A Novel Model for Cybersecurity Economics and Analysis

Paresh Rathod
Laurea SID,
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo, Finland
paresh.rathod@laurea.fi

Timo Hämäläinen
Department of Mathematical Information Technology,
University of Jyväskylä
P.O. Box 35, FIN40351 Jyväskylä, Finland
timo.t.hamalainen@jyu.fi

Abstract*—In recent times, major cybersecurity breaches and cyber fraud had huge negative impact on victim organisations. The biggest impact made on major areas of business activities. Majority of organisations facing cybersecurity adversity and advanced threats suffers from huge financial and reputation loss. The current security technologies, policies and processes are providing necessary capabilities and cybersecurity mechanism to solve cyber threats and risks. However, current solutions are not providing required mechanism for decision making on impact of cybersecurity breaches and fraud. In this paper, we are reporting initial findings and proposing conceptual solution. The paper is aiming to provide a novel model for Cybersecurity Economics and Analysis (CEA). We propose an innovative model for an optimal cybersecurity cost-benefit framework to help decision-making based on a combination of qualitative and quantitative analysis of the cybersecurity risks and their impact on organizational tangible and intangible assets. Cybersecurity Economics and Analysis utilizes a holistic approach to cybersecurity, proposing a model based on a deep and comprehensive analysis of organisations' security – considering not only technological perspectives, but institutional, economic, governance and human dimensions – taking forward existing 'best' and effective practices from national audit frameworks, sectoral guidelines and organisational policies. This new solution will account for the wants and needs of various stakeholder groups and existing sectoral requirements. We will contribute to increasing harmonization of European cybersecurity initiatives and reducing fragmented practices of cybersecurity solutions and also helping to reach EU Digital Single Market goal. By introducing Cybersecurity Readiness Level Metrics the project will measure and increase effectiveness of cybersecurity programs, while the cost-benefit framework will help to increase the economic and financial viability, effectiveness and value generation of cybersecurity solutions for organisation's strategic, tactical and operational imperative. The ambition of the research development and innovation (RDI) is to increase and re-establish the trust of the European citizens in European digital environments through practical solutions.

Keywords— cybersecurity economics; cybersecurity cost-benefit; cybersecurity cost-benefit model; advanced cyber threats; cyber fraud, cyber secure; cybersecurity impact, cybersecurity (key words)

I. INTRODUCTION

The European Commission and High Representative's 2013 Cyber Security Strategy [1] is aiming for safe and secure cyberspace that mainly benefits society and economy. The Impact Assessment clearly suggested three level of impacts: Level of Security, Economic Impacts and Societal Impacts. However, the problem described in the Impact Assessment Proposal [2] for a Directive of the European Parliament and of the Council states, "an overall insufficient level of protection against network and information security incidents, risks and threats across the EU (European Union) undermining the proper functioning of the Internal market." There are practical challenges while implementing pan-European cybersecurity policy to reach the goal of Digital Single Market for all Member States serving over 500 million people and contributes €500 billion in European economy [3]; approximately €1000 per person. On the one hand, the Digital Single Market needs new digital technologies must be trustworthy, safe and secure for citizens. The safe Digital Single Market equally demands functional and effective security mechanism on three layers: people, processes and technologies. On the other hand, 2012 Special Eurobarometer 390 on Cybersecurity states, "Unfortunately, a 2012 Eurobarometer survey3 showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases. An overwhelming majority also said they avoid disclosing personal information online because of security concerns. Across the EU, more than one in ten Internet users has already become victim of online fraud." Therefore, it is evident that the Digital Single Market demands holistic and cost effective cybersecurity solutions.

The Cybersecurity Economics and Analysis research development and innovation study bridges together the traditional focus on technological aspects of cybersecurity frameworks and certifications with its economic and social impacts, developing a new effective and holistic practice framework. While it remains possible to assess with a reasonable degree of accuracy the direct costs of implementing cybersecurity audits, the long-term impacts and benefits of implementing cybersecurity principles at a holistic level are still unclear. CEA creates a case for evaluating the long-term value that increased resilience to cybercrime can bring to society through the development of new transdisciplinary cost-benefit model, building on identified existing best practices and the tangible, 'real- world' requirements of domain experts and stakeholders, drawing upon knowledge not only from a technological perspective,

but also including economic, sociological and other perspectives.

The Cybersecurity Economics and Analysis aims at creating a socio-economic model for an optimal cybersecurity cost-benefit framework to help decision-making based on a quantitative analysis of the cybersecurity risks and their impact on organizational tangible and intangible assets. CEA adopts a wider perspective to economics of cybersecurity, based on strategic, long-term thinking incorporating economics from the outset. The CEA will provide benchmarks for the economic assessment of national and international cybersecurity audits and standards and provide policy recommendations for the alignment of policies and regulations to ensure trust within European citizens and digital environment.

The paper is structured and divided in six sections, starting with a research background and current state of research studies. The first section also formulates research gap and problems. The current research challenge described in section two. The third section is covering the concept of the research and development work. Section four is presenting and justifying research method used in research study. Further, we are presenting conceptual solution and model. Finally, we are exploring other possibilities, discussion and future direction.

II. BACKGROUND AND CURRENT CHALLANGES

The Internet and the broader concept of 'cyberspace' has, over the last 10 years, provided businesses with new opportunities for competitive advantage against competitors and a new vector for further economic growth. At the same time concerns about the security of cyberspace have also grown exponentially as criminals are continuously looking to exploit this new environment for their own economic benefit. Increasingly, a priority concern in this regard is associated with the potentially sensitive, classified and personal information that is stored and processed by organisations - often related to their supply chain, customers and employees. One commonly used tool to take control and to protect information in cyberspace is an information security management system (ISMS). ISMS' are designed to maximise business continuity and minimise risk, defining the policies, procedures and governance needed to secure organisations sensitive data and protect against the risk of cybersecurity breaches. ISMS typically aim to cover the full spectrum of businesses knowledge assets, from data and technology to employee behaviour and business culture. Standards such as ISO/IEC 27001 provide internationally recognised and accredited specifications for the creation of an ISMS. However, there is a growing sense of urgency for multidisciplinary, flexible and adoptable cybersecurity frameworks that go beyond the baseline set by these standards, and make provisions for conditions that arise as a result of the rapidly changing cyber threat landscape and the new and evolving risks that emerge as a result.

While security audits and certifications have been increasingly used in both the public and private sectors, they are often based on generic models and are not wholly applicable and interoperable across all organizations and sectors. These audits primarily address the technological aspects of cybersecurity, i.e. compliance with security requirements. While cybersecurity/cybercrime metrics and statistics are available in a variety of data types, the economic value, especially in the long term, of these metrics is often missing or hard to evaluate (as in the case of reputation loss). In addition, the available metrics and consistency of overall cybersecurity terminology is not always clear. Lack of common definitions and methodologies leaves open the possibility of misinterpretation and thus can result in big differences when assessing the economic implications of cybersecurity incidents. It also creates a challenge for government bodies when devising cybersecurity policies providing due to the availability of many contrasting methodologies and a shortage of reliable data.

A. Current Cybersecurity Challenges and Research Gap

On the one hand, we have asynchronous cybersecurity practices, many standards and frameworks to cope with while on the other hand, nation-states, online criminals, organised hacktivists, insider threats and hackers with malafide intentions to deal with. The Center for Cyber Safety and Education's Global Information Security Workforce Study (GISWS) conducted in year 2015 confirms that globally we are not only loosing but also backpedalling against aforementioned threats and risks at cyberspace [4]. One of the key reasons of rapidly increasing breaches denoted to "attack surface" [5] (the set of ways in which an adversary can attack the system) in addition to increasing vulnerabilities, number of internet users, and number of users accessing online resources. How do organisations conduct and practice their cybersecurity to protect against dramatic attack surfaces? And most importantly, how do they allocate limited cybersecurity resources in defence? Most organisations advices to adopt more systematic approaches using standards, framework, audits and best practices. However, ENISA's recent study [6] also confirms that there are gaps in existing systematic approaches of cybersecurity.

Taking into account the results of existing EU projects looking at defining priority research areas associated with cybercrime and information security, such as COURAGE, CAMINO and CyberROAD it is clear that the actual, tangible, cost of cybercrime is really not yet known [7]. The availability of reliable data is essential for policy-making and revenue allocation from the top (governments) downwards (individual stakeholders) in order to meet the challenges of the future as well as those we face currently. With factors such as traditionally low levels of reporting and the challenges associated with quantifying the medium and long terms of costs of cybersecurity breaches all contributing to the aforementioned challenges, there is clearly no single 'catch-all' solution address these gaps [8].

III. THE CONCEPT OF CYBERSECURITY ECONOMICS AND ANALYSIS (CEA)

This research study is exploring the science and practice of analytical reasoning that provides reasoning framework for building strategic and visual analytics technologies and cybersecurity economics for threat

analysis, prevention and response. In nutshell, analytical reasoning is key to apply cybersecurity judgement to reach conclusions of cybersecurity economics to allocate required resources across the organisations to ensure trust. Analytical reasoning is an iterative and highly collaborative process, both the human and technology synchronously scale to support reasoning, assessment and actions. CEA follows the structured and disciplined approach, further iterates on following steps: gathers evidence based information, generates hypothesis with multiple candidate explanations, and evaluates alternative explanations with evidence to reach outcomes. In a nutshell, CEA proposes to develop a systematic cybersecurity cost-benefit framework, informed and validated by the requirements of end-user organisations themselves, mandated with protecting their own data and infrastructure as well as those organisations charged with responding in the aftermath– insurers, CERTs and law enforcement. The cost-benefit model itself will contribute across all phases of the resilience cycle; prevention, early detection and treatment of cyber-threats and cybercriminal activities, and measures to ensure adequate recovery. The aim is to create an effective cybersecurity cost-benefit framework for cybersecurity economics to maximize the benefits of best practices.

The objective of creating cost-benefit framework is to identify the cybersecurity economics with the best practices of cybersecurity solutions mapped in previous phase of CEA project. The objectives of cost-benefit framework creation further quantified as below:

1) Develop a plan, measurement and verification protocols for cybersecurity cost-benefit analysis.

2) Investigate and identify the tangible and intangible cybersecurity elements for cost-benefit analysis considering people, process and technology model.

3) Measure cybersecurity cost-benefits by performing a cost-benefit analysis.

4) Further report the effectiveness of new CEA cost-benefit framework. The focus will be on protection effectiveness, compliance assurance, value generation and economic impact on a cross-sectoral basis.

The goal is to increase the economic and financial viability, effectiveness and value generation of cybersecurity solutions for organisation's strategic, tactical and operational imperative.

IV. The Research Approach and Method

This research study is aiming to develop a systematic cybersecurity cost-benefit framework using inductive reasoning scientific method considering specific analytic reasoning process. The method is strongly based on providing solutions. The analytic reasoning method draws the premises from unknown to known with iterative process that develops confidence in achieved solutions and hence ensures the trust. This is a structured and iterative process as shown in Figure 1. In this method, the goal of analyst is to reach a judgement about an issue or problem. The outcome of analyses presents the tangible results in the form of a product [9]. The process starts with planning of proving solutions to given issues. The planning phase includes resource usage and timeline plan. The second step in the process includes gathering and familiarising with available information on top of the already gathered information. Next, the analyst hypotheses and outlines multiple candidates with explanations. This step is represented in develop insight steps in Figure 1. Indeed, analyst aiming to reach a judgement by evaluating alternative explanations. The whole process allows to expand and broaden understanding of analyst's previous thinking. The analysis process ends with the final step represented in Figure 1 (i.e., produce result). The final step allows analyst to summarise the judgement with creation of reports, documents and products.

The inductive reasoning method starts with the specific observations and measures that allows to detect patterns and regularities, and resulting into formulate some tentative hypotheses to explore. Finally, the explorations of hypothesis ends with broader generalisations, developing conclusions or drawing theories. In general, scientific method is an ongoing and iterative process. Analytical reasoning is an iterative and highly collaborative process, people, process and technology synchronously scale to support cybersecurity reasoning, assessment and actions. Further, cybersecurity cost-benefits framework will be developed for taking decision to allocated required cybersecurity resources (tangible and intangible) including insurance requirements or not. Finally, cybersecurity improvement program will take place with the processes of standardisation and certification. Finally, the outcomes will be exploited to ensure trust within European digital community and citizens.

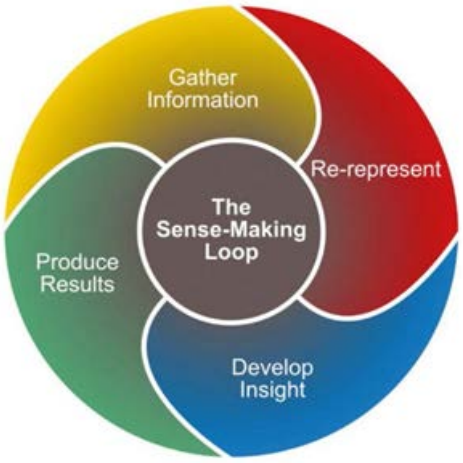

Fig. 1. The Analytical Reasoning Process. Source: Illuminating the Path: The Research and Development Agenda for Visual Analytics. IEEE computer society

A. *Cybersecurity Process Management Framework*

The cybersecurity process management framework (CPM) offers structure for more effective cybersecurity and security operations (see Figure 2 below). The CPM framework includes identifying and collecting cybersecurity requirements and mapping existing cybersecurity best practices. The framework also includes the well-designed metrics, analysis and measurement through CPM framework within a standard project management plan. The CPM framework enables to

meet cybersecurity management requirements and cybersecurity program achieves greater capability, maturity and improvement. The final result demonstrates values and cost effective cybersecurity solutions that helps achieve business goals. Following sections will explain more detail processes and implementation steps of the CEA cybersecurity process management framework.

Many research studies [10] [11] [12] confirm that usage of social and behavioural sciences improves the information and cyber security significantly. Therefore, cybersecurity measurement project is complimented with cybersecurity improvement program that also improves organisation learning and knowledge management to leverage and reuse continuously by enabling metrics and projects.

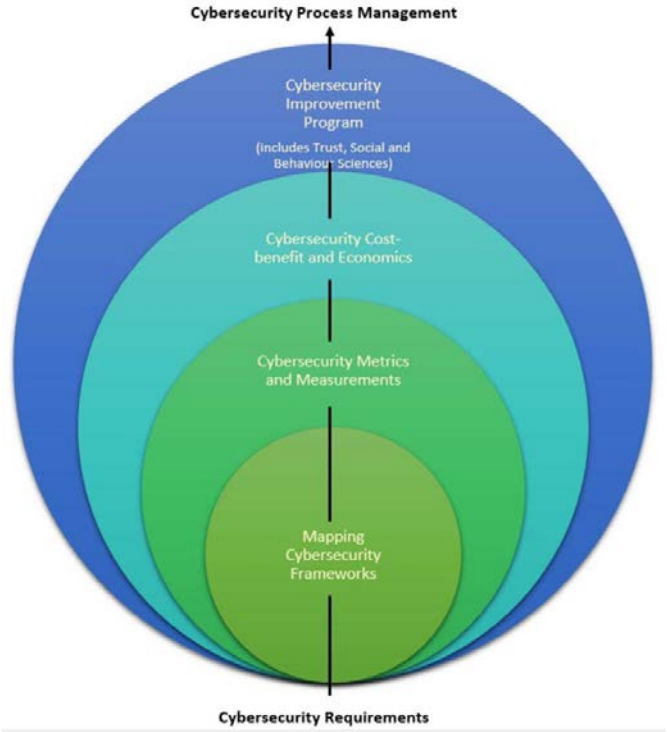

Fig. 2. Cybersecurity Process Management Framework. [1]

V. Proposed Solution – Cybersecurity Economics and Analysis

The research study starts with gathering information about existing cybersecurity practices and standards within and beyond state of the art. Then effective cybersecurity metrics will be developed for improving cybersecurity.

A. Mapping Existing Cybersecurity Frameworks

ENISA conducted study with the recommendation of CSCG (The Cybersecurity Coordination Group of CEN, CENELEC and ETSI) on 'Gaps and overlaps in standardisation' in cybersecurity [6]. The outcome and future recommendation clearly states- cybersecurity is more effective when all the individual cybersecurity domains work together in synergy with each other. CEA project starts with identifying stakeholder requirements and also addressing and mitigating the gaps found in ENISA studies and beyond state of the art. The CEA will conduct a mapping of existing cybersecurity frameworks and standards- based on following Integrated Cybersecurity Model (see Figure 3 below).

The cybersecurity domains are essentially divided into the specific competence areas linked with governance, policies and procedures, roles and responsibilities, risk management, and resources. Every cybersecurity domain provides standard recommendations and guidelines for implementing security measurements and activities. This cybersecurity approach is adopted by current best-practices and standards across the globe. It establishes a common knowledge platform, as an integrated approach that can be implemented across all aspects of an organisation's cybersecurity strategy. The mapping of existing effective and best-practices enables study outcomes to take forward a 'best-of-breed' solution, in the process identifying gap areas in addition and beyond state of the art of ENISA report [6]

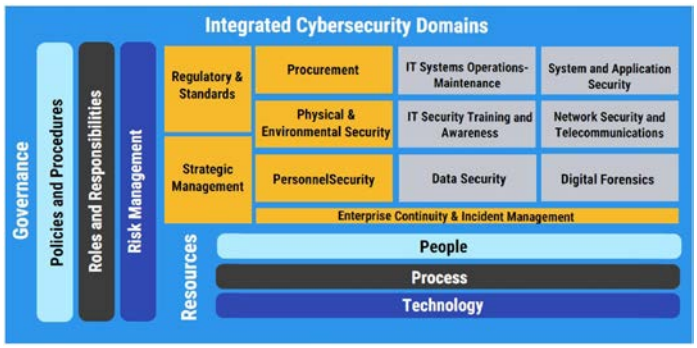

Fig. 3. Integrated Cybersecurity Model [2]

The cybersecurity domains are essentially divided into the specific competence areas linked with governance, policies and procedures, roles and responsibilities, risk management, and resources. Every cybersecurity domain provides standard recommendations and guidelines for implementing security measurements and activities. This cybersecurity approach is adopted by current best-practices and standards across the globe. It establishes a common knowledge platform, as an integrated approach that can be implemented across all aspects of an organisation's cybersecurity strategy. The mapping of existing effective and best-practices enables study outcomes to take forward a 'best-of-breed' solution, in the process

[1] The model is an expanded model from R. Graubart & D. Bodeau, "The Risk Management Framework and Cyber Resiliency.", 2016

[2] This model presents the outcome of combination of information sources and references. A broad set of sources and references include Cybersecurity strategy of the EU, ISO/IEC 27001, ANSI/ISA 62443 (ISO/IEC 62443), EU-NIS Directive, NIST Cybersecurity Framework, ENISA and COBIT

identifying gap areas in addition and beyond state of the art of ENISA report [6].

B. Cybersecurity Readiness Level Metrics

This study also defines the metrics needed to assess readiness levels for a holistic and comprehensive approach to information security auditing. The concept of cybersecurity metrics is not a new one. Despite this, assessing and predicting a given level of security is notoriously difficult.

Taking as an example the case of software development, although it is hard to measure the concept of security in isolation, the idea of quality is measureable to the extent to which a piece of code conforms to a given design specification, how efficient it is and how it easily it can be maintained or updated in future, amongst others. Therefore, if we consider that quality code is a pre-requisite for security then we can begin to use these prerequisite measures as the basis of metrics for assessing the level of security, mainly by incorporating metrics such as these across all domains of cybersecurity. Above logical steps will take place to create Cybersecurity Readiness Level Metrics as depicted in figure-4.

Fig. 4. Cybersecurity Readiness Metrics Process

The outcome of cybersecurity readiness level metrics will be useful in the process of conceptualisation of Cybersecurity Cost-Benefit Framework for a novel model of cybersecurity economics and analysis. One of the key question cybersecurity stakeholder faces - How to measure and take the best cybersecurity decisions for achieving business goals? Continuous measurements have a goal to reach metrics maturity. This study uses following process model for measurement (Figure 7 below).

The model is the combinations of data, analytics and metrics called- cybersecurity metrics maturity model. The model is adopted from the work already done and expanded to address current cybersecurity measurement challenges [13]. First, the sparse data analytics uses limited data to model risk utilising the quantitative techniques. The technique is helpful to take informed decision on new cybersecurity investment. Second, functional security metrics are subject specific and based on initial security investments. Third, security data marts are the most important measurement technique due to measuring cross-domains with big data sets. The security data marts are subject-matter or specific functional area (i.e., finance or marketing) data warehouses. It is measuring across security domains with large data sets [13], provides more precise cybersecurity insight. Forth, prescriptive security analytics is an emerging security measurement technique. This technique is blend of decision and data science using descriptive analytics, predictive analytics and prescriptive analytics. Finally, in addition to all these techniques our study also explores other beyond state of the art and emerging techniques.

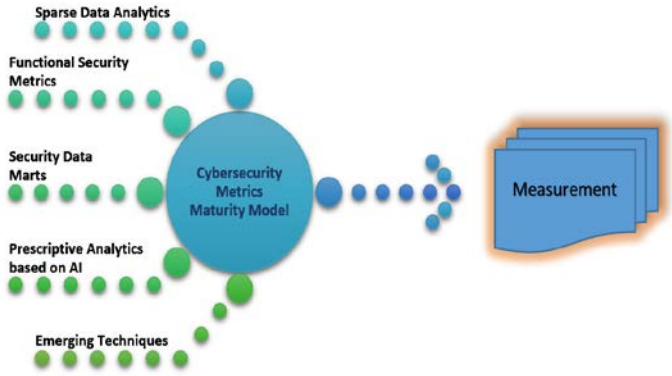

Fig. 5. Cybersecurity Measurement Process

VI. CYBERSECURITY COST-BENEFIT FRAMEWORK

The research study is combining multidisciplinary approaches and methods to build security and privacy cost model. We have explained in previous sections, starting with a mapping of cybersecurity 'best-of-breed' solution then measuring the effectiveness of solutions with cybersecurity metrics. The cybersecurity metrics and measurement process combined with cybersecurity cost-benefit framework (CBF) allows to make informed decisions on digital assets pricing, estimations of the cost of tangible and intangible and investment in information security, risk management and cybersecurity insurance.

ENISA reported [14] that current practices on security cost-benefits are around risk management approaches that measures the return on security investments (ROSI). The current quantitative risk assessment based cost-benefit model uses several components of a risk to calculate the cybersecurity cost. There are some key components considered in the quantitative risk assessment cost-benefit model including single loss expectancy (SLE), annual rate of occurrence (ARO) and annual loss expectancy (ALE). We can take following simple example for the reference [15].

A. Case Example – Return On Security Investment (ROSI)

The ABC Ltd. is suffering with cyber-attacks in the past and new CISO is planning cyber defence solution. The CISO is evaluating a situation and he found ABC Ltd faces about 8 malware related attacks in the past years. Each attacks are costing the loss around 10.000€. New cyber defence solution

can block around 85% of the attacks. The new cyber defence solution can cost 30.000€ per year. Hence, what can be return on security investment (ROSI)?

Solution:

The annual loss expectancy (ALE) = SLE x ARO

$$\text{Return on Investment (ROI)} = \frac{\text{Gain from investment} - \text{Cost of investment}}{\text{Cost of investment}}$$

$$\text{Return on Security Investment (ROSI)} = \frac{\text{Monitory loss reduction} - \text{Cost of solution}}{\text{Cost of the solution}}$$

We can lower ALE by implementing an effective security solution. This is resulting in the final ROSI formula as shown below:

$$\text{Return on Security Investment (ROSI)} = \frac{\text{ALE} * \text{mitigation ratio} - \text{Cost of solution}}{\text{Cost of the solution}}$$

$$\text{ROSI} = (8 * 10.000) * 0.85 - 30.000 / 30.000 = 126\%$$

The result shows the cybersecurity solutions will be useful and cost-effective to ABC Ltd.

B. Risk Management with Multidisciplinary Measurement Models

Cybersecurity metrics and measurement provide an opportunity for detail assessments and insights on security costs and values. However, measuring cybersecurity cost and value is daunting task. Therefore, CEA cost-benefit framework is combined with clear defined objectives, relevant data and creative analytical approaches. This approach combines risk management with multidisciplinary measurement process. The CEA cost-benefit framework is proposing double level (iterative) cybersecurity measurement process as explained below:

Measurement Level-1: The previous section described the process of the measuring cybersecurity operations including risk assessment, vulnerability assessment and detail analysis. Further, measuring compliance, standards, people, organisation and culture using cybersecurity readiness level metrics process (see Figure 4 above). The measurement will take place with tools and techniques like ROSI, generic cost- benefit model, the Poisson distribution, Monte Carlo simulation, statistical process control, societal and behavioural science, and emerging tools and techniques. Now, collected information on cost and values can be further funnel down to get sophisticated insights with CEA cybersecurity cost-benefit framework in next level.

Measurement Level-2: The cybersecurity measurement process (see Figure 5 above) depicts the use of tools and techniques including the sparse data analytics, functional security metrics, security data marts, prescriptive security analytics and other beyond state of the art and emerging techniques [15] [16] [17] [18]. The cybersecurity metrics maturity model will measure and get detail insights for CEA cybersecurity cost-benefit framework. Mainly the outcome will contributing to find the intangible costs and value [19]. Following graph is showing the outcome of the measurement level-2 using cybersecurity analytics maturity model (see Figure 6 below).

C. Cybersecurity Economics and Analysis Model

CEA is going to leverage the benefits of risk management approach combining with multidisciplinary measurement models. There are obvious benefits of using risk management approach as explained in the above example. CEA approach is blending of decision, data, social and cultural sciences using practical quantitative model, security balance scorecard, maturity modelling, and diagnostic method including descriptive, predictive, prescriptive analytics, along with emerging beyond state of the art models. These models will be identified and adopted in the CEA cost-benefit framework.

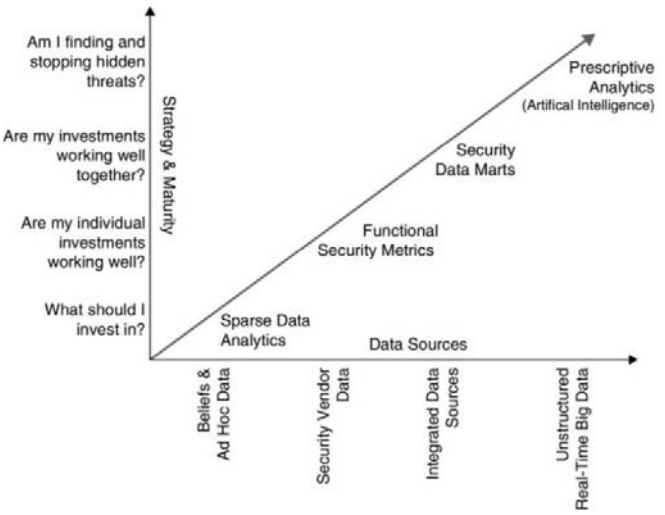

Fig. 6. Cybersecurity Analytics Maturity Model.
Source: Hubbard, Douglas W. "How to measure anything."

The following Figure 7 presents Cybersecurity Economics and Analysis- socio-economic model for an optimal cybersecurity cost-benefit framework to help decision-making based on a quantitative analysis of the cybersecurity risks and their impact on organizational tangible and intangible assets. CEA adopts a wider perspective to economics of cybersecurity. CEA undertakes to leverage existing 'state-of-the-art' (SOTA) in cybersecurity auditing guidelines and frameworks, taking these existing approaches 'beyond' SOTA (BSOTA) by bringing a multidisciplinary perspective to the appreciation of cyber-risk, in order to develop a new cost-benefit framework for cybersecurity.

The concept of cybersecurity metrics is already in practice in current standards, framework and practices. For examples, "By 2017, WISER will provide a cyber-risk management framework able to assess, monitor and mitigate the risks in real-time, in multiple industries"[3]. However, the practices are more focus on securing information assets

[3] WISER is a European collaborative Innovation Action

rather than measuring the effectiveness and value of the cybersecurity. Current practices are also lacking the synergy between all domains of cybersecurity [20]. CEA is focused on quality of measuring while assessing the level of the security, mainly by incorporating metrics across all domains of cybersecurity (please refer Figure-3 Integrated Cybersecurity Model). Currently, there is no cybersecurity readiness level metrics available that is bringing in economics and other disciplines to provide a more holistic and tangible means for organisations to increase their understanding of cybersecurity risks and economics. CEA makes significant improvement in current practices of cybersecurity metrics by creating new set of Cybersecurity Readiness Level Metrics with the cybersecurity economics.

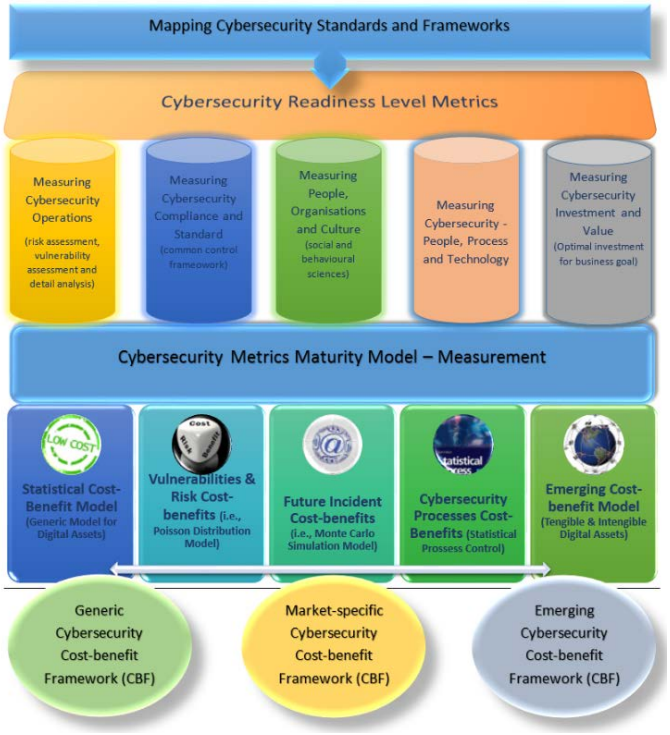

Fig. 7. A Novel Cybersecurity Economics and Analysis Model

The current practices on security cost-benefits are using risk management approaches that measures the cost and return on security investments (ROSI). The current quantitative risk assessment based cost- benefit model uses several components of a risk to calculate the cybersecurity cost and suggestions for investments. There are some solutions available for cybersecurity insurance based on general cost calculations and risk management approaches [19]. However, the majority of cost-benefit work and cybersecurity insurance research work been done on market specific domain. Hence, it is immensely important to create cybersecurity cost-benefit framework and also provide direction to cybersecurity insurance matter (helping companies to decide about insurance requirement). CEA is combining multidisciplinary approaches and methods to build cybersecurity cost- benefit framework. Starting with a mapping of cybersecurity 'best-of-breed' solution then measuring the effectiveness of solutions with cybersecurity metrics. The cybersecurity metrics and measurement process combined with cybersecurity cost-benefit framework (CBF) that allows to make informed decisions on digital assets pricing, estimations of the cost of tangible and intangible and investment in information security, risk management and cybersecurity insurance. As previously mentioned in Cybersecurity Process Management Framework that many research study confirms significance of social and behavioural sciences within information and cyber security improvement. Therefore, CEA framework is equipped with two fold consideration of social and behavioural sciences-measuring people, organisations and culture plus people, process and technology context. This will improve organisation learning and knowledge management to leverage the benefits of social and behavioural sciences for effective cybersecurity and its value.

VII. Conclusion

CEA is built upon existing cybersecurity resilience principles, including those defined by the World Economic Forum[4], national and independent cybersecurity audit frameworks such as the Finnish 'KATAKRI' model[5], the UK Governments 'Cyber Essentials' scheme[6], in addition to other private and independent initiatives[7,8] extracting existing best practice and principles whilst combining experimental research in risk analysis and cost quantification to ensure that the principles and risks of cybersecurity 'speak the language' of business decision makers - i.e. have a quantifiable financial value. The framework itself will be validated and iteratively refined through the projects multi-phase piloting process, to ensure it is as accessible as it is comprehensive and robust. The SME networks attached to the project consist of independent businesses, many of which match the profile of those considered most vulnerable to cyberattack, from small micro SME's to those who employ several hundred people, covering a number of sectors ensuring the suitability and adaptability of the framework in appreciating sectoral specificities and nuance, and moving beyond the one-size-fits-all approaches currently employed.

In this paper, we introduced a novel cybersecurity economics and analysis model. The novel model is based on strategic, long-term thinking incorporating economics from the outset. The CEA will provide benchmarks for the economic assessment of national and international cybersecurity audits and standards and provide policy recommendations for the alignment of policies and regulations to ensure trust within citizens and digital environment. CEA utilizes a holistic approach to cybersecurity, proposing a model based on a deep and comprehensive analysis of organisations' security –

[4] World Economic Forum – Partnering for Cyber Resilience
[5] Information security auditing tool for authorities – Katakri 2015 (Finland)
[6] UK Government- Cyber Essentials' scheme
[7] The Thale Group Cyber Assurance – Audit, Test and Compliance
[8] US-Cyber Consequences Unit – Cyber Security Check List

considering not only technological perspectives, but institutional, economic, governance and human dimensions – taking forward existing 'best' and effective practices from national audit frameworks, sectoral guidelines and organisational policy to put together a 'best of breed' solution.

The early results also showed that a new solution accounts for the wants and needs of various stakeholder groups and existing sectoral requirements. The next phase of study and future research needs an organisation level implementation and dissemination of the novel model. The impact assessment will further enhances effectiveness of the cybersecurity economics and its effects on the relevant business objectives.

REFERENCES

[1] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013.

[2] EU Impact Assessment, "Proposal for a Directive of the European Parliament and of the Council-Concerning measures to ensure a high level of network and information security across the Union", 2013.

[3] M. H. Thelle, "The economic impact of a Digital Single Market (DSM) in Europe", European Policy Centre – EPC, 2010.

[4] (ISC)² Global Information Security Workforce Study: The Professionals' Perspectives: Cyber Security in the DACH Region and Core Europe (CE). 2015.

[5] P. K. Manadhata., & J. M. Wing, "An attack surface metric." IEEE Trans. Softw. Eng., 37(3), 371-386, 2011

[6] C. Brookson et al., "Definition of Cybersecurity - Gaps and overlaps in standardisation", ENISA, 2015.

[7] B. Akhgar, B. Brewster, "Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities.", Springer, 2016.

[8] Yusuf, Simon Enoch, et al. "Security Modelling and Analysis of Dynamic Enterprise Networks." Computer and Information Technology (CIT), 2016 IEEE International Conference on. IEEE, 2016.

[9] Cook, A. Kristin, and J. J. Thomas, "Illuminating the path: The research and development agenda for visual analytics.", No. PNNL-SA-45230. Pacific Northwest National Laboratory (PNNL), Richland, WA (US), 2005.

[10] B. Khan, K. S- Alghathbar, S. I. Nabi & M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories", *.African Journal of Business Management, 5*(26), 10862. 2011.

[11] Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

[12] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

[13] J. Freund & J. Jones, J, Measuring and managing information risk: a FAIR approach, Butterworth-Heinemann, 2014.

[14] Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. Journal of Research and practice in Information Technology, 38(1), 45-56.

[15] Armin, J., Thompson, B., & Kijewski, P. (2016). Cybercrime Economic Costs: No Measure No Solution. In Combatting Cybercrime and Cyberterrorism (pp. 135-155). Springer International Publishing.

[16] Y. H. Moon, J. H. Kim, D. S. Kim, and H. K. Kim. "Hybrid Attack Path Enumeration System Based on Reputation Scores." In Computer and Information Technology (CIT), 2016 IEEE International Conference on, pp. 241-248. IEEE, 2016.

[17] Rajamäki, J., Rathod, P. & Holmström, J.*"Decentralized Fully Redundant Cyber Secure Governmental Communications Concept"*, in Proceedings of the 2013 European Intelligence and Security Informatics Conference, pp. 176-181.

[18] Security Modelling and Analysis of Dynamic Enterprise Networks Simon Yusuf, Mengmeng Ge, Jin Hong, Huy Kang Kim, Paul Kim, Dong Seong Kim, *16th IEEE International Conference on Computer and Information Technology, 7-10 December, 2016*

[19] P. R. Garvey and S. H. Patel. "Analytical Frameworks to Assess the Effectiveness and Economic-Returns of Cybersecurity Investments." In Military Communications Conference (MILCOM), 2014 IEEE, pp. 136-145. IEEE, 2014.

[20] Watkins, L., & Hurley, J. S. (2016). The Next Generation of Scientific-Based Risk Metrics: Measuring Cyber Maturity. International Journal of Cyber Warfare and Terrorism (IJCWT), 6(3), 43-52.