

Lapis Global Cyber Security 25 Index



Cyber Security is Indispensable in a Digital World

Introduction

The **digitization** of the **economy and society** has progressed steadily since the invention of the Internet in the 1990s. Many people in industrialized countries and increasingly in developing countries **spend several hours** a day in front of a PC, tablet, or smartphone for private and professional reasons. Access to the digital world is **possible everywhere** in an easy way. Life without the **Internet and smartphones** has become almost unthinkable. The **commercialization of the data trail** of various applications used by users has taken place long ago. As a result, this **data** is referred to as the new gold. However, the question inevitably arises with increased digitalization as to **how secure the sensitive data** from the private and professional environment is **protected against cyber-attacks**.

Cyber-attacks, also referred to as cybercrime include, for example, the following criminal activities:

- **Phishing attacks:** Fraudulent attempts made to impersonate a trustworthy communication partner via fake websites, e-mails, or text messages to obtain personal data such as passwords.
- **Denial of service attacks:** An extensive number of requests and messages deliberately used to overload a website or server to extort ransom money or cause wanton damage.
- **Malware:** a malicious software that infiltrates computer systems to cause disruption or damage. Examples include ransomware, worms, Trojans, and spyware. **Ransomware** denies access to one's device or files until ransom demands are paid. A **worm** is a program that replicates itself and spreads to as many computers as possible via a network. Unlike a **virus**, a worm is transmitted without the intervention of a person. A **Trojan** is a program that is disguised as a useful application and performs other functions in the background without the user's knowledge. With **spyware**, information is collected without the user's knowledge to allow the attacker remote access to a certain system.

The goal of digitization is to **simplify our everyday lives**. The obverse side of the coin is the **increasing risk of falling victim to cyber-attacks** with people and businesses losing sensitive information, money, or reputation. For this reason, cyber security has recently become a **major topic**. Those companies that have successfully positioned themselves in this sector will benefit hugely from the **increasing need for cyber security**.

Cyber Security Market

Cyber-attacks pose a real **threat to individuals and businesses**. It is estimated that the consequences of cybercrime will result in **USD 6 trillion damages worldwide in 2021**. Looking ahead, experts predict that these damages will increase at an annual **growth rate of 15%** amounting to **USD 10.5 trillion by 2025**. This would be one of the largest transfers of economic wealth in history. **Cybercrime costs** include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. Cyber-attacks can affect not only private individuals and companies, but also **critical infrastructures** such as **power plants, hospitals, and financial service providers**. The security of these and other institutions is essential for the smooth functioning of our economy and society.

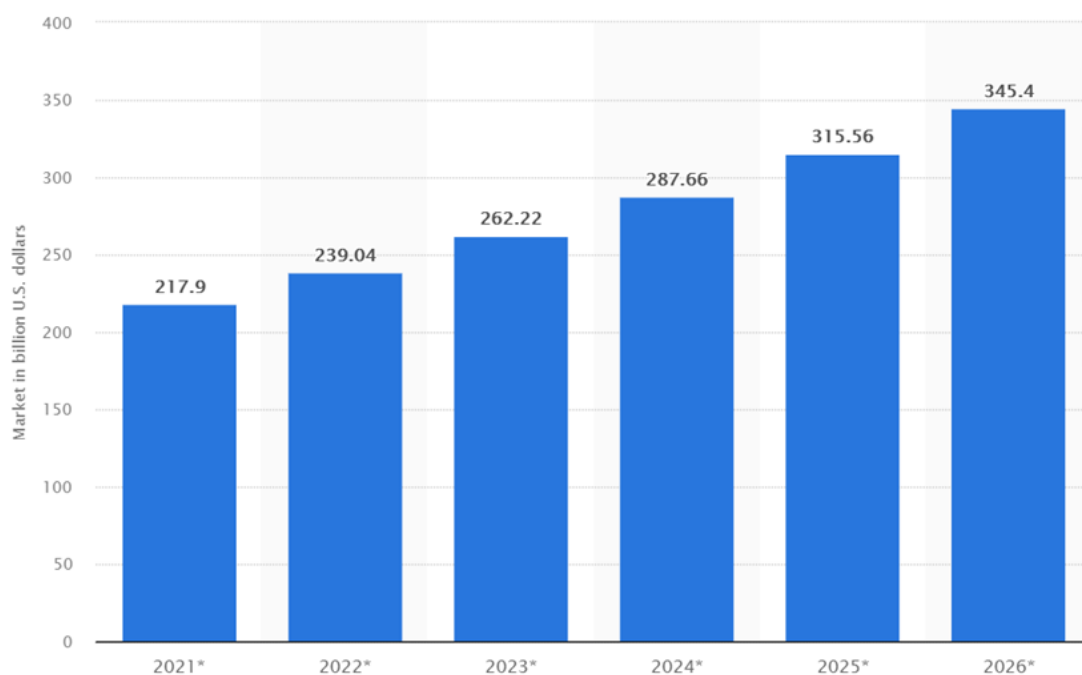
One of the **biggest challenges** is ensuring that cyber security keeps pace with or outclasses the **constant evolution of cybercrime**. Every new technology brings with it the risk opportunity of a **new attack**. As a result, individuals and businesses are effectively **forced to continually adapt their practices to protect their IT systems**. The following table compares

global end-user spending (in USD millions) in **2020 and 2021** and reveals the **high growth rates** reported in **all market segments**.

| Market Segment | 2020 | 2021 | Growth (%) |
|-------------------------------------|----------------|----------------|-------------------|
| Application Security | 3,333 | 3,738 | 12.2 |
| Cloud Security | 595 | 841 | 41.2 |
| Data Security | 2,981 | 3,505 | 17.5 |
| Identity Access Management | 12,036 | 13,917 | 15.6 |
| Infrastructure Protection | 20,462 | 23,903 | 16.8 |
| Integrated Risk Management | 4,859 | 5,473 | 12.6 |
| Network Security Equipment | 15,626 | 17,020 | 8.9 |
| Other Information Security Software | 2,306 | 2,527 | 9.6 |
| Security Services | 65,070 | 72,497 | 11.4 |
| Consumer Security Software | 6,507 | 6,990 | 7.4 |
| Total | 133,776 | 150,409 | 12.4 |

Source: Gartner (May 2021)

The increased spending on cyber security is commensurate with the growth of revenues of companies in the cyber security industry. The following chart **forecasts the size of revenues in the global cyber security market until 2026** (source: Statista):



These **promising revenue growth rates** indicate that the cyber security market would be appealing to long-term equity investors. **Digitization is irreversible**, as are the **associated cyber risks** and the **need for protective counter measures**.

Lapis Global Cyber Security 25 Index

The **Lapis Global Cyber Security 25 Index** is composed of **25 worldwide best-known and leading cyber security companies**. The advancement of technology has left many people and businesses vulnerable to cybercriminal activities such as hacking, data theft and damage, as well as industrial espionage. All companies in our **equally weighted index** have a **market capitalization greater than USD 2.5 billion** and **30 %** of these have paid **uninterrupted and continuously increasing dividends** over the last 3 years. A maximum of **70 %** of the companies included in our unique equity index do not apply a strict dividend payment policy and have paid their regular dividends for less than 3 years. Our **rule-based criteria** for selecting the **most promising companies** is applied during the **quarterly rebalancing process** (end of March, June, September, and December).

We offer our existing customers and prospects the following access to our unique **Lapis Global Cyber Security 25 Index expertise**:

- **Discretionary Mandates and Advisory** based on the Lapis Indices
- **Lapis Index – based Investment Solutions**

We would welcome the opportunity to explain the advantages of our unique equity indices in a **personal advisory meeting** to determine a **long-term and optimal investment strategy** that matches with your risk profile and that is able to **meet your investment goals**. Additional information on the performance and relevant **financial ratios** of our equity indices will be provided upon request. For further information please visit our website: **www.lapis.finance**.

Sincerely,

Andreas Wueger
CEO

Disclaimer

The information provided in this document constitutes marketing material.

The document has been prepared for information purposes only and does not constitute an offer, investment recommendation, personal advice, or solicitation to purchase financial instruments and does not offer or promote any form of investment. This document does not constitute investment advice on financial instruments and therefore the information made available in this document should not be construed as a recommendation or invitation to invest.

The presentation has been prepared with the utmost care and attention; however, errors cannot be excluded. LAPIS Asset Management SA excludes any liability that may result from incorrect or outdated information.

The information, estimates and projections contained in this document are necessarily based on current market conditions, which may change significantly in the short term. Therefore, changes and events occurring after the date of the document could affect the validity of the conclusions contained in the document. LAPIS Asset Management SA assumes no obligation to update and/or revise the document or the information and data on which it is based.

For further information in relations to financial instruments reported in the present document/mail please refer to the official product documentation.