Technology Transfer: Revenues Estimation in the Cyber Security Sector

Michal J. Falkowski[†]
Technology Transfer Department
NASK National Research Institute
Warsaw, Poland
michal.falkowski@nask.pl

Jaroslaw Kaminski
Technology Transfer Department
NASK National Research Institute
Warsaw, Poland
jaroslaw.kaminski@nask.pl

Marta Wachowicz
Technology Transfer Department
NASK National Research Institute
Warsaw, Poland
marta.wachowicz@nask.pl

ABSTRACT

This study investigates the complexities of technology transfer within the cyber security sector, focusing on the financial and operational challenges posed by its dynamic nature. The primary research problem is understanding how to define final cyber product and estimate associated costs, particularly in the context of both traditional and new economy revenue models. Preliminary findings reveal significant discrepancies in cost estimation and revenue forecasting, particularly due to the non-linear contributions of scientists, which complicate the creation of effective license agreements. The paper offers a framework to better align technology transfer processes with the unique characteristics of cyber security innovations, thus improving the accuracy of cost projections and licensing strategies.

KEYWORDS

Technology transfer, cyber security sector, revenue estimation, AI models, new economy, science contribution, license agreements

1 UNCERTAINTIES IN CYBER SECURITY TOOLS SPECIFICATION

Cyber security is a term with widely varying definitions that are frequently subjective and, in some cases, lack precision. According to the America's Cyber Defense Agency (CISA), it is defined as *the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information* [11]. The absence of a clear, universally accepted definition that encapsulates the multidimensional nature of cyber security hinders progress in technology and science [6]. This is because it reinforces a technical perspective on cyber security, while simultaneously isolating disciplines that should be collaborating to address complex cyber security challenges effectively. The complexities involved significantly affect the determination of what constitutes a cyber security product, the criteria for deeming it complete, and the estimation of production costs within defined timeframes and budgetary constraints.

[†]Author Footnote to be captured as Author Note

Information Society 2024, 7–11 October 2024, Ljubljana, Slovenia

1.1 Defining cyber security product

Given the multidisciplinary nature of cyber security and its widespread impact on society, it is essential to establish, utilize, and elaborate a standardized terminology and develop a comprehensive, shared understanding of what constitutes cyber security product and economic risks associated with it [7].

In defining a cyber security product, it is crucial to recognize the role of interdisciplinary contributions, ranging from computer science and engineering to law, economics, and human factors. For instance, a cyber security product may include not only technical components, such as encryption algorithms or intrusion detection systems, but also legal frameworks and organizational practices that enhance security. The integration of these diverse elements requires a standardized terminology that can be universally understood across disciplines, enabling effective communication and collaboration.

Moreover, the definition of a cyber security product must account for its intended purpose and scope. Products may vary significantly in their focus - some are designed to prevent unauthorized access, others to detect intrusions, and yet others to respond to or recover from cyber incidents. This diversity necessitates a clear classification system that categorizes products based on their functionality, target environment, and the specific threats they address. For example, network security tools, endpoint protection software, and identity management systems each serve different purposes but collectively contribute to a comprehensive cyber security strategy.

Economic considerations also play a critical role in defining cyber security products. The value of a cyber security product is often measured by its effectiveness in mitigating risks, which are themselves subject to economic assessment. The economic impact of cyber threats, the cost of deploying and maintaining cyber security products, and the return on investment are all factors that influence how a cyber security product is defined and evaluated. This underscores the importance of aligning technical definitions with economic realities to ensure that cyber security investments are both effective and sustainable.

Furthermore, the lifecycle of a cyber security product must be clearly delineated, from initial development through deployment, operation, and eventual decommissioning. A comprehensive understanding of this lifecycle is necessary to establish criteria for when a product can be considered complete and to identify potential risks and vulnerabilities that may arise at various stages. This lifecycle approach also highlights the importance of adaptability in cyber security products, as they must evolve to address emerging threats and changing environments.

In summary, defining a cyber security product requires a multidisciplinary approach that integrates technical, legal, economic, and operational perspectives. Standardized terminology and clear classification systems are essential to fostering a shared understanding across disciplines, while economic considerations and lifecycle management provide the framework for evaluating the effectiveness and sustainability of cyber security products.

1.2 Estimating cyber product costs

A standardized method for measuring and managing the costs associated with implementing cyber security programs has yet to be established. To advance research and practice in this field, various cost estimation frameworks related to the development and deployment of cyber security products have emerged in recent years [9]. Estimating the costs associated with cyber security products is a critical aspect of cyber security planning and management. However, this task is fraught with uncertainties due to the dynamic and evolving nature of cyber threats, the complexity of cyber security products, and the diverse environments in which they are deployed [8]. Unlike traditional products, cyber security products must continuously adapt to an evolving threat landscape, where new vulnerabilities and attack vectors emerge regularly. This requires ongoing updates, patches, and upgrades, leading to unpredictable and often escalating operational costs over time.

Cost estimation for cyber security products involves several key components: development costs, deployment costs, operational costs, and decommissioning costs. Each of these components must be carefully assessed to provide an accurate estimate of the total cost of ownership (TCO) for a cyber security product.

1. **Development Costs:** These include the expenses incurred during the design and creation of the cyber security product. Development costs can vary widely depending on the complexity of the product, the technologies involved, and the level of expertise required. For example, developing an advanced threat detection system may involve significant investment in research and development, including the use of machine learning algorithms, data analysis tools, and security protocols. Additionally, the need for compliance with industry standards and regulations can add to development costs, as products must be designed to meet specific security requirements.
2. **Deployment Costs:** Once a cyber security product is developed, it must be deployed within the target environment. Deployment costs include the expenses related to integrating the product with existing systems, configuring it to meet organizational needs, and training personnel to use it effectively. In some cases, deployment may also involve significant infrastructure upgrades, such as installing new hardware or enhancing network capabilities. These costs can be substantial, particularly in large or complex organizations with extensive IT environments.
3. **Operational Costs:** The ongoing operation of a cyber security product generates costs related to maintenance, monitoring, and updates. Cyber security products must be continuously updated to address new threats and vulnerabilities, which can involve both software patches and hardware upgrades. Additionally, operational costs include the resources required to monitor the product's performance, respond to security incidents, and conduct regular security assessments. The need for highly skilled personnel to manage these tasks further contributes to operational costs, as cyber security expertise is often in high demand and short supply.
4. **Decommissioning Costs:** At the end of its lifecycle, a cyber security product must be decommissioned, which involves safely removing it from the environment and ensuring that no residual vulnerabilities remain. Decommissioning costs may include data migration, system reconfiguration, and the disposal of outdated hardware. Additionally, organizations may need to invest in new cyber security products to replace those being decommissioned, adding to the overall cost.

Estimating these costs is complicated by several factors, including the unpredictability of cyber threats, the rapid pace of technological change, and the variability in organizational needs and environments [10]. It means that a cyber security product may require extensive customization and integration efforts, which further complicates cost estimation. For example, the introduction of disruptive technologies, such as quantum computing, can render existing cyber security products obsolete, necessitating additional investments.

The need for specialized personnel to manage and maintain cyber security products, combined with the scarcity of cyber security expertise, adds another layer of complexity to cost forecasting. Furthermore, the consequences of underestimating the costs must be carefully considered, as they are often significant and far-reaching, potentially resulting in insufficient protection and increased risk exposure. This contrasts with other products, where cost overruns might primarily affect financial performance without posing immediate security risks. Therefore, the cost estimation of cyber security products must account for not only the tangible costs of development, deployment, and maintenance but also the intangible costs associated with risk management and the potential impact of cyber incidents.

To address these uncertainties, organizations must adopt a flexible and adaptive approach to cost estimation. This may involve using scenario analysis, which considers different potential future states and their impact on costs, as well as incorporating risk assessments to identify and quantify potential cost drivers. Additionally, organizations should consider the total cost of ownership over the entire lifecycle of the cyber security product, rather than focusing solely on upfront costs. This approach ensures that all relevant costs are accounted for and provides a more accurate estimate of the long-term financial commitment required to maintain cyber security.

2 METHODOLOGY

To address issues, this study employs a mixed-method approach. An extensive literature review is conducted. Relevant academic journals, industry reports, and government publications are examined. Additionally, qualitative data is collected through semi-structured interviews with key specialists and experts.

3 REVENUE ESTIMATION AND COMPANIES VALUATION

Cyber security is the practice of protecting individuals' and organizations' systems, networks, applications, computing devices, sensitive data, and financial assets against any digital attacks [3]. It refers to any technology, measure, or practice for preventing cyberattacks or mitigating their impact. We could categorize the main components of cyber security into the following areas: cyber security Governance, Policies, and Procedures, User Identity and Access Management, Network Security, Application Security, Data Protection, Business Continuity and Disaster Recovery Plan, Education. The number of fields results in miscellaneous cyber security business models, reflecting various comprehensive solutions in the evolving landscape of cyber threats and swift pace of technological advancement. The differences are both in revenue streams, cost structures and scalability.

3.1 Cyber security business models

We can distinguish three basic revenue streams: subscriptions, professional services, and licensing [5]. In first case cyber security firms offer their services on a subscription basis, providing continuous protection with regular updates and support in exchange for a recurring fee. This model ensures a steady and predictable revenue flow, development of customer relationships, mutually beneficial vendor relationships with major focus on customer procurement. Cyber security companies focused on professional services as business model often offer consulting, threat assessment, and response services. These include penetration testing, incident response teams and security audits. Finally, many companies operate under licensing model - selling licenses for proprietary security software or technology solution could be significant revenue stream, creates an easier entry into foreign markets, does not require capital investment or presence of the licensor in new geographical regions.

3.2 Classic technology valuation

Tech spending as a percentage of revenue has increased from 3.28% in 2016 to 5.49% in 2023 [4]. With bigger budgets often comes increased oversight and expectations from the business-tech leaders are becoming thoughtful about allocating capital for tech investments. 2023 Deloitte research shows that 6 in 10 executives struggle with measuring the value of these investments. The choice of an appropriate valuation method depends on the circumstances, scope, and purpose of the valuation – the three main approaches concentrate on the cost, market, and income.

Cost methods determine the value of intellectual property based on the historical cost of production or the estimated cost of replacement with assets of comparable utility. These methods involve considering any expenses that need to be incurred to remanufacture the asset or replace it with an asset comparable to the one being valued. Cost methods are applied mostly to unfinished or easily manufactured technologies. It is possible to imagine situations in which a relatively considerable sum of money has been spent on a technology that does not produce the anticipated benefits. In such a case, the valuation of technology by the cost method may significantly overestimate its value, and income methods will come to the rescue.

The income method of technology valuation is grounded in the belief that for a potential investor, a particular asset is worth as much as he can get income from that asset. The risk of the business and the time value of money should be considered. Valuation of technology using the income approach requires determination of the period of economic usefulness of the valued technology. It is done based on projected cash flows discounted at an appropriate discount rate. The income method is most often indicated as the most appropriate for valuing technology for which there is a high degree of confidence in the forecasts of operating income.

Market (comparative) methods of valuing intellectual property, on the other hand, involve estimating the value of technology based on a comparison to market transactions for similar assets. However, information on transactions for the purchase or sale of intellectual property is rarely publicly available. Therefore, the method often uses an analogy with the valuation of technology companies, whose value depends largely or entirely on the technology they own. The main shortcoming of this method is the inability to identify comparable technology. As a rule, each innovative technology is unique and has specific parameters, which leads to limited possibilities of comparison to existing solutions known to date.

3.3 Companies' valuation in cyber security sector

The Market Multiples method is a key tool for valuing companies in the cyber security industry. This approach involves valuing a firm by comparing it to similar private or recently acquired companies in the sector. Specifically, it focuses on two primary types of multiples: Revenue Multiple and EBITDA (Earnings Before Interest, Taxes, Depreciation, and Amortization) Multiple. For startups (especially those that are pre-profit) the Revenue Multiple is often more relevant. It compares the company's value to its revenue, offering a perspective on how the market values the revenue generated. For more mature companies (with significant earnings), the EBITDA Multiple provides a view of the company's value relative to its profitability before accounting for financial and accounting factors.

Applying the Market Multiples method effectively requires a deep understanding of market trends and financial metrics specific to the cyber security sector. The rapidly evolving nature of cyber security, with frequent technological innovations and varying threat landscapes combined with investor confidence in the sector's growth can significantly influence these multiples.
The most common purpose of technology valuation is the needs for commercialization of completed development work in R&D Units. It is determined as part of the commercialization of technology, the value of the sale to an external investor or in-kind contribution to a special purpose vehicle (SPV or Spin-off). Prior to the commercialization of intellectual property, there is often a need to determine the value of these intangible assets and whole company. Another reason, also encountered, for the valuation of technology is the need to recognize the fair value in the accounting books. Less common are cases of estimating the value of technology for litigation, where it is required to determine the value of the subject matter of the dispute or under collateral for financial instruments. In the case of cyber security technology and company valuations, it is useful to define the circumstances valuation determines purpose: accounting, market

(for the current owners or new investors) or liquidation. It would be desirable to strike a balance between qualitative and quantitative measures.

4 IMPLICATIONS FOR TECHNOLOGY TRANSFER OFFICES

From the point of view of technology transfer and commercialization of scientific results, managing the process of new solution building using AI models is particularly difficult. The problematic question of revenue estimation implies further issues related to the creation of licensing or distribution agreements; additional complications also arise from the very characteristics of AI models. First, there are several problems associated with the application and obtaining Intellectual Property Rights (IPR) protection for such solutions. Secondly, cooperation with scientists is done in close cooperation with software developers, and scientific input is expected not in the entire process. Third, the solutions for specific markets generate several difficulties in shaping models for licensing agreements for the cyber security industry.

4.1 Intellectual Property Rights protection

When considering patenting AI-related inventions, there is a need to answer the fundamental questions of whether inventions qualify for patent protection. In European system, while a computer program or software may not be patentable, artificial intelligence and machine learning that serve or achieve a technical purpose may be a desirable alternative. The newest EPO guidelines [2], require the mathematical methods and training data used by an AI-related invention to be disclosed in sufficient detail to reproduce the technical effect of the invention over the whole scope of the claims. To address these issues and prepare a commercialization plan for the cyber security market, Technology Transfer Offices should identify the territories for patent protection for their AI inventions and assess whether such inventions meet the relevant subject matter eligibility criteria. If AI-related patent protection seems unfeasible and ineligible, TTO should consider protection using trade secrets or other alternatives. Protecting rights to training data, AI output, and other crucial training data requires attention, awareness, and careful action.

4.2 Relations with scientists

AI is forcing a change in the attitude of scientists, from that of a strict researcher to one that is far more oriented toward creating a working IT system. In terms of describing the types of scientists according to the Science Council, one can explain the change in attitude of the Explorer Scientist to the Developer Scientist [1]. This reflects a commitment to the area of creating AI solutions for specific and demanding markets. *"The Explorer Scientists rarely focus on a particular outcome or impact, rather they want to know the next piece of the jigsaw of scientific understanding and knowledge. […] The Investigator Scientist digs into the unknown observing, mapping, understanding, and piecing together in-depth knowledge and data, setting out the landscape for others to translate and develop"* [1]. The scientist is needed at specific moments, the innovation forces seasonal involvement, the product is created more as a result of collaboration with programmers and software developers, and there is no space for discovering independent universal truths in the sense of breakthrough ideas or inventions. We observe the non-linear contribution of the researcher to the development of the cyber security product. For TTOs, this is an additional complication, the connection of the author to his work is strong, and the cyber security market forces not only close teamwork but also IT and data professionals themselves are gaining in importance. Data stewards have a significant impact on the development of AI models and thus cyber products. For TTO is a difficulty related to the progress and commercialization plans for a specific solution.

4.3 Risks in license agreement

Forming a license agreement for a product or solution using an AI model requires considering the strict characteristics of training AI models, the difficulty of determining milestones for model development, and the system of subscription or license fees depending on the stage of learning or re-learning the model. The fundamental difficulty in estimating and establishing profit or revenue models depending on the development of machine learning lies in the indefiniteness of the solution itself. Models need successive iterations, the cost of software development changes, and the demand for certain solutions also changes, which makes it exceedingly difficult to forecast profits and build a model of fees and payments in a license agreement. The described problem of revenue estimation forces the adaptation of cyber security solutions using AI models of licensing agreements and billing systems, a thorough reflection is needed in the society of technology transfer professionals on this subject.

5 CONCLUSION

Developing a more precise and universally accepted definition of cyber security products is essential for standardizing cost and revenue estimation processes. Authors will focus on robust methodologies to account for the non-linear contributions of R&D teams in cyber security, as current models are inadequate. These areas will dictate the trajectory of future research, reducing uncertainties in product finalization and financial forecasting.

REFERENCES

[1] Science Council, August 2024, <https://sciencecouncil.org/about-science/10-types-of-scientist/>

[2] Guidelines for Examination in the European Patent Office (2024), ISBN 978-3-89605-361-9

[3] CISCO, August 2024, <https://www.cisco.com/site/us/en/learn/topics/security/what-iscyber security.html>

[4] Global Technology Leadership Study, Deloitte 2023

[5] Cyber security Startup Valuation Report, Finro 2024

[6] Diakun-Thibault, Nadia. (2014). *Defining Cybersecurity*. Technology Innovation Management Review. 2014. DOI: 10.22215/timreview/835

[7] Cains M.G., Flora Liberty, Taber Danica, King Zoe, and Henshel Diane. (2021). *Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation*. Risk Analysis. 42. DOI: 10.1111/risa.13687.

[8] Leszczyna Rafal and Litwin Adrian. (2020). Estimating the Cost of Cyber security Activities with CAsPeA: A Case Study and Comparative Analysis. DOI: 10.1007/978-3-030-65610-2_17.

[9] Radziwill Nicole. (2017). *Cyber security Cost of Quality: Managing the Costs of Cyber security Risk Management*. Software Quality Professional. 19. DOI: 10.48550/arXiv.1707.02653

[10] Basholli Fatmir and Juraev Davron. (2024). *Framework, tools and challenges in cyber security*. 1. 96-106. DOI: 10.13140/RG.2.2.21009.24161

[11] America's Cyber Defense Agency, August 2024, <https://www.cisa.gov>