

The incredible journey of cybersecurity: from military origins to a recession-proof business opportunity

Nabil Suleiman

Rovato (BS) Italy

ORCID Details

Nabil Suleiman: <https://orcid.org/0009-0005-0446-822X>

Abstract - Since the first network was created in 1969 by the Defense Advanced Research Projects Agency, for both the Military MILnet and the civil ARPAnet, the purpose was to give remote access, at the time the risk of cyber breaches was not taken into consideration.

This research analyzes the risk, giving birth to the need or demand for security, making cybersecurity a market product or service aimed to satisfy that demand.

As the use of the internet has been growing to the level of involving any business activity, is a must to protect this business from unwanted risks.

Keywords: Cybersecurity, cyber threat, cyber security business, growing business reality, fear, demand, hackers attack, new business risks, emerging businesses, recession proof businesses.

1. Introduction

According to estimates, the loss resulting from cybercrime will reach about 10 trillion USD by the year 2025. Every 39 seconds there is a new cyber-attack in some corner of the world. Companies of all types, being small or medium-size enterprises, are increasingly becoming victims of cyber-crime (Morgan, 2026).

When threats arise, opportunities come as well. Cybersecurity has become a future-oriented investment: a strong demand, dynamic progress and high profitability make it attractive to both investors and specialists in this field.

Market Statistics

	Metric	Value
year	Startup cost	\$5,000 – \$50,000
	Estimated market growth	~13% per
	Expected revenue (2026)	\$298
billion	Market size (2023)	~ \$223 billion
	Total market size (2030)	~ \$500 billion
job openings	Labor gap	3.5 million

Source: Statista (2025), ISC (2025)

Average Pricing Models

\$15,000/month	Monthly retainer	\$3,000-
\$25,000 post sale	Project fee	\$8,000 –
\$400/hour	Hourly rate	\$150 –

Source: Articsledge (2026)

Definitions

Cybersecurity can be defined as people, processes and technology aimed at protecting networks and data from attacks and unauthorized access (Microsoft, 2026).

Cybersecurity firms are companies that work to secure their clients from espionage, attacks, data loss and ransomware attacks (Articsledge, 2026).

2. Historical Context: The Deficit of Internet Security

Quote: "The internet wasn't built for security" R. Van Kranenburg

History

Year 1969

The first network was created by DARPA both for military needs (MILnet) and civilians (ARPAnet). The original intention of this network was to provide accessibility with no regard to security.

Main Events

1971: The first email is sent by Ray Tomlinson

1973: TCP/IP is created (TCP ensures reliable delivery and IP is used for identifying the destination of packets)

1986: NSF establishes the first internet backbone.

1990: NREN makes improvements in connection for universities and research institutions

90s-2000s: Internet becomes widely used by ordinary users, appears IRC, Napster, user-friendly torrent downloaders, VPN, instant messengers

Early 2000's: The Birth of Cybersecurity as a professional figure and a business.

With the birth of cybersecurity, this science tried to fill the gaps of the vulnerabilities that were exposed by early hackers like Kevin Mitnick, until the more recent ones. After the terrorist acts of September 11, the governments took actions to prevent dangerous usage of the internet, rules like the following were implemented providing cybersecurity protection:

- a. UK Anti-terrorism, Crime and Security Act (2001)
- b. New EU privacy legislation (2005)
- c. GDPR (2008) the European general data protection regulation

3. Threats

3.1 Cyberexperience Attacks

Cryptoviral blackmail which may entail either revealing or locking down the data without the payment of ransom. Cyberexperiences increased by 36% in 2018, with more than 100 new malware families being released.

3.2 AI Growth

Companies are believed to spend \$2.5 billion on AI cybersecurity bots (2016-2025). The advantages of AI systems include the efficiency of work performed and 24/7 operation but lead to thieves taking jobs from human professionals.

3.3 IoT Threats

Over 12.5 billion devices were connected in 2010, and the number of connected devices on the planet reached 25 billion by 2015 (Cisco). Overall, approximately 70% of IoT devices are already vulnerable.

3.4 Blockchain Era

Cryptocurrencies - that affect borderless transactions— used also in cybercrime and money laundering actions.

3.5 Serverless Applications (FaaS).

Offering automatic scaling and no administration, serverless architecture shifts security responsibilities onto the consumer, with potential vulnerabilities.

3.6 Mobile App Permissions

Crucial permissions such as GPS, network state, SMS, camera, and microphone may become potentially hazardous for the user since they can be used by malevolent applications to

steal data, with the option to track users or send paid SMS messages.

3.7 Physical Threats

- a. Not secure password storage
- b. Weak passwords used or repeated password usage
- c. Connecting to unsecured public Wi-Fi
- d. Failing to change passwords frequently

3.8 Personal and Psychological Threats

Long-term engagement in cybersecurity could cause:

- a. Difficulty in disconnecting from the cyber environment
- b. Thinking in patterns (true/false, if/then) which impedes real-life relationship
- c. 'Programmer syndrome' – avoiding interpersonal ties

4. Discussion: CyberSecurity as Business

The essence of business is matching supply and demand. The need for privacy opens the field for products/services – whether tangible (hardware) or intangible (consulting, monitoring, incident response).

Healing versus Prevention

Cybersecurity is not only about firewalls and antivirus but proves to be a whole-system discipline:

Identifying possible damaged channels

Blocking possible actions that may lead to damage

Building secure-by-design systems, which makes it relevant for any industry; manufacturing, healthcare, finance, education.

5. Findings

Risk, as fear in general, creates a need for protection and major security, accordingly, cybercrimes fear is a factor of the market demand for the cybersecurity market.

Cybersecurity is not only about protection against data losing but it also means protecting trust, continuity, and progress in an ever-developing world.

In the design of the internet security was not a main priority but accessibility was a discrepancy we are still trying to fix.

If the fifth-generation (5G) networks are designed correctly, they can create an opportunity for integrating security by design.

The professionals in cybersecurity are experiencing some specific challenges like the necessity to be continuously alert and the necessity to switch off.

There is a shortage of 3.5 Million cybersecurity specialists, this gap can be filled with AI but AI cannot completely replace humans.

However, despite all the difficulties, cybersecurity is one of the most growing industries.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

The author would like to express his sincere gratitude to all professors and university institutions who contributed directly or indirectly to the successful completion of this research. I extend my appreciation to my professors and mentors at the Arab Open University (Kuwait branch) for their insightful discussions, valuable feedback, and continuous encouragement throughout past studies, this one and the future papers.

Funding Source

The authors declare that no financial support or funding was received for this research, underlining the absences of financial interests that could affect this work.

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

Statement of ethical approval

The author confirm that procedures followed the 1964 Helsinki Declaration and its later amendments, or comparable ethical standards.

Reference List:

1. Morgan, S. (2026). *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*. [Online]. *cybersecurityventures.com*. Available at: <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/> [Accessed 19 August 2026].
2. *Articledge.com*. (2026). *Cybersecurity Business: How to Start, Scale, and Profit in 2026*. [Online]. *Articledge*. Last Updated: 20 March 2026. Available at: <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/> [Accessed 19 August 2026].
3. Statista. (2024). *Cybersecurity: market data & analysis*. Statista. (Report), pp.1-82. [Online]. Available at: *Cybersecurity: market data & analysis* [Accessed 19 August 2026].
4. Baran, P. (2011) "Paul Baran and the Origins of the Internet". RAND corporation. Retrieved 29 March 2011.
5. Cerf, Vinton G. & Cain, Edward (1983), "The DoD Internet Architecture Model", *Computer Networks*, 7, North-Holland, pp. 307–318, CiteSeerX 10.1.1.88.7505
6. G. Schneider; J. Evans; K. Pinard (2009). *The Internet – Illustrated*. Cengage Learning. ISBN 0538750987. Retrieved 2015-08-15.
7. Heart, Frank; Kahn, Robert; Ornstein, Severo; Crowther, William; Walden, David (1970). "The Interface Message Processor for the ARPA Computer Network" (PDF). *AFIPS Proc.* 36: 565. doi:10.1145/1476936.1477021
8. Ronda Hauben. "From the ARPANET to the Internet". *TCP Digest (UUCP)*. Retrieved 2007-07-05.
9. Jon Postel Editor, ed. (September 1981). *Internet Protocol DARPA Internet Program Protocol Specification*. p. 23. doi:10.17487/RFC0791. RFC 791
10. M. Kozierok, C. (2005). *The TCP/IP Guide - TCP/IP Overview and History*. [online] *Tcpipguide.com*. Available at: http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm [Accessed 17 Mar. 2019].
11. Peter, I. (2004). *The history of email*. [online] *Nethistory.info*. Available at: <http://www.nethistory.info/History%20of%20the%20Internet/email.html> [Accessed 17 Mar. 2019].
12. P. Bishop, A. (1991). *The National Research and Education Network (NREN): Update 1991*. ERIC Digest.. [online] *Ericdigests.org*. Available at: <https://www.ericdigests.org/1992-4/nren.htm> [Accessed 17 Mar. 2019].
13. *EaPConnect* (2019). *What is an NREN? - EaP Connect*. [online] *EaP Connect*. Available at: <https://www.eapconnect.eu/about-eap/what-is-an-nren/> [Accessed 17 Mar. 2019].
14. Kyung Hee University (2019). *History of Internet*. [online] *Slideplayer.com*. Available at: <https://slideplayer.com/slide/12506369/74/images/2/1+History+of+Internet+Internet+%28not+internet%29.jpg>. Slide 2 [Accessed 17 Mar. 2019].
15. Kyung Hee University (2019). *History of Internet*. [online] *Slideplayer.com*. Available at: <https://slideplayer.com/slide/12506369/74/images/3/Internet+Today+Four-node+ARPANET+established.jpg>. Slide 3 [Accessed 17 Mar. 2019].
16. Blumenthal, A. (2012). *brief_internet_history*. [online] *wordpress.com*. Available at: https://andyblumenthal.files.wordpress.com/2012/04/brief_internet_history.png [Accessed 17 Mar. 2019].

17. Hales, R. (1998). *What is the WWW?*. [online] Uky.edu. Available at: <http://www.uky.edu/~halesr/eds643f98/WWWMSTR/> [Accessed 17 Mar. 2019].
18. Minnie (2014). *What Is the Internet?*. [online] SlideServe. Available at: <https://www.slideserve.com/minnie/what-is-the-internet> [Accessed 17 Mar. 2019].
19. Microsoft (2026) *What is cybersecurity? Key Concepts explained: Microsoft security, Microsoft*. Available at: <https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity> (Accessed: 20 August 2026).
20. Young, A.; M. Yung (1996). *Cryptovirology: extortion-based security threats and countermeasures*. IEEE Symposium on Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676. ISBN 0-8186-7417-2.
21. Andy Greenberg (20 April 2011). "Crypto Currency". *Forbes.com*. Archived from the original on 31 August 2014. Retrieved 8 August 2014.
22. Mason, J. (2018). *5 Cybersecurity Challenges and Trends: What to Expect in 2018*. [online] Globalsign.com. Available at: <https://www.globalsign.com/en/blog/cybersecurity-trends-and-challenges-2018/> [Accessed 17 Mar. 2019].
23. TrendMicro (2019). *12 Most Abused Android App Permissions*. [online] About-threats.trendmicro.com. Available at: <http://about-threats.trendmicro.com/us/library/image-gallery/12-most-abused-android-app-permissions> [Accessed 17 Mar. 2019].
24. Thomas, I. (2018). *Top 10 Security Risks in Serverless Architectures - DZone Security*. [online] dzone.com. Available at: <https://dzone.com/articles/top-10-security-risks-in-serverless> [Accessed 17 Mar. 2019].
25. Geer, D. (2015). *The Internet of Things: Top five threats to IoT devices*. [online] CSO Online. Available at: <https://www.csoonline.com/article/2134265/the-internet-of-things--top-five-threats-to-iot-devices.html> [Accessed 17 Mar. 2019].