№ 1 (5), 2023 ISSN: 2682 – 9517 (print) ISSN: 2683 – 0930 (online)
INSTITUTE OF INFORMATICS AND INNOVATIVE TECHNOLOGIES

Cybersecurity Brokers in Public-Private Partnerships as a Part of the Digital Economy

Denis Petkov
Academic Relations
European Digital Innovation Hub "Trakia"
Plovdiv, Bulgaria
d.petkov@edihtrakia.org

The work analyzes how cybersecurity brokers act in facilitating public-private partnerships (PPPs) in order to provide cybersecurity for the digital economy. Cybersecurity brokers are viewed as key intermediaries, which allow for collaboration between the Public and Private sectors, share threat intelligence and provide resilient business growth by optimimizing cybersecurity investments cost. Additionally, they enable compliance ficilitation and streamlined incident response, which are commonly regarded as pillars of business continuity and data protection. The value of PPPs in cybersecurity is further discussed in the paper, supported by a case study regarding the work of brokers and the provision of scalable cybersecurity solutions. The main challenges highlighted in the work are data privacy, competitive intelligence sharing and trust and by what means a skilled broker can be crucial to managing these risks.

Keywords: brokers, collaboration, cybersecurity, partnerships, digital economy

I. INTRODUCTION

Cybersecurity in the context of the present digital economy is viewed as a paramount factor for business continuity. Therefore, public-private partnerships (PPPs) in cybersecurity are increasingly thought of as a highly needed mechanism. Such partnerships bring government and private sector together in the common strategic objective of mitigating cyber threats and protecting digital assets. In contrast to traditional PPPs, by bringing together regulatory oversight, advanced technology and a shared approach to data sharing, the cybersecurity-based PPPs aim to fortify the business landscape, to create a resilient understanding of cybersecurity and to foster a business-centric approach that relies on innovation, collaboration and risk management.

One can view the Cybersecurity broker as a main actor in the abovementioned processes. Such brokers facilitate contact and collaboration between public and private stakeholders, usually accomplished through the act of bridging technical, regulatory and operational divides. The skilled broker will not only collect, analyze and monetize threat intelligence but follow it with proactively arranged scalable solutions, carefully tailored to the cybersecurity needs of his partners. Such actions cultivate stakeholder trust in the sector, followed by strategic investments in cybersecurity capabilities. Considering this, the cybersecurity broker's role has a wide range of responsibilities, spanning from the provision of affordable access to cybersecurity resources to the provision of regulatory compliance, making such a concept indispensable for the digital economy.

Cybersecurity brokers serve as facilitators in the context of business-driven PPPs, connecting private enterprises with the resources of the public sector to generate mutual value. The process grants businesses access to advanced tools, regulatory compliance, and collective threat intelligence by removing the need for allocation of significant internal resources, which in turn is paramount for small-and-medium enterprises (SMEs). As an example, thanks to partnering with a cybersecurity broker, an organization can utilize the benefits of shared threat intelligence for a fraction of the cost, which otherwise would be required for designing in-house capabilities. Therefore, brokers not only adhere to practical needs, but also foster proactivity in the management of cyber risk.

The goal of this paper is to define in what manner cybersecurity brokers foster business-driven PPPs, focusing on EDIH Trakia. Located in Bulgaria, the European Digital Innovation Hub represents a collaboration between academic institutions, SMEs, and public agencies working with the common goal to support the process of digitalization and the

understanding of cybersecurity in the region. Through the use of case studies and contextual examples, the paper highlights how brokers manage to facilitate not only the technical and operational elements of the cybersecurity spectrum, but also to promote a collaborative, innovation-driven Ecosystem that is based on proactive resilience. Therefore, the thesis of the research suggests that cybersecurity brokers are a cardinal part in the process of conducting PPPs and as a result advance business-centric cybersecurity objectives such as growth, resilience and trust in the digital landscape.

II. Business Value in Cybersecurity PPPs

Cybersecurity public-private partnerships pose as a common ground when it comes to addressing complex cyber threats. This modern form of PPP extends far beyond the traditional resource sharing; regulatory oversight, advanced technology and smart intelligence-sharing mechanisms are present as innovations in modern context. This new form of PPPs boosts businesses in combatting the present challenges of high cybersecurity costs by democratizing the access to resources and information. In this manner, stakeholders from the private sector, and especially SMEs, gain a strategic advantage, enabling them greater precision when addressing cyber threats.

One can view shared intelligence as one of the cardinal selling points of cybersecurity PPPs. Threat intelligence from multiple sources, professionally compiled and delivered in a package by a broker amounts to a very powerful business asset. By provision of monetizable intelligence on rising threats, vulnerabilities and attack patterns, PPPs and their brokers enable companies to take a proactive stance, assuming control over threats before they escalate into risks. On a micro level, this process not only bolsters individual business operations, but also fortifies cyberresilience on an industry-wide level. The responsibility of the cybersecurity brokers as facilitators in these PPPs lies in ensuring that businesses receive timely, accurate and needed data. Having in mind this, businesses which are a part of such PPPs can capitalize freely on the available collective knowledge, thereby once more contributing to the strategic public-private goal of sector-wide cybersecurity resilience and understanding.

Another way of value generation for PPPs in cybersecurity is compliance facilitation, the search for which is constant as the evolution of data protection and privacy regulation. Through compliance with cybersecurity and data protection standards, a company not only fulfills a mere legal obligation, but also develops a competitive advantage by fostering stakeholder trust. In the present context, the process of achieving compliance can be labeled as a daunting task, which can be undertaken in an easier manner with the assistance of PPPs. Public-private partnerships deliver accessible regulatory expertise and guidance through the use of cybersecurity brokers, which help with understanding and implementing best practices in the sector.

A concrete example of the business value generated by this concept is EDIH Trakia's CYBER4All STAR project. Through this initiative, the EDIH brings together the Bulgarian SME and public sector by delivering access to a portfolio of critical cybersecurity services such as vulnerability assessments, penetration testing and threat intelligence. Solutions such as these are usually reserved for bigger enterprises and out of reach for smaller ones due to the requirement of high costs and technical expertise. However, this fact can be changed through the public-private collaboration, established by the EDIH. Furthermore, the project lowers the barriers to access, allowing companies the test-before-invest solution, which in turn escalates their cybersecurity measures to a level on par with that of large corporations. In essence, this concept defines how PPPs bring theoretical potential to reality by democratizing access to cybersecurity and resilient digitalization in a business ecosystem open to every stakeholder. On an even higher scale, the model works towards the strategic goal of rebranding cybersecurity as an operational requisite, used and understood by everyone, rather than a premium corporate cost, reserved for the business elite.

Furthermore, PPPs bolster business continuity with the process of streamlining concrete incident response mechanisms to enterprises. As a part of this model, cybersecurity brokers help with the establishment of communication channels and incident protocols that connect public institutions and private companies in the event of a cybersecurity breach. Thus, ensuring that businesses are ready for a rapid and effective response in a critical situation where every second counts towards the minimization of impact. Such a proactive approach is key in the present business landscape as streamlined incident response protocols and their provision by cybersecurity brokers can be translated into concrete corporate benefits such as cost reduction, data protection, brand reputation and on a macro-level the establishment of a resilient business ecosystem.

In conclusion, PPPs in cybersecurity realize their potential by generating business value on a multifaceted basis, encompassing threat intelligence sharing, compliance support, cost-effective access to advanced solutions and streamlined incident response. The adaptability of the model can also be seen in the delivery of results both at the organizational and industry levels, therefore highlighting the importance of cybersecurity PPPs and their brokers.

III. Cybersecurity Brokers's role in PPPs

Cybersecurity brokers are viewed as the driving force behind business-centric PPPs as they are tasked with facilitating collaboration and coordination between various stakeholders and sectors with the common goal of monetizing their services, generating mutual value and build cyberresilience. Such brokers also serve as indispensable middlemen in the discussion between private businesses, public institutions and regulatory bodies. Furthermore, by streamlining the communication process they enable seamless knowledge exchange and collaboration that extends the micro level of business to business and allows for benefit generation on a broader economic level.

The main contribution of cybersecurity brokers in PPPs is the real-time threat intelligence sharing, which by itself is a variation of the ancient art of monetizing information. Brokers accumulate and process information from government agencies, private partners, academic institutions and cyberintel forums. Afterwards they distill the data collected into an actionable product which private enterprises can purchase and employ directly in order to bolster their cybersecurity posture. By cycling this model of intelligence delivery, brokers boost the stability of business operations and allow stakeholders to put active corporate security in action – to address potential vulnerabilities in a proactive manner, thereby generating a rise in security and cost savings. Nevertheless, it is the broker's responsibility to ensure that the intelligence delivered is both accessible and applicable while also adhering to the specific needs of various stakeholders.

As an addition to intelligence sharing, the services of cybersecurity brokers include compliance support that is crucial for stakeholders when it comes operating in a complex regulatory landscape. As a starting point in this process, brokers need to foster an understanding among stakeholders that maintaining compliance should not be viewed as a regulatory requirement, but as a business asset, providing a competitive advantage and business trust. From there on, brokers have the dual responsibility by first fostering contact with compliance expertise that stakeholders lack in-house and second, advocating for a regulatory environment within PPPs, which is in support for innovation and security, thus generating a boon for investment and compliant operations among stakeholders. In this manner, on a micro level the brokers have the potential to reshape the image of compliance as a benchmark for customer trust and business reliability.

Cybersecurity brokers can also serve as a bridge between SMEs and access to scalable affordable cybersecurity solutions. Usually small and medium companies struggle with allocating major resources for cybersecurity, which in turn makes them a potential target for a cyberattack which would usually leave an enterprise crippled or closed. To address the accessibility gap brokers are coming up with flexible forms of receiving solutions as to reduce the financial stress and remove the need for extensive in-house investments, which are related to the traditional understanding of corporate cybersecurity. For instance, EDIH Trakia is a concrete example of this model by granting access to technological solutions, which are generally kept behind a solid paywall: High-performance computing (HPC) and Cyberrange as a service. By doing so, the DIH establishes an ecosystem consisting of stakeholders from the public, academic and private sectors of Bulgaria, which in turn is a perfect business ground where cybersecurity brokers can facilitate partnerships, address both immediate cybersecurity issues and lay foundations for strategic innovation goals.

Furthermore, brokers are also key in streamlining and coordinating the adoption of incident response strategies and corporate subculture. This practice is shown through the establishment of pre-determined protocols, clear communication channels, responsibility chain, response teams and more. Thanks to the proactive approach brokers guarantee that no enterprise is left alone in mitigating the cascading results, but rather supported by a network of resources and expertise in the event of a cyber incident. The micro level benefits for enterprises in this context consist of reduced downtime, reduced data loss and protection of corporate reputation, whereas the macro level benefits include greater stakeholder engagement and market stability.

IV. Risks and Challenges

Having in mind all the positives associated with public-private partnerships in cybersecurity, one must not forget that they are not without any inherent risks or challenges. It is accepted that the primary challenge of this model is the issue of data privacy. Such collaborations often involve a grand amount of data being exchanged between private parties and public institutions, which in turn requires data protection mechanisms. Reaching the desired level of balance between privacy and the need to share intelligence is often regarded as a daunting task, because when enterprises share information with other stakeholders, especially on an international level, there are often numerous concerns being raised regarding information being accessed by unauthorized stakeholders or data being used beyond its intended scope. In order to combat such challenges cybersecurity brokers within PPPs need to define a concrete set of guidelines for every context which allow for intelligence exchange without a compromise to confidentiality, but also actively excluding any hinderance to the business operations.

In the context of data exchange, there is an additional challenge lying in the management of competitive intelligence risks. It is common knowledge that for an enterprise the value and understanding of cybersecurity is typically found in the competitive advantage of securing business and customer data. In contrast to that, when a stakeholder takes part in a PPP, especially one related to cybersecurity, he might be required to disclose corporate intelligence with competitors as a part of a collaborative commitment to a public-private partnership. The challenge to this model introduces a certain vulnerability for sensitive information to be unintentionally shared or misappropriated. Consequently, it is up to the brokers to control such risks by implementing anonymization and aggregation methods which guarantee that the data employed in mutual projects does not contain specifics regarding an enterprise, thereby eliminating the need for undue corporate risks.

Trust is brought into consideration in the context of every single partnership; therefore, it is imperative that this challenge is addressed proactively in a setting which brings together not only diverse and cautious stakeholders, but also ones hailing from different sectors – public, academic and private. When engaging a partnership in this context, it is more than normal for concerns such as data misuse, regulatory overreach or a misunderstanding in priorities to arise. Companies might suspect that public agencies will prioritize national over business interests and vice versa, thus compromising the project on a conceptual level. To mitigate this, brokers are tasked with keeping a strict neutral stance by representing the interests of all stakeholders involved, as well as highlighting the common ones as a foundation for dialogue. Furthermore, they can employ trust-building mechanisms such as third-party audits or mutual oversight commissions that control whether data is handled in accordance with previously agreed-upon standards.

In summary, the nature of cybersecurity PPPs brings forth challenges such as data privacy, competitive intelligence and stakeholder trust and therefore requires the expertise of cybersecurity brokers. By handling competitive risk and caution, keeping rational safeguards on privacy and fostering trust, brokers allow for stakeholders to become a part of a public-private partnership and generate value without putting at risk their own interests. Through the use of examples, it becomes clear that brokers are indispensable not only as initiators of business but play a two-faced role in the process of balancing varying stakeholder interests for the common goal of delivering concrete results in the collaborative landscape of cybersecurity PPPs.

V. Ethical and Privacy Concerns

For a public-private partnership in cybersecurity to truly be able to work and generate stakeholder value, it must put ethical and privacy considerations on a central point in its operations. The collaborative essence of PPPs and the significant data exchange related to it brings forth complex ethical dilemmas such as the risk of data misuse and instrumentalization for the purposes for an agenda different than the initial one. As mentioned above, the context of such a PPP model predisposes private entities towards caution, making them dwell on the dilemmas of sharing sensitive information with public agencies and whether the whole process could pose as a risk to their operations and competitive standing.

An essential element for establishing trust and confidence in PPPs is the emphasis on privacy preservation, which cybersecurity brokers must intricately navigate toward the balance between individual and corporate rights. This comes to light thanks to the use of privacy-preserving solutions such as data anonymization and encryption. Through their employment, brokers gain the advantage of distributing

relevant intelligence without actually disclosing data, which would otherwise be identifiable and thus bring unwanted consequences for certain stakeholders. In this manner, enterprises can freely pool corporate data which in turn contributes to the formation of threat intelligence without facing any risk of compromising their own competitiveness. By doing so, companies not only foster future cybersecurity initiatives and sector stability, but also gain a competitive advantage as a reputational boon, highlighting their commitment to ethical and responsible practices.

In conclusion, the sustainability and effectiveness of cybersecurity-focused PPPs are heavily reliant on ethical and privacy consideration. Brokers ensure this model by balancing security needs with ethical obligations through data handling practices and ethical standards, which allow stakeholders to engage deep into shared cybersecurity projects by also keeping a high standard of data integrity and data trust.

VI. Conclusion

The rise of cyberthreats in the modern economy is bound to drive the search for cybersecurity solutions delivered by a public-private partnership doing business in the sector. Through cybersecurity brokers, the PPPs will be able to address such needs on a micro level and enable SMEs the access to tailored expertise and shared resources such as intelligence and scalable solutions. In doing so, PPPs will showcase the transformative impact of cybersecurity PPPs on every level of the digital economy.

This model of public-private collaboration will only be becoming more widespread in the long turn as the emergence and rapid adoption of high technologies continues. Such examples include the AI revolution of 2023, which will be followed by AI-powered threat intelligence platforms and other cutting edge cybersecurity solutions that in turn will require the expertise of cybersecurity brokers in order to enter the reach of more modest enterprises. Moreover, it is expected from brokers to not only stay in business but to thrive in the sector, thanks to the need of support from companies when it comes down to navigating regulatory alignment, data privacy laws and access to solutions to maintain business efficiency.

In sum, engaging with cybersecurity brokers and being a part of PPPs is viewed as a golden opportunity for private enterprise due to the ability to easily tap into public and private cybersecurity investments, advanced threat intelligence, up-to-date business stability and many more examples of digitalization. As in the case of EDIH Trakia, such collaborations allow SMEs to harness public sector support, backed by academic expertise to be cybersecure in a cost-effective manner. Moreover, a long-term engagement between an enterprise and a broker will on a micro level have substantial mutual benefit and thereby enhance the resilience of the digital economy on a macro level. By doing so, the model will continue proving the pivotal role of brokers of cybersecurity in a digital business landscape that supports both public and private sectors alike.

References

[1] Carr, A. (2016). Public–private partnerships in national cyber-security strategies. International Affairs. The Royal Institute of International Affairs.

[2] European Digital Innovation Hub Trakia. (2021). Digital Europe Programme (DIGITAL) Dissemination and Exploitation Plan D 2.2

[3] The European Union Agency for Cybersecurity. (2017). Public Private Partnerships (PPP): Cooperative models

[4] Даскалов, Х. (2024). ЕВРОПЕЙСКИЯТ ЦИФРОВ ИНОВАЦИОНЕН ХЪБ ТРАКИЯ И ПРАВОТО НА (САМО)ЗАЩИТА В ДИГИТАЛНОТО ПРОСТРАНСТВО

[5] Даскалов, Х & Атанасов, С. (2024). КИБЕРПОЛИГОНЪТ НА ЕЦИХ ТРАКИЯ ПО ПРОЕКТ „CYBER4ALLSTAR“ КАТО СРЕДА ЗА РАЗВИТИЕ НА ЕКСПЕРТИ В СФЕРАТА НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ В ЮЖЕН ЦЕНТРАЛЕН РЕГИОН“