

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/382378756>

Entrepreneurship Opportunities in Cybersecurity

Chapter · June 2024

DOI: 10.4018/979-8-3693-3498-0.ch008

CITATIONS

0

READS

122

3 authors, including:



Nick Rahimi

University of Southern Mississippi

60 PUBLICATIONS 308 CITATIONS

[SEE PROFILE](#)



Saydul Akbar Murad

University of Southern Mississippi


39 PUBLICATIONS 386 CITATIONS

[SEE PROFILE](#)

Chapter 8

Entrepreneurship Opportunities in Cybersecurity

Nick Rahimi


 <https://orcid.org/0000-0002-1964-1794>

University of Southern Mississippi, USA

Saydul Akbar Murad

University of Southern Mississippi, USA

Sarah B. Lee

 <https://orcid.org/0000-0002-3770-5480>

University of Southern Mississippi, USA

ABSTRACT

Cybersecurity is becoming the center stage and the rightful stage for geopolitical and global business. With data privacy regulations in place, the world has experienced serious attacks. These attacks need specialized attention from highly skilled personnel to counter them. From the international perspective, venturing in cybersecurity business requires one to apply new approaches towards countering the attacks. Cybersecurity companies have raised over 21 billion dollars to create enough capital to enhance security and control. More cybersecurity unicorns such as Orca, Claroty, Wiz, Axonius and BigID have emerged to give their contribution. More and more entrepreneurs have identified this opportunity and are willing to benefit from such funding for easy startups. More than three million cybersecurity opportunities are yet to be exploited. This has been as a result of the talent gap between client's expectation and what service providers are able to offer. New entrepreneurs can utilize this opportunity and adopt the right technology when handling active cyber-attacks.

INTRODUCTION

In an era marked by rapid digital transformation, cyberspace has become a dynamic and constantly evolving domain. This evolution has opened a plethora of entrepreneurial opportunities, particularly in the field of cybersecurity. As businesses globally embrace technologies such as cloud services and

DOI: 10.4018/979-8-3693-3498-0.ch008

Entrepreneurship Opportunities in Cybersecurity

broaden their internet usage, there emerges a critical need for measures to safeguard their digital assets and operations.

The importance of cybersecurity entrepreneurship cannot be overstated in this digital age. With businesses integrating new technologies at an unprecedented rate, they inevitably face heightened risks of cybercrime, including data breaches and attacks from sophisticated hacker groups. These cyber-threats not only jeopardize sensitive data but also pose a significant risk to the overall integrity and performance of businesses. Hence, the emergence of cybersecurity as a vital sector provides a unique and urgent opportunity for entrepreneurs who can offer innovative solutions to combat these evolving digital threats.

This chapter within “Generating Entrepreneurial Ideas With AI” illuminates the diverse and burgeoning field of cybersecurity as a fertile ground for entrepreneurial ventures. The chapter aims to bridge the gap between the fast-paced world of cyber technologies and the strategic approach required for successful entrepreneurship in this area. It focuses on guiding prospective entrepreneurs through the cybersecurity landscape, highlighting how they can leverage artificial intelligence (AI) to identify, evaluate, and capitalize on emerging opportunities.

Scope of the Book Chapter:

- The chapter provides a comprehensive overview of current and emerging trends in cybersecurity, including an analysis of common cyber threats and technological advancements.
- It identifies specific entrepreneurial opportunities within cybersecurity, highlighting successful case studies and unmet market needs.
- The role of AI in cybersecurity ventures is explored, focusing on its use in threat detection, risk assessment, and decision-making.
- Strategies for developing effective cybersecurity business models are discussed, including aspects of capital acquisition and regulatory navigation.
- Finally, the chapter addresses ethical considerations in cybersecurity entrepreneurship and offers insights into the future outlook of the industry.

This paper begins with an exploration of our research methodology, followed by a conceptual framework centered on the cybersecurity entrepreneurial ecosystem and its interconnected components. We then delve into the theoretical framework, examining how entrepreneurs utilize internal resources and capabilities in the cybersecurity market. This leads to a discussion on environmental opportunities, where we analyze the cybercrime market, its risks, and strategies for seizing opportunities. We then present global funding patterns in cybersecurity, highlighting investment trends. The paper progresses to examine the cybersecurity market capitalization, focusing on spending patterns. Next, we explore emerging technologies like ML, AI, and blockchain in cybersecurity entrepreneurship and investigate common cyber-attacks. We also address the challenges entrepreneurs face in cybercrime ventures, followed by proposing solutions and recommendations for protecting businesses against cyber-attacks. Then we discussed future research direction. The paper concludes with a summary of our findings and insights.

Entrepreneurship Opportunities in Cybersecurity

RESEARCH METHODOLOGY

The foundation of this study rests upon a comprehensive review of existing literature related to entrepreneurship opportunities in cybersecurity. The literature review serves as a critical component in shaping the understanding of the entrepreneurial landscape within the cybersecurity domain. By synthesizing insights from academic research, industry reports, case studies, and expert analyses, this review aims to provide a robust framework for exploring various facets of entrepreneurship in cybersecurity.

CONCEPTUAL FRAMEWORK

The conceptual framework revolves around the idea of a cybersecurity entrepreneurial ecosystem, comprising various interconnected elements such as:

- **Entrepreneurs:** Individuals or teams identifying and exploiting opportunities in the cybersecurity market.
- **Venture Capitalists and Investors:** Entities providing financial resources and expertise to cybersecurity startups.
- **Incubators and Accelerators:** Organizations offering support services, mentorship, and networking opportunities to cybersecurity entrepreneurs.
- **Government and Regulatory Bodies:** Entities shaping the regulatory environment and providing policy support for cybersecurity innovation.
- **Academic and Research Institutions:** Institutions conducting research and providing education and training in cybersecurity entrepreneurship.
- **Industry Partners and Customers:** Corporations and organizations seeking cybersecurity solutions and collaborating with startups for innovation.

This framework illustrates the interconnectedness and interdependencies among these elements, highlighting the collaborative efforts required to foster entrepreneurship and innovation in the cybersecurity domain.

THEORETICAL FRAMEWORK

The Resource-Based View (RBV) theory can serve as a theoretical lens to understand how entrepreneurs support internal resources and capabilities to exploit opportunities in the cybersecurity market. By identifying and leveraging unique resources such as technological expertise, intellectual property, and strategic partnerships, entrepreneurs can gain a competitive advantage and sustain long-term success in the cybersecurity industry.

Entrepreneurship Opportunities in Cybersecurity

Institutional Theory

Institutional theory provides insights into the external institutional environments shaping entrepreneurial activities in cybersecurity. Entrepreneurs must navigate regulatory frameworks, industry standards, and socio-cultural norms influencing the adoption of cybersecurity solutions. Understanding institutional pressures and institutional logics can help entrepreneurs align their strategies with prevailing norms and regulations while fostering legitimacy and trust in their offerings.

Entrepreneurial Ecosystems

The concept of entrepreneurial ecosystems highlights the interconnectedness of various stakeholders, including entrepreneurs, investors, policymakers, and support organizations, in fostering entrepreneurial activities. By analyzing the dynamics of entrepreneurial ecosystems in the cybersecurity sector, researchers can uncover opportunities for collaboration, knowledge exchange, and ecosystem development to support the growth of cybersecurity startups and ventures.

ENTREPRENEURIAL OPPORTUNITIES

Since all businesses require cybersecurity, there are various business opportunities where one can focus on control and management of all known and unforeseen risks. This is because with the increased cyberspace, opportunities do not match the approaches of providing the desired protection. Cybercrime organizations have failed to adequately employ risk resilience tactics as one way of managing and mitigating any potential threat from cyberspace activity for the benefit of their clients (Hurel & Lobato, 2018).

Cybercrime involves targeted and sophisticated attacks against a particular business entity. Therefore, it is necessary to undertake appropriate security measures to respond to those specific crimes. This can be done by putting relevant resilience programs that can tackle any uncertainty. This presents another entrepreneurship opportunity where the venture can come up with a comprehensive rapid-response system to cybercrimes.

Cyber resilience is the ability to anticipate to a certain degree of uncertainty. This is because it may be difficult to accurately anticipate what is likely to happen in cyberspace. The increasing and sophisticated mal-space threats have posed a challenge for most of these service providers in keeping pace with the attacks (Atoum et al., 2014; Humayun et al., 2020). Cyber-attacks will always occur regardless of the efforts one put to offer protection. However, cyber resilience will ensure success and sustainability of an enterprise even when subjected to a very serious attack.

State of Cybercrime Market

Cybersecurity market is not as flooded as other markets. This market is well funded as tech market analysts predict that it has been receiving billions of dollars due to its sensitivity. This increased funding has offered ideal terms for entrepreneurs. To enter this market, you should understand that it is composed of strong players. Cyber deception and SCADA security have ventured into the market with newly advanced technology to curb any cybercrime attempts (Igre et al., 2006). The Strategic Information Security Officers (SISO) have been overwhelmed with dozens of cases that need to be evaluated and

Entrepreneurship Opportunities in Cybersecurity

maintained due to large market demands. These established vendors are yet to meet the market demands and therefore, more entrepreneurial ventures need to be undertaken (Goodyear et al., 2012).

Entrepreneurs need to evaluate all cybersecurity technologies so that they can identify a niche where they can focus on and exploit it. Funding conditions should not be a barrier to market entry. This is because breaches occur on a daily basis and businesses will not be willing to incur such losses. Instead, they will be willing to engage investors who are able to help them avoid any unforeseen risks.

It is also clear that most of the enterprises lack cybersecurity talents. According to Cisco, there are more than 1 million cybersecurity opportunities in the world and the number keeps increasing. It is believed that by 2023 it may reach above 1.5 million (Burrell, 2020; Iavich et al., 2019). Peninsula Press has recently estimated that there are more than 209,000 unexploited opportunities in the US alone (Rahimi et al., 2018). Many organizations consistently search for solutions from cybersecurity investors and therefore, this deficit can be effectively eliminated. Most of the companies are not willing to work without these critical services and are always willing to advance cybersecurity.

However, there is a dilemma that has arisen in these entrepreneurship opportunities in cybersecurity. This is because of the challenges faced by the security professionals due to continuous technological advancements which spur the urge for innovative and new security solutions. However, despite these technological disruptions, cybersecurity always gets a new market within a short span of time. This gives entrepreneurs hope to remain relevant in the market since the emergence of new technology comes with a better way of solving the problems presented with the technology. For instance, the technology of drones, virtual containers, and autonomous vehicles has created better opportunities in this market for entrepreneurs. For example, a creative entrepreneur would think of coming up with a technology capable of spawning various and massive security issues.

Opportunities With Serious Risks

Many cyber criminals have used cyberspace as a hunting ground where they bring disruption and even bring down governments and large corporations through online attacks with the aim of getting financial benefits. This calls for the new business ventures in cybersecurity to remain resilient so as to counter the unforeseen events (Lehto & Neittaanmäki, 2015).

It is estimated that cybercrime industry has experienced rapid growth where the annual global economy is about \$400 billion (Chandna & Tiwari, 2023). This income is tentatively higher than most countries' national income. Those industries reduce the development of cybercrime risks and support the targeted industries from suffering losses. It is also true that some businesses underestimate the risk they can get from such crimes and then find it not necessary to get such services.

Furthermore, cybercriminals often exploit vulnerabilities in critical infrastructure systems, such as energy grids, transportation networks, and healthcare facilities, posing significant risks to public safety and national security. The potential consequences of cyber-attacks on these essential services can be catastrophic, leading to widespread disruption, loss of life, and economic devastation. As such, there is an urgent need for cybersecurity entrepreneurs to develop innovative solutions to safeguard critical infrastructure against emerging cyber threats and enhance resilience to cyber-attacks.

Moreover, the proliferation of internet-connected devices and the advent of the Internet of Things (IoT) have introduced new vectors for cyber-attacks, amplifying the scope and complexity of cyber threats. From smart home devices and wearable technology to industrial control systems and autonomous vehicles, IoT devices are susceptible to exploitation by cybercriminals seeking to infiltrate networks,

Entrepreneurship Opportunities in Cybersecurity

steal data, and disrupt operations. As the number of IoT devices continues to skyrocket, cybersecurity entrepreneurs must address the unique security challenges posed by this interconnected ecosystem and develop robust solutions to protect IoT devices and networks from cyber-attacks.

Additionally, the rise of state-sponsored cyber warfare and cyber espionage activities has further heightened the urgency for enhanced cybersecurity measures on a global scale. Nation-states and state-sponsored threat actors routinely target government agencies, military organizations, and critical infrastructure assets in pursuit of geopolitical objectives and strategic advantage. These sophisticated cyber-attacks often involve advanced persistent threats (APTs) and zero-day exploits, making them difficult to detect and mitigate. In response, cybersecurity entrepreneurs must collaborate with government agencies, cybersecurity researchers, and industry partners to develop advanced threat detection and attribution capabilities and bolster cyber defenses against state-sponsored cyber threats.

Strategies of Exploiting the Entrepreneurial Opportunities

For the new entrepreneurs willing to build a strong cybersecurity startup, they have a wide range of approaches to adopt. It is very important for the new entrepreneur to recognize that a viable business model is not obtained from brilliant technology. Instead, one has to perform due diligence to satisfy the need of the existing markets where opportunities exist. You should think of building and selling, otherwise, it will be very difficult to make entry into the market (Lilli, 2020)(Chen, 2019).

An entrepreneur must understand the difference between emergency issues and non-emergency ones (Portna et al., 2019). For instance, just a few years ago, no one thought about drones, and autonomous vehicles. Their security and invention were an afterthought, and these afterthoughts can translate to a billion-dollar business (Yağdereli et al., 2015). However, it is advisable for the entrepreneurs not to create a technology before ensuring that the market is ripe for it. This is because it will be costly to educate customers on a problem that is yet to manifest. After that problem comes to fruition, other entrepreneurs will be ripe from your hard work and benefit from your spending. Therefore, this implies that one has to be speculative enough to understand the approach to undertake towards the markets that are yet to develop and anticipate future demands.

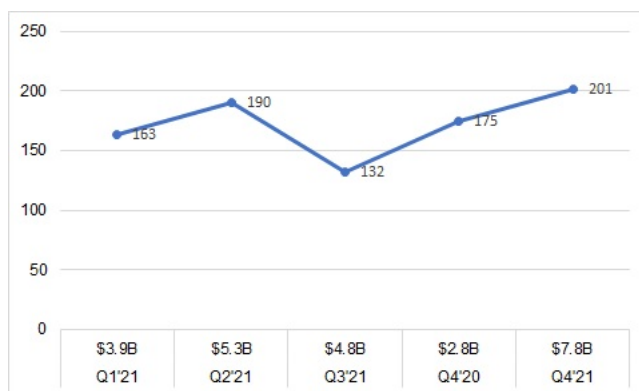
Entrepreneurs should not just feature; instead, they should come up with platforms that are solution oriented (Rahimi et al., 2021). Regardless of your startup size, you should be able to think big. You should initially design a structured solution and integrate it with the available security portfolios. Then try to solve interrelated problems. This will build your reputation and enhance your ability to handle various security dimensions regardless of any indispensable technology.

GLOBAL FUNDING PATTERN

Cybersecurity companies have raised over 21 billion dollars. This funding has been attributed to the attempt to create enough capital bases to enhance cybersecurity and control (Goel, 2020). More cybersecurity unicorns such as Orca, Claroty, Wiz, Axonius and BigID have emerged to give their contribution (Plachkinova et al., 2021). More and more entrepreneurs have seen this opportunity and are willing to benefit from such funding for easy startup. Figure 1. shows the global funding pattern.

Entrepreneurship Opportunities in Cybersecurity

Figure 1. Global funding pattern



The funding environment in today's world reflects the growing opportunity and demand for new entrepreneurs to grow into large scales and become fully independent enterprises. For instance, in the recent past, very few large incumbents dominated the cybersecurity market. They included the Symantec, Cisco, Checkpoint and Palo Alto Networks (Efthymiopoulos, 2019). They had completely dominated the market without any opportunity for new ventures. However, with the increased demand for cybersecurity services and increased external support, new businesses in this field have started penetrating the market (Monica Herz et al., 2016). In those days, the new entrepreneurs only opted to join the only existing giants and work under them. Due to CISOs' increased desire to buy security from new entrepreneurs and the increased technological changes, it has greatly propelled the new startups grow into a cyber-giant. After identifying a niche, they quickly seize the opportunity and become specialized in that field (Jenab et al., 2016).

CYBERSECURITY MARKET CAP

From the tables, it is very clear that Okta, ZScaler, Splunk and CrowdStrike are examples of companies that have not stayed in the market for a long time, but are among the greatest security companies (Rahimi & Gupta, 2021). This indicates that the market is favorable for new entrepreneurs to thrive. The Table 1 below shows the cybersecurity market cap (Analyst & 2010, n.d.).

Entrepreneurship Opportunities in Cybersecurity

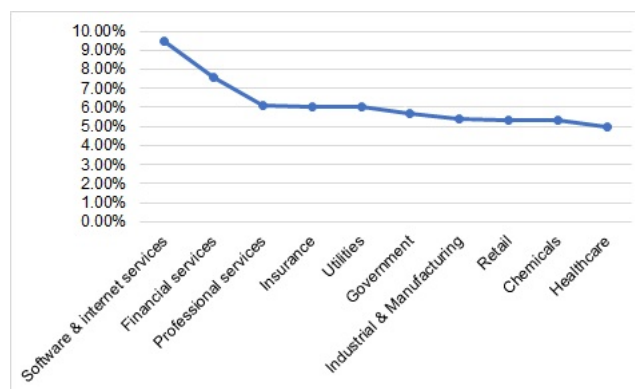
Table 1. Cybersecurity market cap for 2021

Name	Market Cap (\$B)
Symantec Corp	15
Check Point	16
Splunk	19
Verisign	24
Cloudflare	28
Okta	29
Zscaler	34
CrowdStrike	38
Fortinet	46
Palo Alto Networks	48

The Pattern of Security Spend

Cybersecurity can be said to be a wide market with an estimated annual spending of about 150 billion dollars. This accounts for 6% of the total IT spending. However, this security spending varies widely on a vertical dimension with cloud companies having the highest security spending of about 95% of the entire IT budget. With this data, it can be expected that more entrepreneurs can identify that niche and fit as a vertical industry. This will help them employ cloud technology and invest widely in cybersecurity. This will enable the industries to offer more software solutions rather than offering other non-digitalized solutions. Figure 2. Shows cyber spend variation in 2020 (Ferrillo, 2021; Uddin et al., n.d.).

Figure 2. Cyber spend variation



There are many drivers evidenced to cause this change in spending as outlined by CISOs. Entrepreneurial opportunities presented in the cybersecurity need the entrepreneurs to understand that there are increased regulations like CCPA and GDPR that require all the businesses dealing with delicate con-

Entrepreneurship Opportunities in Cybersecurity

sumer data to safeguard it or risk losing their reputation and facing costly fines. This acts like a caution to the cybersecurity providers when handling vast amounts of consumer data that is sensitive to be extra careful (Krishnamurthy, 2020).

According to CB Insights, the cyber market has been flooded with significant capital investment for the new ventures (Murad & Rahimi, 2023, 2024). These acts as a remarkable support to any company that desires to enter the market. For instance, 2017 was the year that broke the record for financial deals in this sector with 7.6 billion dollars invested in 552 new ventures. The U.S. has been leading in these investments followed by Israel and then UK with 69, 7% and 6% of the total deals respectively (Policy & 2017, 2017; Rahimi et al., 2019).

EMERGING TECHNOLOGIES AND TRENDS FOR CYBERSECURITY ENTREPRENEURSHIP

The landscape of cybersecurity is constantly evolving, driven by emerging technologies and new trends that present both challenges and opportunities for entrepreneurs. Understanding these emerging technologies and trends is crucial for entrepreneurs looking to capitalize on the ever-changing cybersecurity market. We explore some of the emerging technologies and trends that present new opportunities for cybersecurity entrepreneurs to innovate and excel in this dynamic field.

Artificial Intelligence (AI) and Machine Learning (ML)

Artificial intelligence and machine learning are revolutionizing cybersecurity by enabling automated threat detection, predictive analysis, and adaptive defense mechanisms. Entrepreneurs can leverage AI and ML algorithms to develop advanced security solutions capable of identifying and mitigating cyber threats in real-time. Here are some specific applications:

- **Anomaly Detection:** AI can analyze vast amounts of network traffic data to identify unusual patterns that might indicate a potential attack. This allows for early detection and response, minimizing damage.
- **Behavior Analysis:** Machine learning algorithms can analyze user behavior patterns to detect anomalies that might indicate compromised accounts or insider threats.
- **Adaptive Authentication Systems:** AI can continuously learn and adapt authentication protocols based on user behavior and threat intelligence, making it harder for attackers to bypass traditional methods.
- **Automated Incident Response:** AI-powered systems can automate tasks like threat investigation, containment, and remediation, expediting the response timeline and reducing human error.

Blockchain Technology

Blockchain technology offers decentralized and immutable data storage, making it inherently secure against tampering and unauthorized access. Entrepreneurs can explore opportunities in blockchain-based cybersecurity solutions:

Entrepreneurship Opportunities in Cybersecurity

- **Secure Identity Management:** Blockchain can create tamper-proof digital identities that users control, eliminating the need for centralized databases vulnerable to breaches.
- **Decentralized Authentication:** Blockchain can facilitate secure logins without passwords, reducing the risk of credential theft and phishing attacks.
- **Transparent Audit Trails:** Transactions and activities on a blockchain network are permanently recorded and verifiable, enhancing accountability and compliance.
- **Securing IoT Devices:** Blockchain can be used to manage access permissions and encrypt data communication between IoT devices, hindering unauthorized access and data manipulation.

Internet of Things (IoT) Security

The proliferation of IoT devices presents significant cybersecurity challenges, as these devices often lack robust security measures and are vulnerable to exploitation by malicious actors. Entrepreneurs can develop IoT security solutions focused on:

- **Device Authentication:** Implement secure mechanisms for verifying the identity of IoT devices on a network, preventing unauthorized devices from connecting.
- **Data Encryption:** Develop encryption solutions specifically designed for the resource-constrained nature of many IoT devices to protect sensitive data in transit and at rest.
- **Intrusion Detection:** Create intrusion detection systems (IDS) tailored to monitor IoT device activity and identify suspicious behavior that might indicate an attack.
- **Secure Communication Protocols:** Develop secure communication protocols that ensure data integrity and confidentiality between IoT devices and other components of the network.

Cloud Security

As organizations increasingly migrate their data and applications to the cloud, ensuring the security of cloud-based environments becomes paramount. Entrepreneurs can innovate in the field of cloud security by developing solutions for data encryption, access control, and threat intelligence tailored to cloud infrastructures. Addressing concerns such as data privacy, compliance, and regulatory requirements will be crucial for success in this space.

Quantum Computing and Post-Quantum Cryptography

The advent of quantum computing poses new challenges to traditional cryptographic algorithms, potentially rendering current encryption methods obsolete. Entrepreneurs can explore opportunities in post-quantum cryptography, which aims to develop quantum-resistant cryptographic techniques capable of securing data against quantum-enabled attacks. Investing in research and development of quantum-safe encryption solutions will be essential for staying ahead of future threats.

Entrepreneurship Opportunities in Cybersecurity

Threat Intelligence and Cyber Threat Hunting

Threat intelligence platforms and cyber threat hunting services are becoming indispensable tools for organizations seeking to proactively identify and mitigate cyber threats. Entrepreneurs can develop innovative solutions for aggregating, analyzing, and visualizing threat intelligence data to empower organizations in their cybersecurity operations. Leveraging machine learning and data analytics techniques can enhance the effectiveness of threat detection and response efforts.

Privacy-Preserving Technologies

With growing concerns about data privacy and regulatory compliance, there is a rising demand for privacy-preserving technologies that enable secure data sharing and collaboration. Entrepreneurs can explore opportunities in cryptographic techniques such as homomorphic encryption, secure multi-party computation, and differential privacy to develop privacy-enhancing solutions for protecting sensitive information in transit and at rest.

Incorporating these emerging technologies and trends into cybersecurity entrepreneurship ventures can position entrepreneurs to address evolving cyber threats and capitalize on market opportunities in an increasingly digital and interconnected world.

COMMON CYBER ATTACKS

It should be noted that cybersecurity is extremely critical in protecting data and systems from threats. However, this is not the solemn purpose, but it also contributes to the protection of customers, gaining client confidence, reducing chances of collapsing your website and increasing the general productivity.

Figure 3. Common cyber-attacks

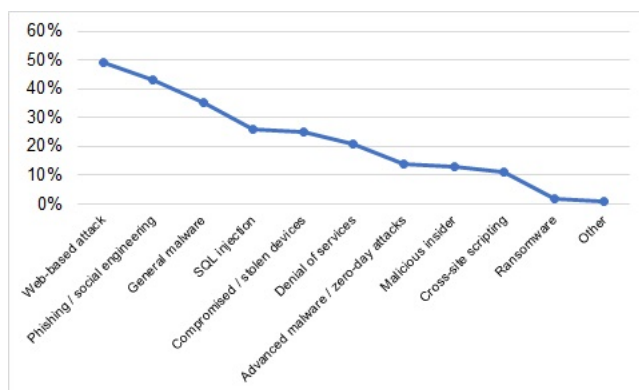


Figure 3. shows the percentages of common cyber-attacks most organizations are likely to experience. From Figure 3, the web-based attack forms the highest percentage with 49% of the total likely attacks. On the other hand, ransomware is the lowest possible attack with 2 per cent of the total likelihood attacks.

Entrepreneurship Opportunities in Cybersecurity

This graph helps the new entrepreneurs in determining which area is of great risk and what strategies can they employ to achieve optimal solution to the possible cyber-attacks (Oueslati et al., 2019; Pattanayak et al., 2018; Rahimi & Martin, 2020).

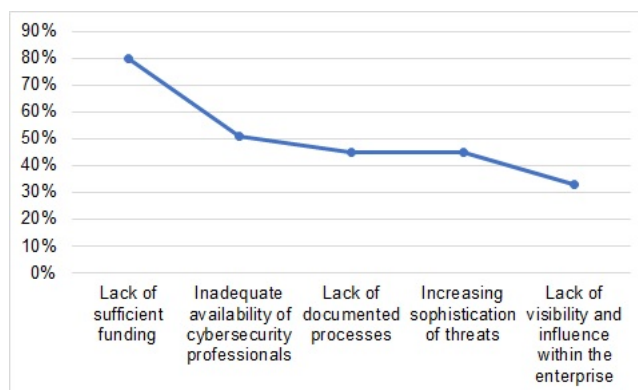
CHALLENGES AN ENTREPRENEUR IS LIKELY TO ENCOUNTER IN CYBERCRIME VENTURE

Although cybersecurity has received significant funding, this may not be sufficient for all entrepreneurs, posing a challenge that needs consideration. Moreover, the talent gap in cybersecurity presents a significant hurdle. While numerous opportunities exist in this field, the shortage of skilled cybersecurity professionals limits the ability of entrepreneurs to fully capitalize on these prospects.

Another notable challenge is the absence of a well-documented process. Merely recognizing entrepreneurship opportunities in cybersecurity is insufficient without a systematic approach to handling and managing cyber-attacks. As threats become increasingly sophisticated due to continuous technological advancements, entrepreneurs must remain agile and adept at leveraging existing technology to effectively combat cybercrimes.

Furthermore, the lack of visibility presents a formidable challenge. Entrepreneurs must possess the foresight to anticipate future developments and prepare for unforeseen outcomes. In addition, navigating the complex regulatory landscape adds another layer of complexity to cybersecurity ventures. Compliance with various regulations and standards requires careful attention to detail and may entail significant time and resources. Lastly, the evolving threat landscape constantly introduces new challenges and risks. Cyber adversaries continuously adapt their tactics, making it essential for entrepreneurs to stay vigilant and proactive in identifying and mitigating emerging threats. Figure 4, below is the graph of the challenges they are likely to encounter in cybercrime business (Morgan, 2019; Rahimi et al., 2020).

Figure 4. Challenges and entrepreneur may encounter in cybersecurity



Entrepreneurship Opportunities in Cybersecurity

Talent Gap in Cyber Security

The talent gap remains a persistent challenge affecting both cybersecurity providers and their clients. Entrepreneurs can seize this opportunity by adopting appropriate technologies for handling active cyber-attacks, taking into account human capacity to ensure effectiveness. Managing this gap entails offering capabilities that other providers struggle to deploy and maintain. Creativity in recruiting and retaining talent is essential for entrepreneurs to remain competitive and secure a market share in the cybersecurity industry. Understanding client needs and transitioning to annual subscription models can enhance business sustainability. Moreover, initiatives such as the National Security Agency (NSA) and Committee on National Security Systems (CNSS) designation as Centers of Academic Excellence (CAE) have aimed to train cybersecurity talent in recent years, with over [insert number] institutions recognized for their contributions. Additionally, the complex regulatory landscape presents challenges for entrepreneurs seeking to navigate compliance requirements across various industries and jurisdictions. Keeping pace with evolving regulatory frameworks and ensuring adherence to data protection laws adds another layer of complexity to cybersecurity ventures (Jones et al., 2021; Smith & Brown, 2023).

Visibility Gap

Another entrepreneurial opportunity in cybercrime is the visibility gap. Entrepreneurs should be able to identify the visibility gap in digital infrastructure so that they can be able to recognize why, when and where the problem occurs. The survey conducted by McKinsey of about 200 buyers of cybersecurity applications such as security orchestration and security-information in the available enterprise market indicated that more than 60 percent were not able to correctly analyze at least 40 percent of their log data. Therefore, this calls for a third-party involvement to accurately collect and analyze their data (Islam et al., 2019).

Complex Regulatory Landscape

Navigating the complex regulatory environment poses a significant challenge for cybersecurity entrepreneurs. With the increasing emphasis on data privacy and security regulations worldwide, entrepreneurs must ensure compliance with various legal frameworks, which can be daunting and resource intensive. Additionally, regulations are subject to frequent updates and changes, requiring entrepreneurs to stay informed and adapt their strategies accordingly. Failure to comply with regulatory requirements can result in legal penalties, reputational damage, and loss of business opportunities. Overcoming this challenge involves investing in legal expertise, staying abreast of regulatory developments, and implementing robust compliance programs to mitigate risks effectively.

Evolving Threat Landscape

The cyber threat landscape is a relentless adversary, constantly shifting and evolving tactics. Unlike a static battlefield, cybersecurity entrepreneurs face a moving target where cybercriminals relentlessly innovate. They develop ever more sophisticated methods to exploit vulnerabilities across software, hardware, and human behavior. This continuous evolution demands not only effective cybersecurity

Entrepreneurship Opportunities in Cybersecurity

solutions but also agile ones. Legacy approaches built around static defense perimeters are becoming increasingly obsolete.

The challenges for cybersecurity entrepreneurs are multifaceted. Unpredictable attack vectors emerge constantly, with social engineering campaigns bypassing firewalls and weaponized artificial intelligence automating attacks. The interconnectedness of today's technology ecosystem introduces supply chain vulnerabilities, where a seemingly unrelated breach can have a domino effect impacting multiple vendors and their customers. Further complicating the landscape is the evolving regulatory landscape. As cyber threats escalate, governments worldwide enact stricter data protection regulations. This necessitates solutions that address security concerns while complying with these evolving legal frameworks.

To navigate this dynamic environment, cybersecurity entrepreneurs must prioritize several key actions. Continuous threat intelligence is crucial, requiring investment in capabilities that keep them updated on the latest attack trends, malware variants, and emerging vulnerabilities. Security by design becomes paramount. Solutions need to be inherently resilient, incorporating features like zero-trust architecture and encryption from the very beginning of development. Finally, collaboration is key. Fostering partnerships with industry peers, researchers, and security experts allows for knowledge sharing, identification of emerging threats, and the development of collective defense strategies.

By embracing a proactive and adaptable approach, cybersecurity entrepreneurs can stay ahead of the curve. This allows them to develop effective solutions and contribute to building a more secure digital future.

SOLUTIONS AND RECOMMENDATIONS

In an increasingly digitized world, cybersecurity has emerged as a critical concern for individuals, businesses, and governments alike. This section explores key strategies and recommendations aimed at fostering entrepreneurship in cybersecurity, addressing challenges, and maximizing opportunities for aspiring entrepreneurs and stakeholders in the cybersecurity ecosystem.

Enhancing Entrepreneurial Education and Training

Given the technical and business complexities of the cybersecurity industry, there is a need to enhance entrepreneurial education and training programs tailored to aspiring cybersecurity entrepreneurs. Universities, incubators, and accelerators can collaborate to offer specialized programs focusing on cybersecurity entrepreneurship, covering topics such as technology commercialization, venture financing, and cybersecurity risk management.

Facilitating Access to Funding and Resources

To support entrepreneurship in cybersecurity, policymakers and industry stakeholders should work together to facilitate access to funding and resources for startups and emerging ventures. This may involve establishing dedicated funding mechanisms, such as venture capital funds or government grants, specifically targeted at cybersecurity startups. Additionally, initiatives to foster collaboration between startups and established cybersecurity firms can provide access to mentorship, expertise, and market networks.

Entrepreneurship Opportunities in Cybersecurity

Promoting Collaboration and Information Sharing

Collaboration and information sharing are essential for addressing the evolving threat landscape in cybersecurity. Entrepreneurs, cybersecurity professionals, and policymakers should collaborate to exchange knowledge, share best practices, and coordinate responses to cyber threats. Initiatives such as industry consortia, public-private partnerships, and information sharing platforms can facilitate collaboration and collective action to enhance cybersecurity resilience across sectors.

Advocating for Regulatory Clarity and Supportive Policies

Entrepreneurs operating in the cybersecurity industry require regulatory clarity and supportive policies to navigate legal and compliance challenges effectively. Policymakers should engage with industry stakeholders to develop clear and flexible regulations that promote innovation while ensuring cybersecurity safeguards. Additionally, policymakers can provide incentives such as tax breaks, grants, and regulatory exemptions to incentivize entrepreneurship and investment in cybersecurity.

Investing in Research and Development

Investment in research and development (R&D) is crucial for driving innovation and competitiveness in the cybersecurity sector. Governments, industry organizations, and philanthropic entities should allocate resources to support R&D initiatives focused on developing cutting-edge cybersecurity technologies and solutions. By fostering a culture of innovation and supporting breakthrough research, stakeholders can fuel the growth of entrepreneurship and technological advancement in cybersecurity.

By integrating these theoretical frameworks, solutions, and recommendations into your manuscript, you can offer a holistic perspective on entrepreneurship opportunities in cybersecurity and provide actionable insights for entrepreneurs, policymakers, investors, and other stakeholders invested in the cybersecurity ecosystem.

FUTURE RESEARCH DIRECTIONS

As researchers in the field of cybersecurity entrepreneurship, we have explored various dimensions of entrepreneurial opportunities in cybersecurity. Through our analysis of market trends, funding patterns, and common cyber threats, we have identified key areas where entrepreneurs can innovate and create value. Additionally, our examination of the challenges encountered by cybersecurity entrepreneurs has highlighted the importance of supportive ecosystems, access to funding, and regulatory clarity. Looking ahead, we believe there are several promising avenues for future research in this area. Longitudinal studies can provide valuable insights into the evolving nature of entrepreneurship opportunities in cybersecurity over time. Regional analyses can help us understand the nuances of entrepreneurial ecosystems in different geographic regions and identify opportunities for collaboration and growth. Moreover, investigating the impact of emerging technologies such as artificial intelligence, blockchain, and IoT on entrepreneurship in cybersecurity can shed light on new avenues for innovation and disruption. As we continue our exploration of entrepreneurship opportunities in cybersecurity, we remain committed to advancing knowledge and understanding in this critical and rapidly evolving domain.

Entrepreneurship Opportunities in Cybersecurity

CONCLUSION

In summarizing the insights garnered from this review, it becomes evident that the field of cybersecurity presents a fertile ground for entrepreneurial innovation. This is largely due to the vast array of untapped opportunities within the sector, which can be transformed into viable business ventures. Theoretical implications of this finding suggest that cybersecurity entrepreneurship is aligned with theories of market gaps and innovation, where identifying and addressing unmet needs drives business success. Practically, entrepreneurs can gain a competitive advantage in this tightly funded sector by focusing on specific niches that address digital security concerns in various industries, such as logistics, manufacturing, or healthcare.

Furthermore, the rapidly evolving nature of cybersecurity threats means that the relevance of current opportunities can quickly diminish, necessitating continual innovation and adaptation from entrepreneurs. As the threat landscape evolves, entrepreneurs must remain agile and responsive to emerging risks, leveraging cutting-edge technologies and strategic partnerships to stay ahead of cyber adversaries.

Moreover, this review underscores the importance of considering the diverse regulatory environments across different regions, which can significantly impact entrepreneurial ventures in cybersecurity. Entrepreneurs must navigate a complex web of regulations and compliance requirements, often requiring expertise in legal and regulatory affairs to ensure business operations remain compliant and resilient in the face of regulatory scrutiny.

Looking to the future, further research is needed to explore the impact of emerging technologies in cybersecurity and their entrepreneurial applications. Emerging technologies such as quantum computing, artificial intelligence, and blockchain hold immense potential for transforming cybersecurity practices, and entrepreneurs must stay abreast of these developments to capitalize on new opportunities.

Additionally, it is crucial to investigate the role of policy and regulatory frameworks in shaping the landscape of cybersecurity entrepreneurship. Policy decisions at the national and international levels can have profound implications for the cybersecurity industry, influencing funding priorities, regulatory requirements, and market dynamics. Understanding the interplay between policy, technology, and entrepreneurship is essential for building a resilient and innovative cybersecurity ecosystem that can effectively address the evolving challenges of cyberspace.

ACKNOWLEDGEMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

- Analyst, J. M.-T. P. E. 2010, undefined. (n.d.). Smart Grid Cyber-Security Is Big Issue For IT Companies, VCs. *Search.Proquest.ComJ MiyazakiThe Private Equity Analyst*. <https://search.proquest.com/openview/6892dae7d88f7202cdeb7337fb3fe73d/1?pq-origsite=gscholar&cbl=40214>
- Atoum, I., Otoom, A., & Ali, A. A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22(3), 251–264. 10.1108/IMCS-02-2013-0014
- Burrell, D. N. (2020). An Exploration of the Cybersecurity Workforce Shortage. In *Cyber Warfare and Terrorism* (pp. 1072–1081). Concepts, Methodologies, Tools, and Applications. 10.4018/978-1-7998-2466-4.ch063
- Chandna, V., & Tiwari, P. (2023). Cybersecurity and the new firm: Surviving online threats. *The Journal of Business Strategy*, 44(1), 3–12. 10.1108/JBS-08-2021-0146
- Chen, Y. S. (2019). E-entrepreneurship and innovation in franchising. *International Journal of E-Entrepreneurship and Innovation*, 9(1), 1–12. 10.4018/IJEEI.2019010101
- Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, 8(1), 12. Advance online publication. 10.1186/s13731-019-0105-z
- Ferrillo, P. (2021). To over Disclose or Not: That Is the Question with Cybersecurity. *Florida State University Business Review*, 20. <https://heinonline.org/HOL/Page?handle=hein.journals/fsubr20&id=85&div=7&collection=journals>
- Goel, S. (2020). National cyber security strategy and the emergence of strong digital borders. *Connections*, 19(1), 73–86. 10.11610/Connections.19.1.07
- Goodyear, M., Goerdel, H. T., Portillo, S., & Williams, L. (2012). Cybersecurity Management In the States: The Emerging Role of Chief Information Security Officers. *SSRN Electronic Journal*. 10.2139/ssrn.2187412
- Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, 45(4), 3171–3189. 10.1007/s13369-019-04319-2
- Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy*, 3(1), 61–76. 10.1080/23738871.2018.1467942
- Iavich, M., Gnatyuk, S., & Fesenko, G. (2019). *Cyber security European standards in business*. SCSA. https://journal.scsa.ge/wp-content/uploads/2019/07/03_32.pdf

Entrepreneurship Opportunities in Cybersecurity

- Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, 25(7), 498–506. 10.1016/j.cose.2006.03.001
- Islam, C., Babar, M. A., & Nepal, S. (2019). A Multi-Vocal Review of Security Orchestration. *ACM Computing Surveys*, 52(2), 37. 10.1145/3305268
- Jenab, K. (2016). Cyber Security Management: A Review. *Researchgate.NetK Jenab, S Moslehpour-Business Management Dynamics*, 2016•*researchgate.Net*, 5(11), 16–39. https://www.researchgate.net/profile/Kouroush_Jenab/publication/305220294_Cyber_Security_Management_A_Review/links/578510d408aef321de2a8f90.pdf
- Krishnamurthy, V. (2020). Symposium on the GDPR and international law a tale of two privacy laws: The GDPR and the international right to privacy. *AJIL Unbound*, 114, 26–30. 10.1017/aju.2019.79
- Lehto, M., & Neittaanmäki, P. (2015). *Cyber security: Analytics, technology and automation*. Springer. <https://link.springer.com/content/pdf/10.1007/978-3-319-18302-2.pdf>
- Lilli, E. (2020). President Obama and US cyber security policy. *Journal of Cyber Policy*, 5(2), 265–284. 10.1080/23738871.2020.1778759
- Monica Herz, P., Anna Gudrun Christina Leander, P., & Manuel Rebelo Fernandes, L. (2016). *Unraveling the cyber security market: The struggles among cyber security companies and the*. DBD. https://www2.dbd.puc-rio.br/pergamum/tesesabertas/1412452_2016_completo.pdf
- Morgan, S. (2019). 2019 Official Annual Cybercrime Report. *Cybersecurity Ventures*, 12.
- Murad, S. A., & Rahimi, N. (2023). Secure and Scalable Permissioned Blockchain using LDE-P2P Networks. *2023 10th International Conference on Internet of Things: Systems, Management and Security*. IEEE. 10.1109/IOTSMS59855.2023.10325762
- Murad, S. A., & Rahimi, N. (2024). Secure and Efficient Hierarchical P2P Fog Architecture: A Novel Approach for IoT. *IEEE Internet of Things Journal*, 11(10), 1–1. 10.1109/JIOT.2024.3365071
- Oueslati, N. E., Mrabet, H., Jemai, A., & Alhomoud, A. (2019). Comparative Study of the Common Cyber-physical Attacks in Industry 4.0. *2019 International Conference on Internet of Things, Embedded Systems and Communications, IINTEC 2019 - Proceedings*, (pp. 68–74). IEEE. 10.1109/IINTEC48298.2019.9112097
- Pattanayak, A., Best, D., Sanner, D., & Fifth, J. S.-P. (2018). Advancing cybersecurity education: pink elephant unicorn. *DL.Acm.OrgA Pattanayak, DM Best, D Sanner, J SmithProceedings of the Fifth Cybersecurity Symposium*. ACM. 10.1145/3212687.3212862
- Plachkinova, M., & Pittz, T. (2021). Assessing the awareness of cybersecurity within entrepreneurship students: The Cyberpreneurship Project. *Journals.Sagepub.ComM Plachkinova, TPittzEntrepreneurship Education and Pedagogy*, 4(3), 564–582. 10.1177/2515127420913056
- Policy, M. C.-J. of C., & 2017, undefined. (2017). Cyber risk and the changing role of insurance. *Camillo Journal of Cyber Policy*, 2(1), 53–63. 10.1080/23738871.2017.1296878

Entrepreneurship Opportunities in Cybersecurity

Portna, O., Melikhov, A., Dragomirova, I., Noha, I., & Soichuk, R. (2019). Entrepreneurship model of cybernetic security professionals. *Journal of Entrepreneurship Education*, 22(5), 22.

Rahimi, N., & Gupta, B. (2021). Security Issues, Vulnerabilities, and Defense Mechanisms in Wireless Sensor Networks: State of the Art and Recommendation. *Integration of WSNs into Internet of Things*, 1–15. Taylor & Francis. <https://doi.org/10.1201/9781003107521-1/SECURITY-ISSUES-VULNERABILITIES-DEFENSE-MECHANISMS-WIRELESS-SENSOR-NETWORKS-STATE-ART-RECOMMENDATION-RAHIMI-GUPTA>

Rahimi, N., Gupta, B., & Rahimi, S. (2018). Secured data lookup in LDE Based Low Diameter Structured P2P Network. *Proceedings of the 33rd International Conference on Computers and Their Applications, CATA 2018, 2018-March*. CSE. https://www.cse.msstate.edu/wp-content/uploads/2020/04/I6_rahimi.pdf

Rahimi, N., & Martin, N. L. (2020). Challenges and Strategies for Online Teaching in Information Technology and Other Computing Programs. *SIGITE 2020 - Proceedings of the 21st Annual Conference on Information Technology Education*, (pp. 218–222). ACM. 10.1145/3368308.3415369

Rahimi, N., Maynor, J., & Gupta, B. (2020). Adversarial machine learning: Difficulties in applying machine learning existing cybersecurity systems. *EPiC Series in Computing*, 69, 40–47. 10.29007/3xbb

Rahimi, N., Nolen, J., & Gupta, B. (2019). Android Security and Its Rooting—A Possible Improvement of Its Security Architecture. *Journal of Information Security*, 10(02), 91–102. 10.4236/jis.2019.102005

Rahimi, N., Roy, I., Gupta, B., Bhandari, P., & Debnath, N. C. (2021). Blockchain Technology and Its Emerging Applications. *Blockchain Technology for Data Privacy Management*, 133–157. <https://doi.org/10.1201/9781003133391-7/BLOCKCHAIN-TECHNOLOGY-EMERGING-APPLICATIONS-RAHIMI-ROY-GUPTA-BHANDARI-DEBNATH>

Uddin, M. & Mollah, S. (n.d.). *Does cyber tech spending matter for bank stability?* Elsevier. <https://www.sciencedirect.com/science/article/pii/S1057521920302313>

Yağdereli, E., Gemci, C., & Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *Journal of Defense Modeling and Simulation*, 12(4), 369–381. 10.1177/1548512915575803

KEY TERMS AND DEFINITIONS

Artificial Intelligence and Machine Learning: AI and ML refer to technologies and techniques that enable computers and systems to perform tasks and make decisions autonomously or semi-autonomously, leveraging algorithms, data analytics, and pattern recognition to enhance cybersecurity capabilities such as threat detection, anomaly detection, and predictive analytics.

Blockchain: Blockchain is a decentralized and distributed ledger technology that enables secure and transparent recording of transactions across a network of computers. Each block in the chain contains a cryptographic hash of the previous block, creating a tamper-resistant and immutable record of data, transactions, or digital assets.

Entrepreneurship Opportunities in Cybersecurity

Cloud Computing: Cloud computing is a model for delivering computing services over the internet, providing on-demand access to a shared pool of resources, including computing power, storage, and applications. Cloud computing enables organizations to scale resources dynamically, reduce infrastructure costs, and access advanced technologies and services without the need for on-premises hardware or software.

Cybersecurity Risk Management: Cybersecurity risk management involves identifying, assessing, and mitigating potential risks and threats to information systems, networks, and digital assets within organizations, employing strategies such as risk analysis, risk mitigation planning, and security controls implementation.

Entrepreneurial Education: Entrepreneurial education refers to formal and informal learning experiences designed to equip individuals with the knowledge, skills, and mindset necessary to identify, evaluate, and pursue entrepreneurial opportunities in the cybersecurity sector.

Incubators and Accelerators: Incubators and accelerators are programs or organizations that provide support services, mentorship, and resources to early-stage cybersecurity startups and entrepreneurs, helping them develop and grow their businesses through structured programs, networking opportunities, and access to funding.

IoT (Internet of Things): The Internet of Things (IoT) refers to the network of interconnected devices, sensors, and objects embedded with software, sensors, and connectivity capabilities, enabling them to collect, exchange, and analyze data autonomously. IoT technology has applications in various sectors, including smart homes, industrial automation, healthcare, and transportation.

Privacy-Preserving: Privacy-preserving techniques and technologies aim to protect the confidentiality, integrity, and availability of sensitive data and information while ensuring compliance with privacy regulations and standards. These techniques include encryption, anonymization, and differential privacy, which help mitigate privacy risks and enhance data protection in cybersecurity application.

Quantum Computing: Quantum computing harnesses the principles of quantum mechanics to perform calculations and solve complex problems at speeds exponentially faster than classical computers. Unlike classical computers that use binary bits, quantum computers use quantum bits or qubits, which can exist in multiple states simultaneously, enabling them to process vast amounts of data and perform parallel computations.

Technology Commercialization: Technology commercialization is the process of transforming research or innovative ideas into marketable products, services, or solutions within the cybersecurity industry, involving activities such as product development, intellectual property management, and market entry strategies.

Threat Intelligence: Threat intelligence involves collecting, analyzing, and disseminating information about cybersecurity threats, vulnerabilities, and adversaries to support decision-making and enhance security posture. It encompasses activities such as threat monitoring, threat hunting, and intelligence sharing to proactively identify and mitigate cyber risks.

Venture Financing: Venture financing refers to the process of raising capital from investors to fund the growth and expansion of cybersecurity startups and ventures, typically through equity investments, venture capital funding, or other forms of private equity financing.