Cybersecurity Startup Investments

Tetiana Moiseienko[1] and Anastasiia Kiva[1]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," 37 Peremohy ave., Kyiv, 03056, Ukraine*

Abstract

The rapid growth of computer systems in different industries, such as financial systems, industrial equipment, aviation, consumer devices, government and others, means that there is an increasing number of systems at risk. Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information, protected health information, personal information, intellectual property, data, and governmental and industry information systems. This paper examines roles of startups in cybersecurity systems in different industries. Cybersecurity products, services and professionals have never been in higher demand. A contributing factor to the cybersecurity skills gap is the large number of security startups that have been founded in recent years.

Keywords

Computer systems, cybersecurity, cybersecurity market, startup.

1. Introduction

The pandemic has had a major impact on cybersecurity. Cybercrimes now cost the world nearly $600 billion each year, according to Mordor Intelligence - equivalent to nearly 0.8% of the global GDP. Meanwhile, the World Economic Forum reports that the likelihood of identifying and prosecuting the perpetrators of cyberattacks in the U.S. has fallen to a dismal 0.05% [1].

According to a research report "Cybersecurity Market with Covid-19 Impact Analysis by Component (Software, Hardware, and Services), Software (IAM, Encryption, APT, Firewall), Security Type, Deployment Mode, Organization Size, Vertical, and Region—Global Forecast to 2026" published by MarketsandMarkets, In the post-COVID-19 scenario, the global cybersecurity market size is projected to grow from USD 217.9 Billion in 2021 to USD 345.4 Billion by 2026, recording a Compound Annual Growth Rate (CAGR) of 9.7% from 2021 to 2026. The market's growth can be attributed to the increasing awareness and rising investments in cybersecurity infrastructure across global organizations operating across verticals [2].

Amidst the COVID-19 pandemic crisis, various governments and regulatory authorities mandate both public and private organizations to embrace new practices for working remotely and maintaining social distancing. Since then, the digital ways of doing business became the new Business Continuity Plan (BCP) for various organizations. With the widespread use of BYOD devices, and internet penetration across the corners of the globe, individuals are progressively inclined towards the use of digital technologies such as cloud solutions, driving the need for cybersecurity measures for protection against cyber-attacks. There is growth in the need for endpoint and Virtual Private Network (VPN) security measures and rising demand for cyber hygiene practices to ensure robust security policies and practices amid Covid-19 pandemic [3].

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine

EMAIL: t.e.moiseenko@gmail.com (T. Moiseienko); kiva.anastassia@gmail.com (A. Kiva)
ORCID: 0000-0002-2074-8062 (T. Moiseienko); 0000-0002-6610-5898 (A. Kiva)

2. Cybersecurity Definition and Impact

Cybersecurity is part of the information security of any organization. Since the outbreak of the COVID-19 pandemic, organizations around the world have sent their employees to their home office for work. This decentralization of the organization's IT landscape has created new vulnerabilities for malicious actors to use, which is consistent with the observations of IT professionals that the number of cyberattacks is increasing after the COVID-19 pandemic. As a result, cybersecurity remains a priority among business leaders to ensure the company’s performance and data security.

There are several definitions of “cybersecurity,” but they are quite similar.

According to Glossary of Key Information Security Terms by National Institute of Standards and Technology (NIST) cybersecurity or computer security it is measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated [3].

According to Cybersecurity and Infrastructure Security Agency cybersecurity is 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 [4].

The Law of Ukraine “On Basic Principles of Ensuring Cyber Security of Ukraine” defines the following [5]:

1. Cybersecurity is the protection of vital interests of man and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace.
2. Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information, protected health information, personal information, intellectual property, data, and governmental and industry information systems.

We can resume that cybersecurity is related to criminal attacks such as unauthorized access from the inside or outside of an organization. It is the framework of protecting and securing anything that is vulnerable to hacks, attacks, or unauthorized access which mainly consists of computers, devices, networks, servers, and programs.

Cybersecurity is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. Much of this data may be confidential information, whether intellectual property, financial data, personal information or other types of data, for which unauthorized access or disclosure may have negative consequences. Organizations transmit sensitive data over networks and other devices in the course of doing business. Companies and organizations, especially those tasked with protecting information related to national security, health care or financial records, need to take steps to protect their confidential business and personnel information.

The growth in the number of computer systems and the increasing reliance upon them by individuals, businesses, industries, and governments means that there is an increasing number of systems at risk (Table 1).

Table 1
Type of industries under the cybersecurity risk

Industry at risk	Type of risk
Financial systems	The computer systems of financial regulators and financial institutions like the National Bank of Ukraine, National Commission on Securities and Stock Market, Ministry of Finance of Ukraine and Physical Deposit Guarantee Fund, investment banks, and commercial banks are prominent hacking targets for cybercriminals interested in manipulating markets and making illegal possessions. Websites and apps that accept or store credit card numbers, brokerage or intermediary accounts, and bank account information are also remarkable hacking targets, because of the potential for immediate financial gain from transferring money, shopping, or selling the information on the black market.
Utilities and industrial equipment	Computer management functions in many utilities, including coordination of telecommunications, power grids, nuclear power plants, opening and closing valves in water and gas networks.
Aviation	The aviation industry is highly dependent on a number of complex systems that can be attacked [6]. A simple power outage at one airport can have consequences around the world, much of the system relies on radio transmissions that can be disrupted, and aircraft control of the oceans is particularly dangerous because radar surveillance extends only 175-225 miles from shore. There is also the potential for an attack by an aircraft.
Consumer devices	Desktops and laptops are usually used to collect passwords or financial account information or to create a botnet to attack another target. Smartphones, tablets, smartwatches, and other mobile devices, such as quantified stand-alone devices such as activity trackers, have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers that can be used, and they can collect personal information, including sensitive health information. Wi-Fi, Bluetooth, and cell phone networks on any of these devices can be used as attack vectors, and sensors can be remotely activated after a successful violation [7].
Large corporations	Large corporations are a common goal. In many cases, attacks are aimed at obtaining financial gain by stealing personal data and involve data breaches. This could be even medical records theft or health insurance fraud.
Automobiles	Cars are becoming increasingly computerized: many models feature engine synchronization, cruise control, anti-lock brakes, seat belt pretensioners, door locks, airbags and advanced driver

	assistance systems. In addition, connected cars can use Wi-Fi and Bluetooth to communicate with on-board consumer devices and the mobile phone network. Self-driving cars are expected to be even more complex. All of these systems carry some security risk, and such issues have attracted attention [8].
Government	Government and military computer systems are commonly attacked by foreign powers. Local and regional government infrastructure, such as traffic light management, police and intelligence communications, personnel records, student records, and financial systems, are also potential targets, as they are all now largely computerized.
Energy sector	In distributed generation systems, the risk of a cyber-attack is real. An attack could cause a loss of power in a large area for a long period of time, and such an attack could have just as severe consequences as a natural disaster.

3. Cybersecurity startup investments

In the modern information age when more and more things are getting connected, cybersecurity becomes an ever-relevant topic.

The statistic shows the size of the industrial cybersecurity hardware, software, and services market worldwide, in 2017 and 2022 forecast (Fig. 1). Analyzing the cybersecurity services industry market size chart, we can summarize that it has increased steadily since 2017, reaching a value of approximately $188 billion in 2020. Despite the economic effects of the coronavirus (COVID-19), the industry is expected to increase by 11 percent in 2021.

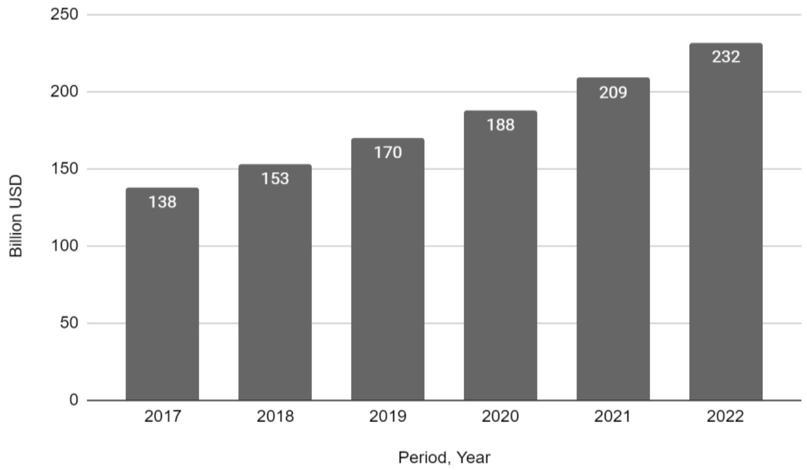

Figure 1: Size of the cybersecurity market worldwide, from 2017 to 2022 (in billion U.S. dollars) [9]

The pandemic has had a major impact on cybersecurity. Cybercrimes now cost the world nearly $600 billion each year, that’s perhaps why venture capital (VC) funding in cybersecurity more than doubled year-over-year during the first half of 2021, while the total number of mergers and acquisitions (M&A) in the sector more than quadrupled. A new report from AllegisCyber Capital, Momentum Cyber, and NightDragon finds that investors poured $11.5 billion in total VC financing in H1 2021, up from $4.7 billion in H1 2020, and that M&As jumped from $9.8 billion across 93 transactions to $39.5 billion across 163 transactions during the same period [1].

PwC and CB Insights' Q3 2020 MoneyTree report highlights the latest trends in venture capital funding globally. ICT in different forms (SW, HW, telecommunication) fully dominates the US VC industry. Monitoring and security deals grew more than double in Q3'20 (Fig. 2). According to a joint study by CBInsights and PwC, Cybersecurity startups received over $10.7 billion in funding in 2020 (Fig. 3).

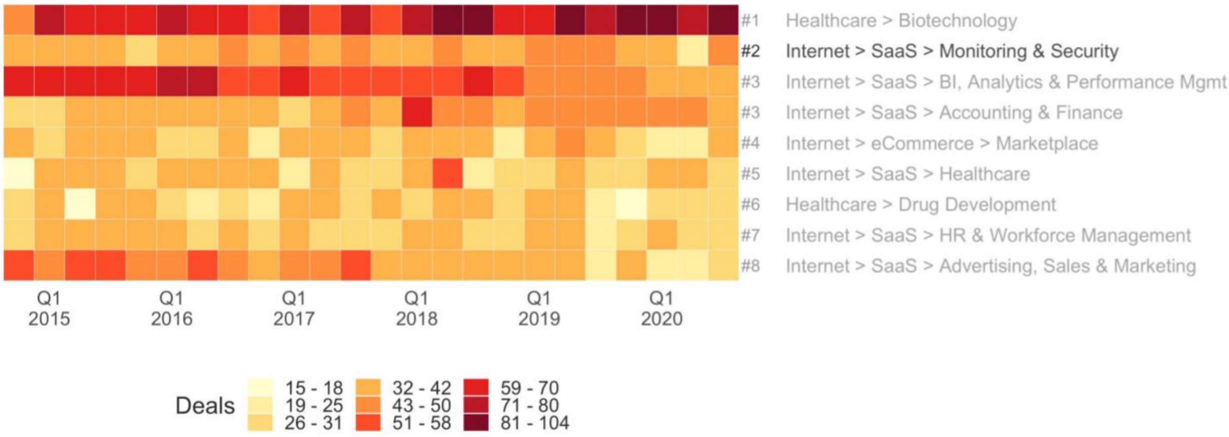

Figure 2: Top 10 US verticals by deal activity [10]

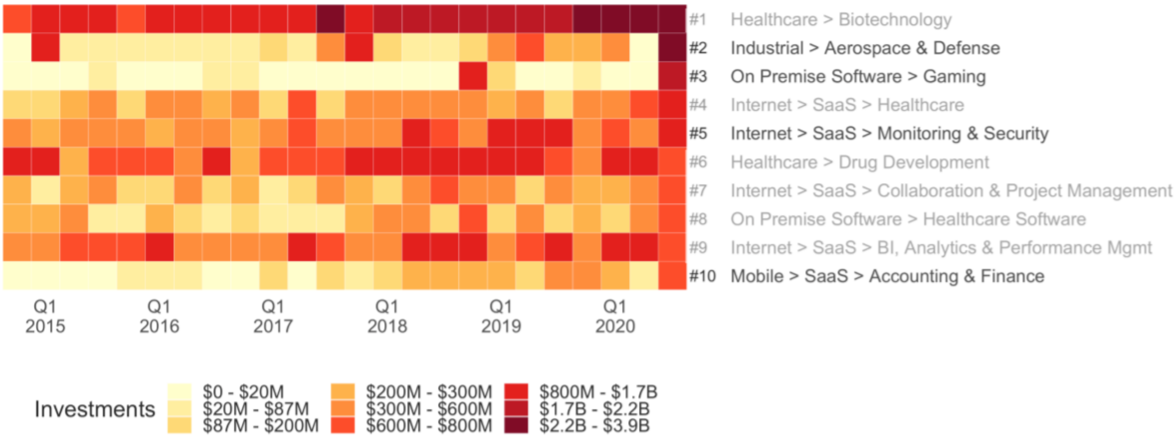

Figure 3: Top 10 US verticals by investments [10]

Overall cybercrime costs are expected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015, according to Cybersecurity Ventures. As a result, security is expected to more than double in size to $300 billion by 2025 [11].

As attack methodologies evolve due to AI, machine learning and nation-state hackers, security startups are receiving a lot of funding to develop products that can secure application access for remote workers, provide real-time visibility into cyber attacks and protect data as it travels from the cloud to IoT devices. In this article, we'll cover the top cybersecurity startups to watch in 2021 [11].

New startups and well-known suppliers are attracting record levels of investment as all organizations seek to thwart the growth of complex, costly and unpredictable cyberattacks. The Cybersecurity Ventures report estimates that the total cost of cybercrime will be $10.5 trillion by 2025. While attack methodologies continue to evolve with new technologies such as artificial intelligence, machine learning, cloud computing, etc., cybersecurity novices are also embracing them to find the exit door.

Here are the areas of cybersecurity that are currently the most promising in our opinion:

- Data protection. A data breach can cost a business million and even lead to bankruptcy. According to IBM, the average damage from data breaches is estimated at $3.62 million. And given the fact that the ingenuity of crackers and, accordingly, the frequency of hacking increases, products that solve problems in this area will be in great demand.
- Global business digitalization and privacy assurance. Whether a company uses a private server or a cloud platform to run its business, most businesses require security protocols to keep communications, data transfers, and so on, confidential. The deeper the business goes to the Internet, the more the need for cybersecurity solutions will grow.
- Working with Big Data. It is relevant both for business and for the public sector, urban infrastructure. Attacks on such systems are fraught not only with financial losses, government threats, but also with the actual paralysis of all life.
- Phishing and propaganda. The emergence and continuous development of the virtual space gives people many new opportunities—for communication, work, education and recreation. At the same time, cybercriminals have also found their niche and are successfully using it: cyber espionage, cyberattacks, propaganda of extremist ideas and movements are only part of the crimes committed using technologies, the number and variety of which is increasing every year. The creation of new methods of counteraction and combating all this is more urgent than ever, and needs an innovative approach.

The advantage of startups over industry giants is flexibility, responsiveness, and relatively modest product development budgets. Thanks to this, they have every chance to become a locomotive for the development of innovations and very highly specialized solutions, which everyone - both people and business, and even entire states—is in dire need of now.

4. Conclusion

The Covid-19 pandemic and consequent lockdowns have obliged companies to face new challenges such as smart working, remote work and digitalization, accelerating all previous efforts in that direction. As reported by Gartner, most organizations were already moving their digital agenda forward at a steady pace, but the Covid-19 pandemic required a significant leap in the development of digital products and services, with the goal of maintaining and fostering customer engagement. However, digitalization has generated many cybersecurity issues and the intensification of cyberattacks all around the world [12].

Amidst the COVID-19 pandemic crisis, various governments and regulatory authorities mandate both public and private organizations to embrace new practices for working remotely and maintaining social distancing. There is growth in the need for endpoint and Virtual Private Network (VPN) security measures and rising demand for cyber hygiene practices to ensure robust security policies and practices amid Covid-19 pandemic [3].

Cybersecurity is the protection of vital interests of man and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine’s national security in cyberspace.

Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information, protected health information, personal information, intellectual property, data, and governmental and industry information systems.

According to a research report “Cybersecurity Market with Covid-19 Impact Analysis by Component (Software, Hardware, and Services), Software (IAM, Encryption, APT, Firewall), Security Type, Deployment Mode, Organization Size, Vertical, and Region—Global Forecast to 2026” published by MarketsandMarkets, In the post-COVID-19 scenario, the global cybersecurity market size is projected to grow from USD 217.9 Billion in 2021 to $345.4 billion by 2026, recording a Compound Annual Growth Rate (CAGR) of 9.7% from 2021 to 2026. The market’s growth can be attributed to the increasing awareness and rising investments in cybersecurity infrastructure across global organizations operating across verticals.

Overall cybercrime costs are expected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015, according to Cybersecurity Ventures. As a result, security is expected to more than double in size to $300 billion by 2025 [12].

As attack methodologies evolve due to AI, machine learning and nation-state hackers, security startups are receiving a lot of funding to develop products that can secure application access for remote workers, provide real-time visibility into cyber attacks and protect data as it travels from the cloud to IoT devices. In this article, we’ll cover the top cybersecurity startups to watch in 2021 [11].

5. References

[1] K. Wiggers. Cybersecurity startup investments more than doubled in H1 2021, 2021. URL: https://venturebeat.com/2021/08/25/cybersecurity-startup-investments-more-than-doubled-in-h1-202

[2] Cybersecurity Market Overview. Markets and markets, 2021. URL: https://www.marketsandmarkets.com/PressReleases/cyber-security.asp

[3] R. Kissel, Editor. NIST. Computer Security Division Information Technology Laboratory. Glossary of Key Information Security Terms, 2019. doi: https://doi.org/10.6028/NIST.IR.7298r3

[4] CISA. What is Cybersecurity? Cybersecurity and Infrastructure Security Agency, 2019. URL: https://us-cert.cisa.gov/ncas/tips/ST04-001

[5] Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine" of October 5, 2017 № 2163-VIII, 2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[6] P. G. Neumann, Computer Security in Aviation: Vulnerabilities, Threats, and Risks, 1997. URL: http://www.csl.sri.com/neumann.html

[7] A. Shahani, Is Your Watch Or Thermostat A Spy? Cybersecurity Firms Are On It, 2014. URL: https://www.npr.org/sections/alltechconsidered/2014/08/06/338334508/is-your-watch-or-thermostat-a-spy-cyber-security-firms-are-on-it

[8] Edward J. Markey, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk, Report, 2015. URL: https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf

[9] Size of the cybersecurity market worldwide, Statista, 2021. URL: https://www.statista.com/search/?q=Size+of+the+cybersecurity+market+worldwide&Search=&qKat=search

[10] MoneyTree Report 2020 Q3, PricewaterhouseCoopers and CB Insights, 2020. URL: https://www.pwc.com/us/en/moneytree-report/assets/MoneyTree_Report_2020_Q3.pdf

[11] K. Guercio, Top 22 Cybersecurity Startups to Watch in 202, eSecurity Planet, 2021. URL: https://www.esecurityplanet.com/networks/hot-cybersecurity-startups/

[12] M. Bozzetti, L. Olivieri, F. Spoto, Cybersecurity Impacts of the Covid-19 Pandemic in Italy. ITASEC’21: Italian Conference on CyberSecurity, Italy, 2021, pp. 145-155. URL: http://ceur-ws.org/Vol-2940/paper13.pdf