CYBER SECURITY: A MUST FOR YOUR PORTFOLIO?

From risk to opportunity

- Allianz Cyber Security ("The Fund") aims at long-term capital growth by investing in equities in the global equity markets with a focus on companies whose business will benefit from or is currently related to cyber security in accordance with environmental and social characteristics. With the adoption of the Sustainability Key Performance Indicator Strategy (Relative) ("KPI Strategy (Relative)"), the Fund aims to achieve the reduction in greenhouse gas emissions ("GHG") of the Fund's portfolio which shall be at least 20% lower than that of its benchmark index within the same period ("Sustainability KPI").
- The Fund is exposed to significant risks relating to investment/general market, concentration, cyber security, emerging market, company specific, currency (such as exchange controls, in particular RMB), and the adverse impact on RMB share classes due to currency depreciation.
- The Fund is exposed to sustainable investment risks relating to KPI Strategy (Relative) (such as foregoing opportunities to buy certain securities when it might otherwise be advantageous to do so, and/or selling securities when it might be disadvantageous to do so or relying on information and data from third party ESG research data providers and internal analyses which may be subjective, incomplete, inaccurate or unavailable). The Fund focuses on the Sustainability KPI which may reduce risk diversifications and may be more volatile compared to broadly based funds. Also, the Fund may be particularly focusing on the GHG emission efficiency of the investee companies rather than their financial performance which may have an adverse impact on the Fund's performance.
- The Fund may invest in financial derivative instruments ("FDI") which may expose to higher leverage, counterparty, liquidity, valuation, volatility, market and over the counter transaction risks. The Fund's net derivative exposure may be up to 50% of the Fund's net asset value.
- This investment may involve risks that could result in loss of part or entire amount of investors' investment.
- In making investment decisions, investors should not rely solely on this material.

Note: Dividend payments may, at the sole discretion of the Investment Manager, be made out of the Fund's capital or effectively out of the Fund's capital which represents a return or withdrawal of part of the amount investors originally invested and/or capital gains attributable to the original investment. This may result in an immediate decrease in the NAV per share and the capital of the Fund available for investment in the future and capital growth may be reduced, in particular for hedged share classes for which the distribution amount and NAV of any hedged share classes (HSC) may be adversely affected by differences in the interests rates of the reference currency of the HSC and the base currency of the Fund.

In the time it takes you to read this sentence (about four seconds), cyber criminals will have carried out around 27,780 attacks. There are almost 7000 attacks per second worldwide, happening 24 hours a day, 365 days a year. The good news?

This situation presents an investment opportunity

Twenty years ago it was possible to avoid the Internet if you wanted to, something that is inconceivable today. We meet online, manage our finances via an app, store photos in the cloud and control thermostats remotely. This digital connectivity makes our lives easy and efficient, but we are also more vulnerable than ever. Not only in our personal lives, but also at work. According to a report from Microsoft, there are no fewer than 600 million cyber attacks worldwide every day[1].

It is therefore no coincidence that the Allianz Risk Barometer 2025[2] has named cyber incidents as the most important global business risk for the third successive year. The potential damage is not only financial – there is also a risk of reputational damage, legal liability, production downtime and even compromised national security.

> Some 20 billion devices are now connected to the Internet, and the figure is still growing exponentially

1) Source: **news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe/**
2) Source: **commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf**

From the railway to supermarkets

Hospitals, water treatment plants, public services, steel plants, car manufacturers, railway operators ... no sector is safe from the growing prevalence of cyber crime.
In Q2 this year, a cyber attack cost the UK Retailer M&S an estimated GBP 300 million, almost a third of its total annual profits. The attack forced the company to resort to pen and paper, among other measures, because its automated stock systems were crippled.

As cyber crime grows, so too does cyber security

As the threats increase, the cyber security sector is booming like never before. According to McKinsey, around USD 200 billion was spent worldwide in 2024 on products and services to protect digital networks[3]. The figure has been increasing for a number of years now, and that doesn't look like changing any time soon, with McKinsey anticipating annual growth of some 12% over the coming years.

Various developments reinforce this trend

- **Digitalisation and connectivity:** Society is increasingly online. Smart devices in our homes, driver assistance technology in our cars, cloud services and mobile networks connect everything and everyone. Some 20 billion devices are now connected to the Internet, and the figure is still growing exponentially[4]. Every connected device can be a gateway to cyber criminals, from a simple printer to a sophisticated industrial robot.

- **Geopolitical tensions:** The tensions playing out between countries are increasingly moving to the cyber space environment. Last year in Belgium, the FOD Economie website and, notably, the website of the Centre for Cybersecurity were crippled by an attack believed to stem from a Russian group. Attacks and espionage cost money every day, making cyber security a strategic priority for countries and businesses. This digital warfare often goes beyond just taking a website offline, with targeted attacks on critical infrastructure and intellectual property.

- **Advent of new technology:** AI and automation are changing the playing field. While cyber criminals use AI to carry out even more sophisticated attacks (e.g. deep-fake phishing or automated ransomware), security companies are using it to automate repetitive tasks. Employees are also increasingly being trained to cope with more complex and costly cyber threats.

- **Regulatory and compliance:** Governments are imposing increasingly stringent regulations, such as privacy laws and guidelines that obligate organisations to report vulnerabilities and implement robust security measures. These

FIVE LINES OF DEFENCE

1. **Perimeter security**
   Firewalls, threat detection and access control
2. **Network security**
   Protection of internal data traffic
3. **Endpoint security**
   Protection of devices such as laptops, smartphones or sensors
4. **Application security**
   Protection of apps and their underlying code
5. **Data security**
   Encryption, access control and detection of unauthorised access

3)Source:**https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer**
4) Source: **iot-analytics.com/number-connected-iot-devices/**

rules are forcing organisations, ranging from financial institutions to public utilities, to invest millions in digital security every year.

This mix of digitalisation, the geopolitical situation, technological revolution and regulatory frameworks means there is a constant structural demand for cyber security. Companies and organisations must constantly create new lines of defence. This makes cyber security a self-reinforcing growth market: The challenges are increasing, the solutions are becoming more complex, and investment is rising accordingly.

Allianz Cyber Security

Allianz Cyber Security is adapting to this evolution with a global portfolio of 30 to 60 carefully selected companies operating in all spheres of cyber security. The emphasis is on pure plays – companies for whom cyber security is not a secondary activity, but a high priority. The selection process is based on a dedicated, clearly defined universe of more than 200 listed companies. Only companies that are found to be sufficiently relevant or even as "pure" players after thorough examination are considered.

The portfolio contains a mix of promising growth stocks and established stocks, with a preference for mid-sized companies with a strong technological edge. The portfolio is managed by Voya IM as the delegated administrator – based in San Francisco near Silicon Valley. With more than 20 years of experience, the team has built up a unique level of expertise with cyber security stocks and has one of the longest track records in the sector.

Agentic AI

"One of the developments we are following closely is the emergence of agentic AI. This is the new generation of AI that can make independent decisions and manage complex workflows", says Fund Manager Erik Swords. "The technology provides huge efficiency gains for businesses but does also increase the complexity of security. AI agents use real-time data, connect systems independently, and work with minimal human intervention. Cyber security is crucial here, because any weak link can be a target. We believe that the importance of identity management, among other things, will increase as a result, and this is reflected in our positioning within the Fund."

Although the mix of digitalisation, the geopolitical situation, technological revolution and regulatory frameworks means there is a constant structural demand for cyber security, it goes without saying that this topic is not evolving in a straight line upwards on the market; losses are possible and the potential of other opportunities can be overlooked by focusing solely on this topic.