - consisting of direct deposits and indirect deposits - amounted to EUR 977.2 million. Direct collection amounts to 599.3 million euro. Cash receivables with customers net of value adjustments (asset item 70) amount to euro 460.3 million.

This research, as it is a case study, fits into this framework. In fact it concentrates on the topic of cyber risk management in a credit cooperative bank. The bank is Banca Credito Cooperativo di Bene Vagienna - BeneBanca an Italian credit cooperative bank in the North-West of Italy.

The aim was twofold: firstly it is interesting to analyse how this small institution manage cyber risk and secondly it is important to find out how effective the process of managing cyber risk is.

This study could be extremely useful for the bank itself to improve and consider all the weaknesses of the process and try to modify some phases and activities. For other small credit cooperative banks, this case study can be regarded as an example, useful to adapt their process. For researchers in the field of risk management and credit cooperative banks, this research might be the first step to stimulate further developments in the field.

The remainder of the study is organised as follows: in paragraph 1 a brief literature review is presented, in section 2 methodology and research design are described, paragraph 3 instead presents findings, while comments and discussion follow this section and finally we present the conclusions.

1. Literature Review

With reference to the topic of credit unions and credit cooperative banks, Smith et al. (1981) discussed about the economic theory of these businesses and Labie and Perilleux (2008) studied the Corporate Governance in Microfinance. Several researchers concentrated on this kind of banks, in terms of characteristics and role within the Italian banking sector (Bonfante, 2010; Agostini, 2009; Costa, 2007; Capriglione 2005; Vella, 2004; Appio, 1996). Zago and Dongili (2014) examined in depth the impact of the financial crisis on the Italian credit cooperative banks and the technical efficiency of the Italian BCCs for the period 2003 to 2012, discussing and testing different specifications and objective functions for BCCs. The importance of local small banks, such as BCCs, was emphasized in few studies. Ferri and Messori (2000) stressed that close and long lasting customer relationship between small banks and firms can promote a favourable allocation of credit for economic growth. Usai and Vannini (2005) distinguished among various types of banks while studying the finance-growth nexus in Italian regions. Good capitalisation, stable funds availability and liquidity give BCCs the ability to provide credit even during the recent financial crisis, replacing other banks suffering more from the credit crunch. These elements positively affect the local community in which the BCC operates, by supporting families and the development of businesses. In 2007-2008, the financial crisis caused significant new problems in risk assessment and management. As a consequence, some researchers tried to locate the perimeter within which identify the financial risk and study methods for good management, in accordance with the requirements of Basel (Álvarez and Rossignolo 2015; Angelini et al. 2011).

This research is a contribution in the field of cyber risk management and cybercrime in the banking system.

Cyber risk can be defined as the risk of incurring in financial, reputational and market share losses in relation to the use of information and communication technology (ICT) (Mukhopadhyay et al., 2013; Öğüt et al., 2010).

Therefore, cyber risk is considered as an operational, reputational and strategic risk that has three fundamental characteristics: vulnerability, threat and damage. Furthermore it cannot be

completely managed and eliminated because of the speed of change of the surrounding environment, globalization and IT connections (CIS Sapienza, 2015).

This kind of risk should be managed throughout the organisation, enhancing data and information sharing, in addition to knowledge sharing, but also globally because cyber risk is a systemic risk, with no territorial and physical boundaries.

There are several works using different methodologies that focus on cyber risk. They concentrate on cyber security as a tool to manage exposure to IT risk and protect an organization against a new form of business loss (Biener et al., 2015; Mukhopaday et al., 2013; Mukhopaday et al., 2005; Laurence et al., 2003). Others focus on specific tools to mitigate this risk (Hoffman and Ramay, 2011; Hieb, 2007). There are some professional guidelines that underlines the importance of building cyber resilience (PwC, 2015; MMC, 2016).

They all stress the importance of developing sound risk management and an appropriate approach, without mentioning a possible solution for companies. In particular, in the business literature, little has been studied in the subject of the banking world and its problems in dealing with cyber risk. In the present economic scenario, the definition and implementation of a risk management system becomes a driving factor for the bank improvement and growth as well as a crucial competitiveness factor. But the problem emerges when facing cyber threats. The majority of people involved in managing risks do not have the proper skills to deal with cyber risk (PwC, 2015). Consequently, it is difficult to integrate cyber risk management into the general risk management process of each company

This case study combines the two topics and aims at analysing the peculiar reality of a small credit cooperative bank, in which the cyber risk management process is outsourced.

There are no previous studies concentrating on this phenomenon and analysing this process with its phases without considering the technical aspects of ICT sources and possible practices to manage cyber risk.

2. Methodology

Research design

A qualitative case study is an approach to research that facilitates exploration of a phenomenon within its context using a variety of data sources. This ensures that the issue is not explored through one lens, but rather a variety of lenses which allows for multiple facets of the phenomenon to be revealed and understood (Baxter and Jack, 2008).

Case studies are tailor-made for exploring new processes or behaviors or ones that are little understood (Hartley, 1994). Hence, the approach is particularly useful for responding to how and why questions about a contemporary set of events (Leonard-Barton, 1990). Moreover, researchers have argued that certain kinds of information can be difficult or even impossible to tackle by means other than qualitative approaches such as the case study (Sykes, 1990).
Gummesson (1988:76) argues that an important advantage of case study research is the opportunity for a holistic view of the process: "The detailed observations entailed in the case study method enable us to study many different aspects, examine them in relation to each other, view the process within its total environment and also use the researchers' capacity for 'verstehen' ".
The case study is open to the use of theory or conceptual categories that guide the research and analysis of data (Meyer, 2001).
A case study design using multiple levels of analysis was employed for this study. This approach was necessary to 'get close' to the actors' perspectives on the complex processes of network interaction (Blackburn and Kovalainen, 2009; Curran and Blackburn, 2001). Data sources included interviews with directors, members of the audit committee, risk managers, compliance managers, internal audit function and anti-money laundering responsible.
The case reported here is represented by Bene Banca, a small credit cooperative bank in Piedmont, North-West of Italy. It was founded in November, 14 in 1897.
This paper concentrates on this small bank because of its size, its role on the local territory and because one of the authors is a member of the audit committee. Furthermore this single case is particularly critical and typical because the cyber risk management process is outsourced, while in other banks the function is internal to the bank. Consequently thanks to this study this particular phenomenon can be observed and analysed.
This research represents the second step of a far deeper analysis that would involve other realities, by elaborating a multiple case study. In addition, it is interesting to analyse how a small financial institution assesses and manages cyber risk.

Data collection and procedure

The case study research was conducted by the authors over a period of six months from September 2016 to February 2017, during which time the main method for data collection was through semi-structured interviews of an open-ended nature. Thirty-five interviews were conducted in total, from which eleven interviews were carried out in the case study reported here. The major data collection was accompanied by a brief questionnaire. The purpose of the

questionnaire was to collect information regarding the risk methodology employed to manage cyber risk and to build RM capability.

The study has the aim to formulate research questions by problematizing some dominant assumptions in existing research (Davis, 1971). In particular, the main research questions are the following:

- *Research question 1*: How do a small financial institution manage cyber risk?
- *Research problem 2*: How effective is the methodology pursued?

This approach would support a more reflective-scholarly attitude (Abbott, 2004) and consider a different epistemological approach.

In this case the epistemological approach is that of induction because it finally helps reach a verdict on the hypotheses, previously analysed in the phase of abduction, and the nature of the verdict is dependent on the number of testable consequences that have been verified.

Furthermore, we decided to focus on the topic of cyber crime because IT attacks have increased drastically in recent years, both in terms of complexity and resources, and they cannot be stopped by single organizations, because they need a response at country level, as they tend to diminish its economic prosperity and independence.

Consequently this paper has been motivated by the gaps in the understanding and in considering cyber risk and cyber risk management as an integral part of the business management. And the attention here is on a critical infrastructure (as defined by the NIST Framework, elaborated by the FSSCC), which is also a small company.

3. Findings

Thanks to the interviews and questionnaires, we found that Bene Banca applies a methodology common to all banks in the consortium. The consortium carries out an outsourced function to the bank in relation to IT risk management. This function complies with:

- Banca d'Italia - Circolare n. 263, of 27 December 2006 15° update of 2 July 2013;
- Provisions provided by applicable privacy laws (D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali", and subsequent measures of 10.13.2008 and 11.27.2008);
- "*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 ;

- "*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 - in January 2014;
- Recommendations for the Security of Internet payments - European Central Bank - in January 2013.

In addition this function follows 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 - Information security risk management; and ISO 31000 Risk management - Principles and guidelines.

The Cyber Risk Model contains a representation of the elements and scenarios that must be considered in the field of Cyber Risk, defined on the basis of best practices in the industry.

The Cyber Risk Model consists of: business processes of banks; the representation of the main elements IT (risk factors); the relevant relations between elements and processes; threats that insist on such elements; the related impact on the business of the banks.

In particular, in the IT environment it is important to identify all the IT Application on which may insist Threats of IT; relationships between IT resources and the ways in which banks perform integration of IT risk with Enterprise Risks, especially reputational, strategic and operational.

It is illustrated a representation of the elements and of the scenarios that characterize the Model, and which therefore must be considered in context Risk Computer.

a) Business Processes

They are a component of the IT risk model since they contribute, through the hazards to which they are subject, to the assessment of impacts associated with the Risk Scenarios relating to the components of the information system that support them; and identification of critical components of the computer system.

b) Business Organizational Units

The contact people of the organizational business units of banks in the consortium are the reference actors for the evaluation of impacts. Among them, the Banks of the Consortium identify Users Officers representing end-user systems and IT applications and in dealing with internal ICT Department to the Bank.

c) IT Elements

The complexity of IT elements that must be analyzed and evaluated within the model, using a proportional approach to the analysis dimensions, is described below. They are represented by:

- IT services: consist of one or more IT applications, whose purpose is to support the delivery of the functionality required by business processes to achieve its strategic and operational objectives.
- IT Applications: a group of components in support of one or more IT Services.
- IT Processes: the management and governance of IT operational machine common to all IT applications.
- Infrastructure: elements of the model constituted by the technological and infrastructure components that support the operation of the other IT elements.

d) IT Threats

The IT threat is any event or circumstance that may lead to negative consequences (impact) on information systems. Any threat can be characterized in terms of vulnerability of the components of the computer system, exposure of the components to the threat and types of consequences, whereas some threats can be realized according to different modes.

The IT Threats are declined according to a hierarchical structure (Threats of I, Level II, Level III, ...) depending on the granularity of the same. This organization supports the Risk Analysis implementation at different levels of detail, depending on the availability and quality of information available on the elements to be analyzed.

e) Risk Scenarios Computer

It defines "Cyber Risk Scenario", or simply "Scenario IT Risk ", a homogeneous set of IT threats that can cause a certain type of impact for the business.

The main features of the IT risk scenario are:

- identification of a type of consequences for business and, accordingly, the association or one or more IT threats that have the character to generate the sort of consequences identified by the scenery or one or more types of operational, reputational, strategic and compliance defined by the methodology in place at the individual bank of the Consortium;
- Association, through threats, to one or more elements of the IT model;
- definition, for banks, the rules of distribution of impacts from the Enterprise Risks on IT Threats;
- definition of the rules of distribution of probability values associated with threats;
- Identification of security measures to mitigate the risk associated Threats to the scenario.

The outsourcer for the portion of outsourced resources by the Bank is in charge of preparing, updating of IT Risk Scenarios and related documentation.

f) Probability of occurrence

The probability of occurrence of one or more IT threats is the frequency with which they may occur on one or more IT elements in a given period of time causing an impact on the consortium that will result in a negative impact for the Bank.

The estimated probability of occurrence, as well as the characterization of the associated risks, requires specific skills and knowledge of the IT environment, as well as the availability of appropriate time series.

g) Impact of IT

The impact of IT is the negative consequence for each bank of the Consortium, caused by the realization of one or more IT Threats. A IT Impact can be assessed qualitatively or quantitatively and includes economic damage, operating costs, violations of regulatory compliance and can be evaluated as part of the risk management process.

h) Measurements of IT Security

A IT security measure, whose main purpose is to reduce the risk that hangs over a computer IT element where it is applied, may act by reducing the exposure of a certain element to a IT Threat or limiting the impact of a threat. A security measure may act with respect to the various threats with a different degree of effectiveness which is defined as the level of risk that the measure helps smooth.

The set of security measures, called "IT Security Measures Library", is defined by identifying all the measures that have the ability to mitigate the impact or likelihood of occurrence of the threats contained in the "IT Threats Library". The library may take into account the fact that different security measures can act alternately in order to mitigate the risk associated with a threat to an appropriate level. In the identification of Security Measures to counter the IT Threats must be taken into account all the policies, procedures, regulations and guidelines in order to identify easily organizational security measures and procedural.

The methodology therefore identifies the essential safety measures for the mitigation of risks related to IT Threats associated with a scene.

The principles that have guided the definition of the Technological Risk analysis methodology are: the consideration of the impacts of ICT on the corporate operation risks; the desired level of granularity for analysis; compliance with general principles such as repeatability of the methodology, compliance and consistency with regulatory, and feasibility.

The prerequisites including the main stages of analysis and IT risk management are:

- *Defining the Context*: establish the main parameters of the process, collect all the key elements of the IT risk management process, define the scope of analysis and prepare a work plan;

- *IT risk identification*: identify the risk scenarios applicable to IT resources object of analysis. For the correct identification of the applicable scenarios it is necessary to consider the consequences defined by each scenario and determine whether such impact may occur on the Application IT under examination;
- *Census of IT applications*: identify IT Applications in the scope of analysis to provide sufficient information for risk analysis. This level can be redefined in successive sessions of application of the methodology;
- *Identification of IT Risk Scenarios and Threats*: such as Total Unavailability of information systems, Degradation of service quality, Breach of data privacy, Compromised data integrity, Loss of Data Quality. The association between each scenario of IT Risk and Threats IT is contained in the "IT Threats Library".
- *Definition of metrics for the evaluation of the probability of occurrence*: the evaluation of the probability of occurrence of one or more IT threats is calculated on the basis of certain assumptions criteria and the subsequent evaluation of the likelihood is represented using a qualitative scale of increasing levels of probability assessment: "Very Low", "Low", "Medium ","High", "Criticism". It is defined: a)Very Low: probability that an event will occur 1 once every three years; b) Low: probability that an event will occur 1 once a year; c) Media: probability that an event will occur 1 time every 6 months; d) High: probability that an event will occur 1 once every 3 months; e) Criticism: probability that an event will occur 1 time per month.
- *Definition of metrics for impact assessment*: the impact assessment is performed taking into account at least the aspects regarding a) the economic impact resulting from reduced or absent in the Bank's ability to generate profits through its business processes, arising from destruction or damage to physical or logical assets, of any penalties arising from non-compliance with contracted, connected service levels impossibility to comply with a legal obligation due to the occurrence of the adverse event; b) operating cost related to staff that is employed in the resolution of adverse event that occurred phases, supported by the Bank to compensate for the failure to support IT; c) the risk of non-compliance for compliance violations that may occur as a result of the occurrence of the adverse event; d) reputational damage to the bank, generated by the event and its adverse package delivery and the modes reputational damage to the bank, generated adverse event and its consequences; e) strategic damage to the bank, generated by the event and its adverse consequences.

- *Definition of thresholds for acceptance of the risk Computer*: the bank defines the correlation to operational risk, as well as their thresholds of risk acceptance, in relation to the Risk Appetite Framework (RAF).
- *Definition of IT risk calculation model.*

In this context, there is the annual production of "synthetic report on IT risk situation."

The process of analysis and management of Computer Risks must be repeated, at least every three years and, in any case, for all new projects related to the development of new IT Services /IT Applications, with particular urgency for the most critical areas; for all infrastructural projects that may alter the level of risk previously assessed on infrastructure; in the event of serious accidents or deficiencies in the controls carried out; in the event of new threats or the dissemination of news regarding new vulnerabilities in IT applications; in the case of new legal provisions, regulations, standards and industry standards imposed by contract; and occurrence of events or threats that may affect the effectiveness of data quality assurance measures and controls covered by the Data Governance perimeter.

4. Critical Comments and Discussion

To answer *the first research question*, the case study underlines the importance and significance of cyber risk for the bank. In fact, although it is a small reality, this issue is particularly monitored. This topic is dealt with by Bene Banca in a compliant manner with the rules of the Bank of Italy and has established all the procedures necessary to detect and limit this risk.

As regards the *second research question*, comprehensively cyber risk is managed properly and the process is proportionate to the bank size and the activity. However it is highly recommended to modify the procedures when specifying that the Computer Risk Analysis and Management process should be repeated at least every three years unless clearly identified in the document.

This time frame seems too broad and the proposal is to see it again as well as the underlying risk is constantly evolving. Cyber risk requires a prompt reaction when a threat materialises, while with this long time frame in updating the evaluation model, the bank risks to undergo too heavy damages. Consequently, the process might be revised at least once a year or more.

Another suggestion is to analyze the NIST Framework for Improving Critical Infrastructure Cybersecurity, elaborated from the FSSC, in 2014, which is a conceptual theoretical framework that focuses on the internal organisation of financial institutions and has the

fundamental aim to clarify the understanding of the organisation's business drivers and security procedures. The Framework refers to the risk management process to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. From this document there may be some interesting steps in implementing the procedure.

Furthermore, in 2015, CIS Sapienza in cooperation with CINI Cyber Security National Laboratory National Interuniversity Consortium for Informatics translated and adapted the NIST Framework to the Italian context, considering both listed companies and small- and medium-sized enterprises, underlying the differences and the specific problems in implementing the framework.

5. Conclusions

This research is a case study, in which we studied in depth the cyber risk management mechanisms of one Italian credit cooperative bank, by delineating the key characteristics of the model implied.

There emerged the difficulties of this small reality to sustain costs related to the management of cyber risk, in fact the elaboration of the methodology is outsourced.

However the topic of cyber crime and threats cannot be underestimate because of the potential impact on reputation, image and market share.

Therefore it is essential, despite laws and regulations, to develop, spread and communicate the right culture at every level of the organisation because every company bases its own activity on people and their values. The proper organisational behaviour impacts on growth and value-creation, not only of the bank itself, but in particular on the local community in which the BCC operates because sound corporate governance and internal controls have become the determinant elements for the stability of every single institution and of the overall financial system.

This last element can help underline that this study represents the second step of a far deeper analysis regarding the risk management process in credit cooperative banks. In the following analyses we would like to compare and contrast other realities, elaborating a multiple case-study. It would be interesting to evaluate the impact of cyber risk on the overall performance and on the efficiency of these banks.

References

Abbott, A. (2004). Methods of Discovery: Heuristics for the Social Sciences. New York: W.W. *Norton*

Agostini S., (2009), Le banche di credito cooperativo, Cooperativa e consorzi, n.10, Ipsoa, Milano

Álvarez, V. A., and Rossignolo A.F., (2015), Comparative Analysis of Techniques (IMA) for Determining Minimum Capital Regulated by Basel, Facing Crises in Emerging Markets, Social Science Research Network. ODEON (8),13-14. Available at SSRN: http: //ssrn.com/abstract = 2566754 .

Angelini, P., L. Clerc, V. Cúrdia, L. Gambacorta, A. Gerali, A. Locarno, R. Motto, W. Roeger, S. Van den Heuvel, and J. Vlček, (2011), Basel III: Long-Term Impact on Economic Performance and Fluctuations, Federal Reserve Bank of New York Staff Report, 485.

Appio, C.L., (1996), Le banche di credito cooperativo tra Testo Unico e disciplina del diritto comune, in Dir. banc. merc. Fin.

Banca d'Italia, Circolare n. 263 del 27 novembre 2006, Nuove disposizioni di vigilanza prudenziale per le banche, www.bancaditalia.it

Banca d'Italia, *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, www.bancaditalia.it

Banca d'Italia**,** *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 - in January 2014, www.bancaditalia.it

Baxter, P., and Jack, S. (2008). Qualitative case study methodology: study design and implementation for novice researchers, The Qualitative Paper, 13(4), 544-559

Biener, C., Eling, M., Wirfs, J.H. (2015). Insurability of Cyber Risk: An Empirical Analysis, Working Paper of Finance, Universit of St.Gallen, no. 2015/3, 31 pp.

Blackburn, R. and Kovalainen, A. (2009). Researching small firms and entrepreneurship: Past, present and future. International Journal of Management Reviews, 11(2), 127–148.

Bonfante, G.,(2010), La nuova società cooperativa, Zanichelli, Bologna

Capriglione, F., (2005), Le banche cooperative e il nuovo diritto societario. Problematiche e prospettive, in Banca borsa tit. cred.

CIS Sapienza and CINI (2015) Italian Cyber Security Report. Un report nazionale per la cyber security., www.cybersecurityreport.com [Last accessed: February, 2017]

Costa, C., (2007), La riforma delle società e le banche cooperative, in Il nuovo diritto delle società: Liber amicorum Gian Franco Campobasso, Torino

Curran, J. and Blackburn, R. (2001). Researching the Small Enterprise. London: Sage.

Davis, M. S. (1971). That's interesting! Towards a phenomenology of sociology and a sociology of phenomenology. Philosophy of Social Sciences, 1, 309–44.

D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali", and subsequent measures of 10.13.2008 and 11.27.2008

European Central Bank, Recommendations for the Security of Internet payments, January 2013, www.ecb.europa.eu

Ferri, G. and M. Messori (2000), Bank–firm relationships and allocative efficiency in Northeastern and Central Italy and in the South, Journal of Banking and Finance 24, 1067–1095.

Gummesson, E. (1988). Qualitative methods in management research. Lund, Norway: Studentlitteratur, Chartwell-Bratt.

Hartley, J.F. (1994). Case studies in organizational research. In Qualitative methods in organizational research: A practical guide, edited by C. Cassell and G. Symon, 209–29. London: Sage.

Hieb, J.L. (2007). Cyber security risk assessment for SCADA and DCS networks, ISA Transactions, 46(2007), 583-594

Hoffmann, A., and Ramaj H. (2011). Interdependent risk networks: the threat of cyber attack, International Journal of Management and Decision Making, 11(5/6), 312-323

ISACA Cobit 5 for Risk, www.isaca.org

ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements, www.iso.org

ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management, www.iso.org

ISO 31000 Risk management - Principles and guidelines, www.iso.org

Labie M., Perilleux, A., (2008) Corporate Governance in Microfinance: Credit Unions, CEB Working Paper n. 08/003

Laurence, A.G., Loeb, M.P., and Sohail, T. (2003). A Framework for Using Insurance for Cyber-risk Management, Communications of the ACM, 46(3), 81-85

Leonard-Barton, D. (1990). A dual methodology for case studies: Synergistic use of a longitudinal single site with replicated multiple sites. Organization Science, 1 (3), 248–66.

Meyer, C.B. (2001). A case in Case Study Methodology, Field Methods, 13(4), 329–352

MMC Cyber Handbook (2016). Increasing Resilience in the digital economy, Global Risk Center, www.mmc.com [Last accessed: February, 2017]

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

Mukhopadhyay, A., Saha, D., Chakrabarti, B.B., Mahanti, A., and Podder, A. (2005). Insurance for Cyber-risk: A Utility Model, Decision, 32(1), 153-169

National Institute of Standards and Technology. (2017). Framework for Improving Critical Infrastructure Cybersecurity,www.nist.gov/cyberframework [Last accessed: February, 2017]

Öğüt, H., Raghunathan, S., Menon, N. (2010). Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection, Risk Analysis 31 (3), 497–512

PricewaterHouseCoopers, Enhancing business resilience: Transforming Cyber risk management through the role of the Cief Risk Officer (CRO), December 2015, www.pwc.com/financialservices

Sykes, W. (1990). Validity and reliability in qualitative market research: A review of the literature. Journal of the Market Research Society, 32 (3), 289–328.

Smith, D.J., Cargill, T.F. and Meyer, R.A. (1981) Credit unions: an economic theory of credit unions, The Journal of Finance, 36(2), 519–528

Usai, S. and M. Vannini (2005), Banking structure and regional economic growth: lessons from Italy, Annals of Regional Science 39, 691–714.

Vella, F., (2004). La governance delle società cooperative, in La riforma delle società cooperative, a cura di Borzaga – Fici, Trento

Zago, A., Dongili, P., (2014), Financial Crisis, Business Model and the Technical Efficiency of Italian Banche di Credito Cooperativo, Quaderni di ricerca del credito cooperativo, n.4, www.creditocooperativo.com