ABOUT THE REAL VALUE OF KNOWLEDGE, INTELLECTUAL CAPITAL AND RESILIENCE IN THE NEW COGNITION ECONOMY

Călin M. RANGU[1]

Financial Supervision Authority, Romania

Abstract

The society in which we live is defined as a knowledge society, and the economy is a post knowledge economy which is a mixture of knowledge and networks. In Intellectual Capital (IC) terms this means that Structural Capital (SC) derived from Human Capital (HC) and Relational or Strategical Alliance Capital (SAC) are becoming the key aspects.

People possess IC based on knowledge like intangible, explicit or tacit assets.

They hold some values, informally recognized, but often formally ignored. Cyberattacks target exactly these values.

The word "knowledge" has many valences. One being targeted by cybercrime (money, identities, intellectual property, etc.).

One of the main problems is that knowledge does not provide you with skills, and knowledge-skills fracture leaves free attacks, fraudulent practices, astronomical losses brought by cybercrime.

Accounting standards remain a tribute to classical principles not adapted to the reality of the knowledge society. For this reason, the value of the assets lost as a result of cyber losses is difficult to quantified. This is partially caused because companies have inventory of their tangible assets whilst most cyber-crime focusses on intangible assets which rarely have inventory. This can partially be dealt with by using enabling technologies such as machine learning, Artificial Intelligence and robotics. This is best seen in the extremely low level of cyber risk insurance. We should take policies, strategies to cover this gap.

At human level it is necessary to shift from the accumulation of knowledge to the development of skills, to cognition.

At the accounting level it is necessary to create the system of evaluation and registration of intangible assets of knowledge and networks, human, structural and relational capital.

[1] Corresponding author, **Calin Randu** - calin.rangu@asfromania.ro

Keywords: capital intelectual, risc cibernetic, active

JEL Clasification:: D81, G22, H56, M15

1. About cyber risk and (un)known or (un)covered assets

If we are looking technically, cyber-attacks lead to disruption of activities/business, by freezing public or private infrastructures, productive, financial infrastructures, etc. affecting people and property, through compromising the confidentiality, availability or integrity of the data or services[2]. But that's the effect. The cause is human, we are talking about people and their assets that are affected, people who are assuming responsibilities and taking actions, or those who disregard them with good science or ignorance. In the same time fellows orchestrate and attack.

According to the thematic analysis of the Romanian Financial Supervisory Authority (A.S.F.) on cyber risk insurance[3], the management of institutions and companies in the same time with employees are responsible for, the role of people being essential.

Institutions or companies need a comprehensive cyber-risk management strategy to return to normal operations as quickly as possible with the lowest cost. People need to develop skills in addition to the necessary technical education to provide them with basic knowledge. This knowledge, the experience gained must be monetized.

Education should not be found only at the expense cap, but also to intangible assets accumulated in the wake of education, to implement structures, procedures, knowledge-based mechanisms.

When talking about risks we are talking about threats (external, from those who have interest, knowledge and skills) on the one hand, and vulnerabilities on the other side (those who have intangible values of data type, information, monetary or identity value) who do not know, do not can, or do not have skills, cognition and no defense capabilities. All gains obtained by attacking intangible assets are also unlawful acquisition by affecting the image of companies or people, leaking information, disruptions of activities. **If someone is gaining, where is the loss recorded**, where are those assets that disappear, where we will see it in accounting? The fact is that they are not found in accounting as a direct loses, as assets destroyed. Maybe the goodwill will be affected. It creates problems in sizing the real loss. There are default problems in securing that loss. An insurer cannot ensure that even the owner of the active needle does not evaluate it prior to the risk of the damage to the product.

Threats may be **intentional** (criminal, terrorist, hostile, activism, blackmail or personal reasons), or represent **accidental events** (data deletions, service interruptions). **Estimating the cost of cyber incidents is a challenge**, companies avoiding reporting losses, whether they can't calculate them, or they don't want their image to be affected (another intangible asset of intellectual capital). The **damage caused by cyber risks** is estimated at around

[2]L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019

[3] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf [Accessed May. 09, 2019]

0.5% of the world's GDP and almost twice as much as the annual average of losses caused by natural disasters[4].

On the basis of a risk barometer, conducted by interviews on 968 participants, the main causes of the losses generated by cyber incidents were established in the year 2019 (Fig. 1):[5] 1. Business Interruption; 2. Loss of reputation; 3. Damage caused by data loss; 4. Data restoration costs; 5. Fines and penalties. Vulnerabilities can be covered with internal resources or by outsourcing the risk. The **residual risk**, which costs too much to be covered internally can be taken over by the insurance system. But this also leads to lack of knowledge and cognition in order to retrieve it. The cyber-risk coverage of only 2025 will cover 1% of total insurance, according to Swiss Re, while uncoated losses are huge.

According to L. Badea (2019) "The amount of financial losses generated by cyber risk is difficult to estimate, with a shortage of information. **Some cyber-criminality activities do not have a direct cost or cannot be quantified**.

Fig. 1. The main causes of economic losses caused by cyber incidents (Source: Allianz Risk Barometer, 2019)

The industry is attempting to estimate the total costs, costs per incident, and the cost of registering a data violation according to Table 1. Fig. 2 present estimates of average annual cybercrime costs by areas and main affected countries"[6].

Table 1. Estimated cybercrime costs (Source: Geneva Association, 2016)

[4] L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019
[5] Allianz Global Corporate & Specialty, „Allianz Risk Barometer" 2019
[6] Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, Nov 2016

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

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

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

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

According to Accenture, the biggest cyber-crime damage is registered in the field of loss of information stored electronically, followed by business, turnover losses and equipment damage (Fig. 2.):

According to L. Badea and C. Rangu (2019), cyber risk insurance can play a key role in taking over/transferring the risks to which companies and people are exposed. "This can be a tool that complements (and does not replace) the risk management framework that each organization should have and should be an element of economic and social stability, both for critical infrastructures, both commercial and personal, including for the financial sector. Cyber risk insurance should be used in assessing financial soundness/health and supporting activity through rapid recovery of losses and continued activity". But how to do it is the biggest challenge, in which IC methodologies are essential.

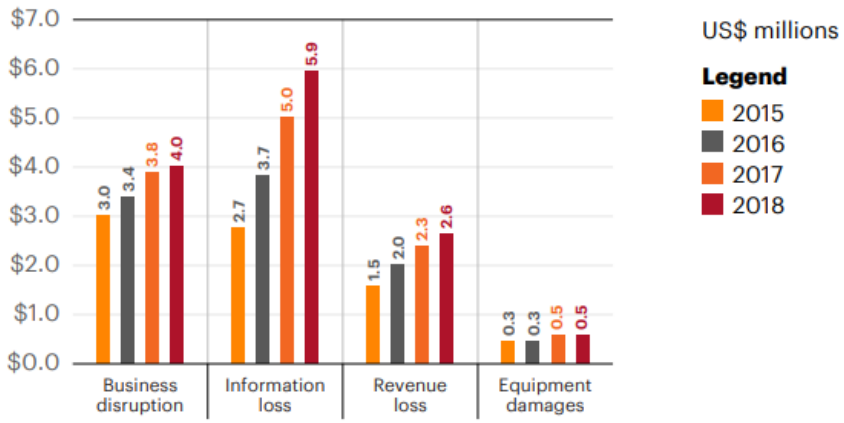

Fig. 2. Average annual cyber Crime costs on the main areas of losses (Source: Accenture, 2019)

2. About the Intellectual Capital (CI)

According to F. Stibli6 "intellectual capital of an organization is divided into four categories: human-centered assets, infrastructural assets, intellectual property assets and market assets". It can be seen that all these assets can be impacted cyberspace and can

generate profits to the attackers. Each of them should be evaluated, including monetary to be able to establish the risk picture, and protect them because "knowledge can be converted into value" according to Leif Edvinsson and Sulivan Pat. Thomas Davenport (Davenport, 1999) builds a model of the employee as an investor in human (educational) capital"[7]. He notes that in recent years, the number of highly specialized jobs has increased at all levels of education, to the detriment of unskilled, poorly specialized work, as well as managers on lower levels (major, team leaders etc.). Investing in lifelong learning thus appears as a priority for individuals and insurance against the risks of unemployment and poverty. On the other hand, companies can obtain a higher profit by investing, rather, in the education of their employees, than in increasing the stock of economic capital". Since 1999[8] it has been noticed that it would be time to define the concepts of intangible assets, human capital, and knowledge. The International Accounting Standard Committee - International Accounting STANDARD IAS 38 defines an intangible immobilization as a non-monetary identifiable asset, no physical substance. According to IAS 38 "intangible assets", an intangible asset is a nonmonetary identifiable asset, without material support and held for use in the production process or the supply of goods or services, to be rented to others, or in Administrative purposes. Particularities are represented by the identifiable nature, control over a resource and the existence of future economic benefits. The intellectual capital (CI) that interests us in this analysis are the Human capital (referring to knowledge, skills, motivation, team relationships, briefly all factors in relation to employees who promotes the performance that customers are willing to pay) and the Structural Capital, referring to "all that remained when people left the night" (Edvinsson & Malone, 1997, p. 17), such as databases, structure detailed procedures transposed into the software, etc.[9] The effective management of IC lies in managing the hybrids particularly HC-SC, SC-SAC, SC-CC, HC-SAC and HC-CC.

The human value is defined by OECD[10] as being the knowledge, skills, competences and attributes incorporated into individuals that facilitate the creation of a personal, social and economic goodwill. Education is not the only or main form of HC development. Experience, insights and networks may be equally important. But Education is important for human capital development. In the company's records we only have the expense of the studies, not the human asset as an additional human value. Man/woman is the only asset that should be continuously appreciated, compared to the other assets that are continuously depreciating. There are researchers such as Ludo Pyis from Areopa which also proposes the formula for calculating the human value. When the human asset is evaluated, it will find it placed in the balance sheet/accounting balance of company, then the man will be positioned correctly in the company, in society. But for that, the general ledger and accounting methods have to be updated, and there are specific methodologies.

---

[7]F. Stibli, Intellectual capital - the key resource for expanding organisational intelligence, https:// intelligence.sri.ro/capitalul-intelectual-resursa-cheie-pentru-extinderea-inteligentei-organizationale/ [Accessed: May. 10, 2019]

[8] 10 June 1999 HOLISTIC MEASUREMENT OF INTELLECTUAL CAPITAL COUNTRY covered: AUSTRIA RESEARCH TEAM: Manfred Bornemann, Karl Franzens University Adolf Knapp, Karl Franzens University

[9] Edvinsson Malone Intellectual Capital, Realizing your Company's true Value by finding its hidden Brainpower. New York: Harper Business, 1997, p. 17

[10] Human Capital-The Value of People https://www.oecd.org/insights/humancapitalthevalueofpeople.htm

An example is the Wissensbilanz -the declaration on intellectual capital - developed by Fraunhofer Institute[11] which is 'an instrument essential for maintaining the competitive advantage and maintaining their business successfully in the knowledgebased economy."

A generally recognized classification divides KBC[12] into three categories: "Computer information (software and database), innovative properties (patents, copyrights, design, trademarks) and economic skills (including capital Brand, company-specific human capital, people's networks and institutions and organizational knowledge that increase the efficiency of the Enterprise (Corrado, Hulten, and SIchel, 2005)". Thus appears the third important component of intellectual capital, the relational/customer capital. As a summary, the Table 2 define the main categories of IC phenomena.

According to AREOPA[13], „apart from Structural Capital, the base IC classes are in fact shared capital. For instance, Human Capital (HC) is shared with its 'owners': when a staff member decides to leave the organization, he/she takes his/her skills and competences, reputation and potential along. Similar rules apply to both Customer Capital (CC) and Strategic Alliance Capital (SAC): when the customer takes his business elsewhere or an alliance breaks up, the customer's revenue potential and partnership's leverage are gone. The consequence of this is that Intellectual Capital may flow from one sector into the next. And this is where management of IC comes into play. It is important for companies to realize where their IC is situated, and which actions need to be taken to convert IC that is at risk of being lost into IC that has become structural, i.e. to structuralize its Human, Customer and Strategic Alliance Capital to the maximum extent possible".

Table 2. IC calculation building blocks (Source: Areopa slides, Guthrie, 2001)

[11] Wissensbilanz, https://www.academy.fraunhofer.de/en/continuing-education/technologyinnovation/intellectual_capital_statement.html

[12] OECD (2013), "Introduction and Overview", in Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing, http://dx.doi.org/10.1787/9789264193307-4-en

[13] Ludo Pyse, NO CURE, NO PAY? Would applying this rule bring IT projects failure statistics down? … and how do we measure sure success?, ww.areopa.com

Intellectual Capital Calculation
Building Blocks – Elements/Phenomena

	Human Capital	Customer Capital	Structural Capital (Organizational Capital)
GUTHRIE (2001)	• Know-how; • Education; • Vocational qualification; • Work-related knowledge; • Work-related competencies; • Entrepreneurial spirit • Innovativeness, • Proactive and reactive abilities • changeability	• Brands • Customers • Customer loyalty • Company names • Distribution channels • Business Collaborations • Licensing agreements • Favourable contracts • Franchising agreements	• Patents • Copyrights • Trademarks • Management Philosophy • Corporate Culture • Management processes • Information Systems • Networking Systems • Financial Relations

Their conclusion is that „the knowledge company travels light. …Not only are the key assets of a knowledge company intangible, it's not clear who owns them or is responsible for caring for them."

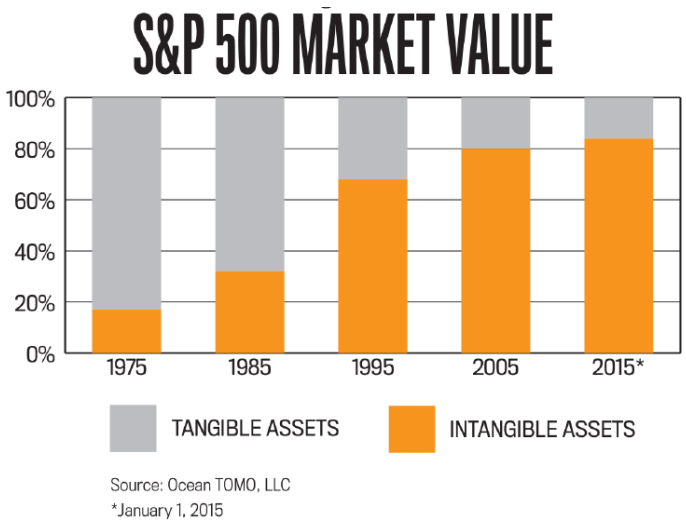

Fig. 3. The evaluation of intangible assets in S&P 500 Market Value (Source: G. Cokins, 2017)

According to Cokins, G. and Shepherd, N. (2017), figure 3 shows how "hidden value" can be made visible. The left side of the Figure represents the publicly disclosed financial statements prepared according to Generally Accepted Accounting Principles (GAAP) or

International Financial Reporting Standards (IFRS). First consider the published balance sheet at the top. Early efforts to understand and quantify the difference between the book value and the adjusted value with added intangible assets can be traced back to the early 1990s and the rise of knowledge management and intellectual capital. More recent and ongoing work in the science of valuing intellectual capital has been undertaken and published by AREOPA, a thought-leading consulting firm specializing in this area"[14].

Gary Cokins[15] (2017) show clear in fig. 4 that the new world is of the intangible assets and „the traditional balance sheet understates the economic value of a company because it doesn't include a large portion of intangible assets…..Forty years ago, more than 80% of the average valuation of companies on the S&P 500 was represented by tangible assets such as property, plant, and equipment—the majority of which were reflected on an organization's balance sheet. - the number is now reversed with more than 80% of an organization's attributed value represented by intangibles such as its intellectual capital, workforce, supply chains, and other key relationships.

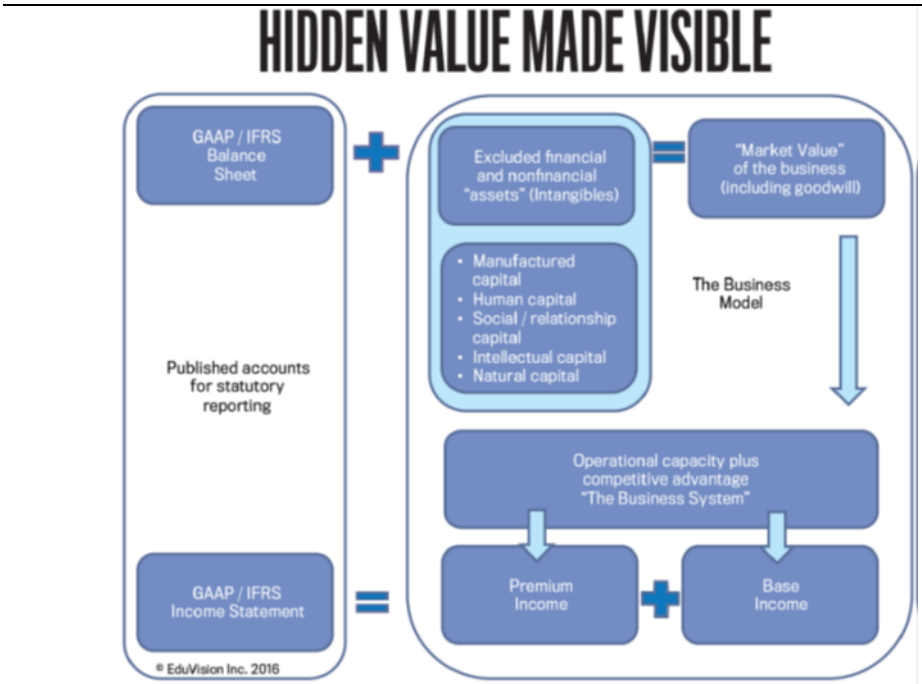

Fig. 4. Hidden Value Made Visible Source G. Cokins, 2017

From an accounting perspective, this has driven the growth in calculating a goodwill amount as organizations have been bought, sold, and amalgamated, and the excess of the

[14]THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, https://sfmagazine.com/post-entry/may-2017-the-power-ofintangibles/
[15] THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, https://sfmagazine.com/post-entry/may-2017-the-power-ofintangibles/

purchase paid over accounting book value has been reported as goodwill. A recent article by Bloomberg quoted a Goldman Sachs Global Investment Research study that showed the continued growth in goodwill in U.S. companies reached $2.5 trillion dollars overall by 2015. (See https://bloom.bg/2pIcKNS.)".

3. Assessment of Intellectual

Capital European Commission mentions in the Intellectual Property Valuation Report[16], in 2013 "the opportunity of, if not need for, leveraging on intangibles, and especially those with a legal recognition, such as brands and IPRs, for favoring innovative and more knowledge-consistent forms of bank financing for company growth and investment processes. This is particularly true for European research-intensive SMEs".

EU is stressing "the need for developing new segments of financial markets devoted to the valuation, exchange and funding of IPRs and other intangibles, by creating the necessary pre-conditions and infra-structures for such markets to operate in an efficient and effective way on a European scale"[17].

The lack of measurement of intangibles at micro-level (i.e. company) is another recurrent policy priority which underlies many of the above issues. Shared methods for valuation and accounting are a relevant basic issue which may explain the difficulty to see intangibles in company annual financial statements and disclosures. This issue is particularly true for internally generated intangibles; such are - in many cases - the IPRs. As Mr. Hans Hoogervorst, Chairman of the International Accounting Standards Board (IASB), pointed out recently[18] "Intangible assets go unrecorded (or underrecorded) on the balance sheet…. we know that the [accounting] standard [IAS 38] is rudimentary because it is based on historical cost, which may not reflect the true value of the intangible asset". A brief analysis of international practices for the development of Intellectual Capital reports[19] can mention by Brooking[20] which fragments in four categories: Human-centered assets; Infrastructural assets; Intellectual property assets; Market assets.

Leif Edvinsson has made a standardized model and language for the presentation of the CI. Edvinsson concludes that the result of a decrease in the accounting value of an organization's market value actually signifies the CI existing in that organization, according to the formula:[21]

Market value = Financial Capital + CI

[16] https://ec.europa.eu/research/innovation-union/pdf/KI-01-14-460-EN-N-IP_valuation_Expert_Group.pdf
[17] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=11602&no=1
[18] https://magazine.lucubrates.com/intellectual-capital-and-knowledge-management/
[19] http://www.incd2020.ro/sites/default/files//Analiza%20bune%20practici%20intl%20rapoarte%20CI.pdf
[20] Brooking A., 1996. Intellectual Capital: Core Asset for the Third Millennium Enterprise. New York: International Thomson Business Press
[21] Leif Edvinsson Intellectual Capital: Realizing Your Company's True Value by Finding Its Hidden Brainpower Hardcover, 1997

Leif Edvinsson[22] has decomposed the CI in four distinct areas: Human capital; Customer capital; Process capital; Innovation capital. L. Pyis[23] presents eloquently in Fig. 5 the stages by which the bits pass through the date due to the implementation of a syntax, to information through semantics, to the actual knowledge due to the placement in context, know-how, experience and expertise through use, by practice and an effective approach. We note that at each level the cyber risk is there, the intellectual capital assets are more valuable and interested for both the company and the external factors.

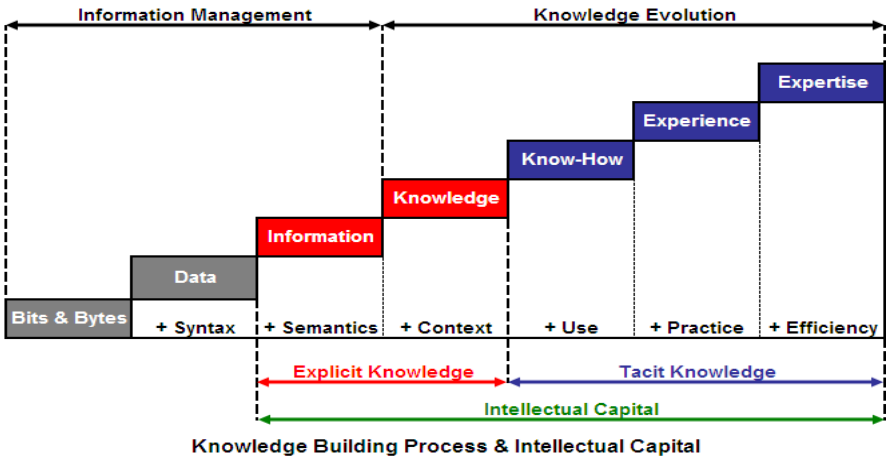

Fig. 5. The IC Building Process (Source: Areopa, 2015)

If we analyzed the risks posed by the brainstem they are related to the operational risks of those generated by people, processes and systems.

Intellectual capital deals with: Human Capital Control, Structural Capital Control, Controlling the relational capital and alliances.

IT is the entry into change management and knowledge management, risk management, evaluation, coverage and insurance. According to AREOPA:

- Knowledge is critical in time, virtual, now relevant, reflective, complex, evolving, interactive, untidy, created for a purpose, but based on past, social, often self-organizing experience, carried out by questions, challenges and debates, filter, creative, selective.

- Knowledge is found in presentations, reports, journals, licenses, patents, licenses, intellectual property, databases, software, risk instruments, audits, libraries, catalogues, archives, manuals, policy documents, memoirs, individual capacity, memory, know-how, experience, teams, communities, groups, networks.

[22]https://www.researchgate.net/profile/Selcuk_Burak_Hasiloglu/publication/28263308/figure/fig1/AS: 394353668313091 @ 1471032649090/Edvinssons-Categorization-of-Capital-Resource-LeifEdvinsson-and-M-S-Malone.png
[23]Ludo PYIS, AREOPA GROUP, IS IT WORTH PROTECTING YOUR INTELLECTUAL CAPITAL FOR CYBER INTRUDERS (PPT presentation), 2013

- Explicit knowledge is easily identifiable, re-usable in a consistent and repeatable manner-for decision making and/or for the exercise of judgement, can be stored as a written procedure or as a process in a computer system, stored as artifacts-artificial, physical or virtual entities that can be measured, identified, distributed and audited.

- Tacit knowledge are as lessons learned, methodologies, cases, stories, staff, specific context, difficult to formalize and communicate, insights, mental rules, mind sets, unwritten rules, values unconsciousness, the fundamental philosophy.

Karl-Erik Sveiby proposed a model for the methods to evaluate IC in accordance with Fig 6, in four categories: market capitalization, return on assets, direct IC, score card methods.

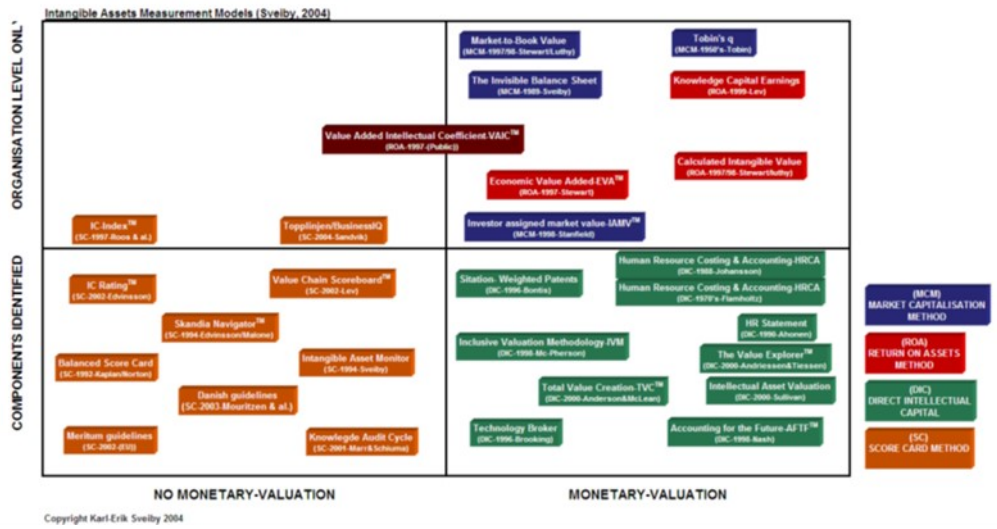

Fig. 6. The model for the methods to evaluate IC (Source: Areopa slide, 2015)

Starting from this approach Areopa proposes a calculation model, from unstructured to the very structured intellectual capital types.

AREOPA has developed such a model for identifying and quantifying intangibles as components of Intellectual Capital (IC). This model serves to evaluate a company's return on all the capital it employs, helping to explain the difference between book and market value. It also provides guidance as to how and where management should put its attention to grow the organization's overall IC.

Starting from the new IAS 38, Lucurbate Peter Walch mention that „accounting for IC does in fact create a supplementary balance sheet also based on the debit and credit system in the same way as financial accounting standards. Thus IC accounting creates a recognition of otherwise not-reported or off-balance sheet assets. The charts below should be studied carefully"[24].

[24] Lucubrate Peter Welch October 12th, 2018 Magazine article No: 42, October 8th, 2018

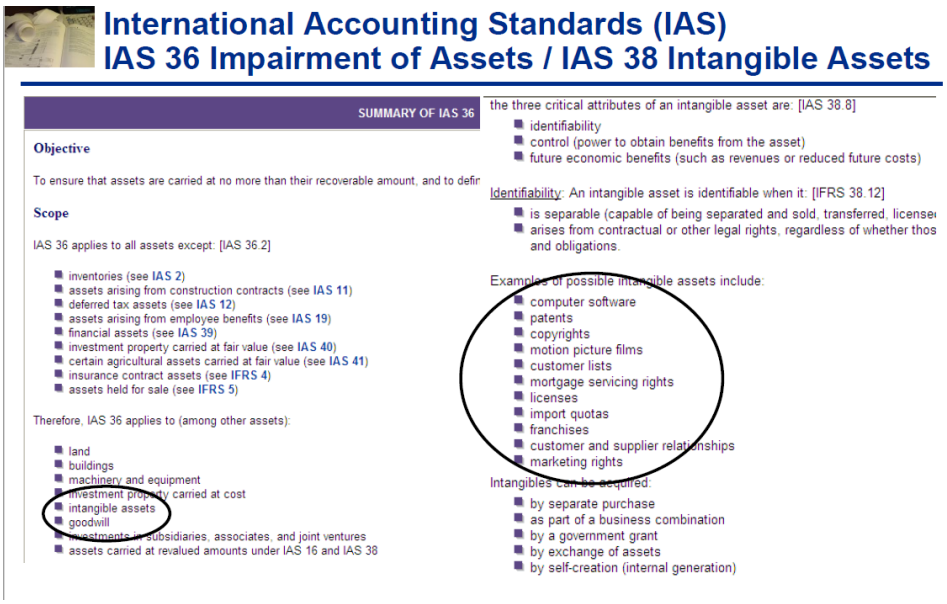

Fig. 7. Summary of IAS 36 (Source: Welch, 2018)

On the basis of this model Areopa proposed a model of the balance sheet relating to the intellectual capital to be complementary but integrated to the classical one, as defined over 400 years, an example refining in Fig. 8.

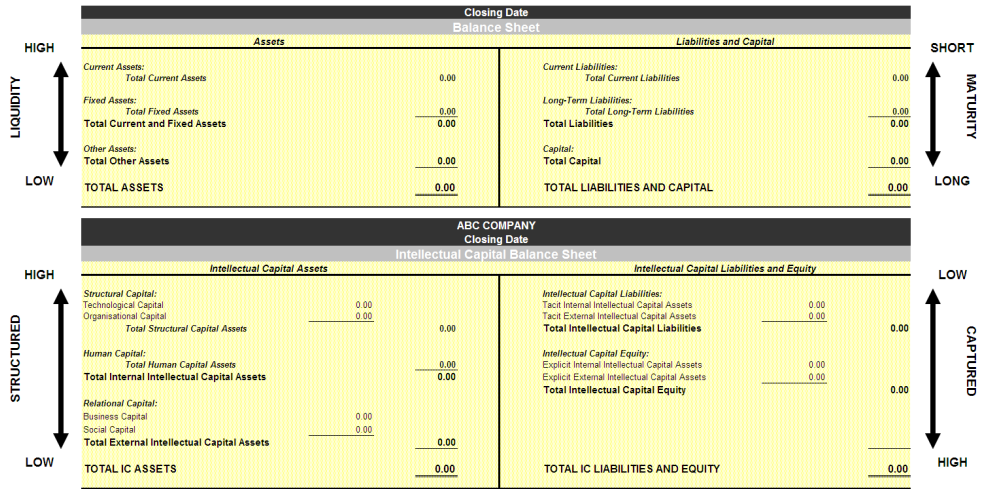

Fig. 8. IC Balance Sheet: Follows the structure logic of the FINANCIAL BS (Source: Welch, 2018)

Accountability should be connected knowledge and network economy, to cyber world, to face the cyber-threats because the real IC is not protected at all, intellectual property (patents, author rights, trademarks etc.) representing only few percent of the IC.

Cyber-attacks escape only the IC that is captured, stored and made reusable through the computer, the explicit knowledge, which is in the form of data, information, know-how, etc. But they can also attack the tacit knowledge, the development plans, which can be found in emails, R&D, at developers, strategic exchanged of top management etc.

4. Building resilience

Mrs. Sabine Lautenschlager, member of the ECB, mentions[25] that for the financial market the information, knowledge and expertise of public institutions and industry will be essential because:

- Close interconnection and complexity of the financial system creates vulnerabilities that can be exploited by cyber attackers.

- The attackers seem to gain an ever deeper understanding of how the financial system operates. This allows them to quickly detect and exploit weaknesses in a more efficient way and should be a concern for all of us.

- Both banks and financial market infrastructures strive to find staff with the skills and experience necessary to prevent cyber-attacks. Lack of skills extends far beyond the financial sector. All relevant stakeholders must urgently work on strategies to ensure that the workforce has the skills needed for our future economies and that our society is able to seize the advantages of innovation.

- True innovation is always disruptive. Fintech could disrupt financial markets in positive ways. But it also comes with risks: a more violent competition could lead some market players to adopt and adopt new technologies, services or methods, before taking full advantage of the associated risks-cyber risks in this case.

In March 2017, the governing Council of the IMF endorsed the Eurosystem's cyber resilience strategy. In fact, we are talking about the resilience of these intangible assets, data, information, knowledge, assets, identities, know-how. These assets have immense value. We must be able to inventory, evaluate, measure, appear in the accounting systems, so that we can secure them.

According to L. Badea (2019), to identify the risk we should evaluate:

- The business processes relevant to the cyber risk, with their assets and their corresponding values, must be established.

- Data on weaknesses must be collected, always in connection with existing assets, threats and protection methods. A first potential risk identification indicator can be ensured by the cyber risk self-assessment. For example, methods proposed by specialized companies in the distribution of such insurance[26]. These tools can help determine the risk exposure and

[25]https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_1~5803aca48c.en.html
[26] http://www.marsh-stresstest.eu/.

awareness of the risk of the company and provide indications for the risks still unidentified. Another aspect would be how an attack of cyberspace can be detected as soon as possible from the time when it happened. A tool for analyzing the consequences of operations is of course the Business Impact Analysis (BIA).

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

In general, the transfer of risk is possible by purchasing an insurance contract.

5. Conclusions

In order to achieve the correct positioning of intellectual capital assets of the post-knowledge economy, part of the cognition society, and for a more resilient cyber space, the following conclusions are revealed:

- We are leaving in other economy, in a cognition economy, and we should define it correctly, including new tools and methodologies

- The human layer positioning is essential for a correct set-up of the cyber world and to act against cyber-attacks over knowledge assets. The set-up of Intellectual Capital Excellence Centers will promote and keep in country people with knowledge, know-how, expertise.

- It is vital to formulate and to assume policy and to support the regulation of cyber risk by reducing political, social and economic impacts[27]. These policies will have beneficial effects on both demand and supply levels.

- It is essential to establish a new accounting framework for assessing knowledge and networks economy. Also, to establish a system for the reporting of losses generated by cybercrime and policies for cyber insurance.

- It is necessary to develop and use evaluation models, based on internationally recognized standards and certifications, in an auditable way, based on new skills in the engineering of cyber risks.

- Cyber risks require the achievement of a common front to increase the level of cyber-maturity and cybersecurity, application of the principles of risk management and for combating cybercrime.

- Human, structural and relational/customer capital should be reflected in balance sheets and calculated as knowledge assets part of Intellectual Capital of companies.

[27] L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019

References

[1] Allianz Global Corporate & Specialty, „Allianz Risk Barometer" 2019.

[2] Brooking A., 1996. Intellectual Capital: Core Asset for the Third Millennium Enterprise. New York: International Thomson Business Press.

[3] Edvinsson Malone Intellectual Capital, Realizing your Company's true Value by finding its hidden Brainpower. New York: Harper Business, 1997, p. 17.

[4] F. Stibli, Intellectual capital - the key resource for expanding organisational intelligence, https://intelligence.sri.ro/capitalul-intelectual-resursa-cheiepentru-extinderea-inteligentei-organizationale/. [Accessed: May. 10, 2019].

[5] Human Capital-The Value of People https://www.oecd.org/insights/ humancapital-thevalueofpeople.htm.

[6] L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019.

[7] Leif Edvinsson Intellectual Capital: Realizing Your Company's True Value by Finding Its Hidden Brainpower Hardcover, 1997.

[8] Lucubrate Peter Welch October 12th, 2018 Magazine article No: 42, October 8th, 2018.
[9] Ludo PYIS, AREOPA GROUP, IS IT WORTH PROTECTING YOUR INTELLECTUAL CAPITAL FOR CYBER INTRUDERS (PPT presentation), 2013.

[10] Ludo Pyse, NO CURE, NO PAY? Would applying this rule bring IT projects failure statistics down? … and how do we measure sure success?, ww.areopa.com.

[11] Manfred Bornemann, Karl Franzens University Adolf Knapp, Karl Franzens University, 10 June 1999, Holistic measurement of intellectual capital country covered: Austria research.

[12] OECD (2013), "Introduction and Overview", in Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing, http://dx.doi.org/10.1787/9789264193307-4-en.

[13] Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, Nov 2016.

[14] THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, https:// sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/.

[15]Wissensbilanz,https://www.academy.fraunhofer.de/en/continuing-education/technology-innovation/intellectual_capital_statement.html.

[16]https://ec.europa.eu/research/innovation-union/pdf/KI-01-14-460-ENNIP_valuation_Expert_Group.pdf.

[17]http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=11602&no=1.

[18]https://magazine.lucubrates.com/intellectual-capital-and-knowledgemanagement/.
[19]http://www.incd2020.ro/sites/default/files//Analiza%20bune%20practici%20intl%20rapoarte%20CI.pdf.

[20]https://www.researchgate.net/profile/Selcuk_Burak_Hasiloglu/publication/28263308/figure/fig1/AS: 394353668313091 @ 1471032649090/ Edvinssons-Categorization-of-Capital-Resource-Leif-Edvinsson-and-M-SMalone.png.

[21] https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf. [Accessed May. 09, 2019].

[22]https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_1~5803aca48c.en.html.

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