Note: Below are extracts from an article published by First Trust (02nd March 2023) and as referenced below.

CYBERSECURITY: Another day, another threat vector.

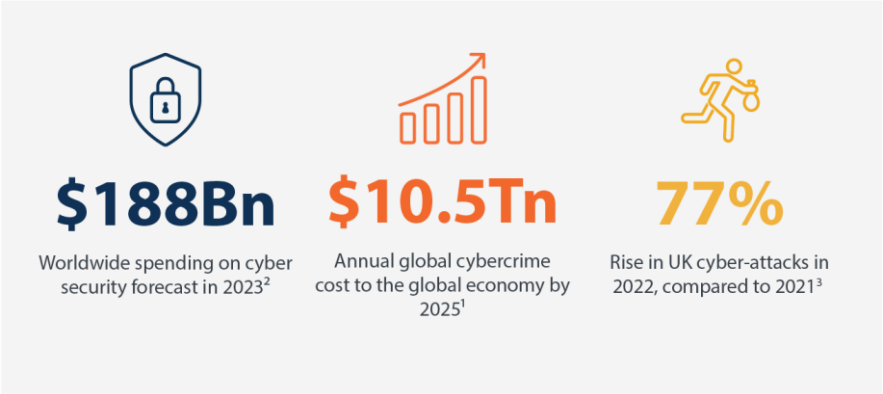
First Trust (2023) outlines for the professional investor the current landscape regarding cyber attack and its impact on business both financially, reputationally and in its day-to-day operation. The comparison is now being made between cybercrime and natural disasters such are its devastating consequences for the world's economy:

> The cybersecurity landscape is shifting. Cyber risks are taking on new meaning for businesses not only technologically, but also financially, reputationally, and operationally. As essential services become more reliant on digital control systems, cyber-attacks may soon be economically comparable to natural disasters. Cybercrime is expected to cost the global economy $10.5 trillion per year by 2025, up from $3 trillion in 2015[1].
> Cyber-attackers quickly adapted to changes in the political, technological, and regulatory landscapes in 2022. Attacks on critical infrastructure, supply chains, and cloud-based enterprises became increasingly high-profile. The divide between private and public sector attacks appears to have closed completely, with cyber criminals targeting critical infrastructure such as power grids, water systems, hospitals, and transportation networks, causing widespread disruption. Companies at the forefront of cyber-defence, on the other hand, are fighting back.
> (FIRST TRUST 2023)

According to First Trust (2023) , as cybercrime becomes increasingly sophisticated, so too the firms responsible for protecting and safe-guarding our privacy and data must develop sophisticated products and techniques to counteract it. The coming year will see increased investment in cyber- security by CEOs worldwide and heightened regulation globally :

> The nature of cybercrime is becoming increasingly unpredictable as digital surface areas continue to grow, but innovation is broadening. With cyber attackers accelerating their levels of sophistication, so too must the cyber firms responsible for safeguarding our privacy and data.
> As cyber threats proliferate, organisations and governments will focus on strengthening their defences. Following President Biden's "Cyber Incident Reporting for Critical Infrastructure Act" and the European Union's proposed cyber hygiene rules, we may see additional regulations globally with new rules aimed at increasing transparency in cybersecurity disclosures. CEOs continue to see cybersecurity as a necessity as companies prepare for a widely anticipated recession in 2023. The utility-like qualities of cybersecurity are expected to translate into $188bn in spending per calendar year[2]. Below, we look at some of the key trends for the cybersecurity industry.
> (FIRST TRUST 2023)

Global statistics as presented to us in this infographic by First Trust(2023), outline how spend on cyber security, costs incurred as a result of cyber crime and the number of attacks are all on the rise:



(FIRST TRUST 2023)

The key future trends as envisaged by First Trust(2023) are outlined in some detail below, with the top 10 trends described as follows:

1. **Utilities of the Digital Age -** AI, cybersecurity, and cloud computing have become the utilities of the digital age. These technologies are interconnected and necessary for businesses to thrive, assisting leaders in reimagining the traditional business models on which they have built their success and enabling new ways to leverage their vast amounts of data for future growth.

2. **Cloud Security -** Businesses have been compelled to invest in cloud solutions by the more recent hybrid working paradigm. As more companies move their operations to the cloud, there will be a greater need for robust security measures to protect sensitive data and systems. Gartner predicts organisations will spend nearly $6.7 billion on cloud security in 2023.

3. **Good vs Bad AI -** Artificial Intelligence has the potential to significantly impact a host of businesses, particularly cybersecurity. Broadly, AI for good can augment cybersecurity safeguards and help fill gaps in the workforce, while bad AI could launch automated sophisticated cyberattacks. Interestingly, those companies which have integrated AI into their cybersecurity efforts save an estimated $3 million.

4. **Expanding IoT Attack Surface -** With over 29 billion IoT devices globally by 2030, the attack surface is rapidly expanding. A set of cybersecurity labelling requirements has been requested by the White House National Security Council to safeguard consumer electronics. The issue; IoT devices fresh out of the box and packed with useful features are introduced without any consideration for their internet security.

5. **Better Cyber-hygiene -** From hesitating on opening email attachments to being more cautious as to which apps we let track our movements, our cyber hygiene is getting better. 72% of us are now unwilling to install apps which are perceived as collecting too much data. We expect that consumer spend could follow here as the number of connected devices increases.

6. **Ransomware-as-a-service (RaaS) -** In the face of a possible recession, hacking for hire is an illicit but potentially highly- profitable business model. During 2022, cyberattacks targeting critical infrastructure jumped from comprising 20% of all nation-state attacks detected to 40%. These "guns for hire" are targeting private companies. The famous Colonial Pipeline attack had 100GB of data stolen from their network, and allegedly paid almost $5million to a RaaS business, DarkSide.

7. **Targeting Critical Infrastructure -** Critical infrastructure is becoming increasingly complex and dependent on networks of interconnected devices. Critical infrastructure used to operate in isolation for decades. Now, the failure of one could cause a devastating chain reaction. Russia's invasion of Ukraine was preceded by a cyber-attack on infrastructure, revealing a new frontier. Several high-profile attacks have occurred globally with the social consequences outweighing the financial ones.

8. **Zero Trust -** Historically, IT policies were based on the assumption that if an email originated from within a company, it was safe. Zero trust is founded on the principle of strict access controls and not trusting anyone by default, including those already inside the network. According to EMR, Zero Trust will be the fastest growing network segment globally, with a market value expected to rise from $22 billion in 2021 to $60 billion by 2027.

9. **Blockchain to the rescue? -** Blockchain provides a different path to greater security, one that is less travelled and less inviting to cybercriminals. This method reduces vulnerabilities, provides strong encryption, and verifies data ownership and integrity more effectively. As the threat level rises, blockchain technology is laying the groundwork for improved innovation to meet the threat. We believe this an area to watch.

10. **Quantum Resilience** - Quantum resilience is no longer the stuff of science fiction. It may eventually improve cybersecurity by solving problems that are impossible to solve with traditional computers. Quantum is already assisting in the protection of our data, whether via satellite or network. With 2.5 quintillion bytes of data generated every day and a higher potency of cyberattacks expected, quantum resilience assistance may be timely.

(FIRST TRUST 2023)

In conclusion, First Trust(2023) emphasizes its belief that cyber security is here to stay and that the trends described in this outlook are likely to continue to grow and develop:

> The digital surface area has significantly increased due to the rapid development of technology and the growing reliance on digital platforms and devices. Subsequently, this has increased the number of ways that cybercriminals might launch attacks, but it has also created new avenues for innovation and security measures. Threats change as does technology, therefore it's crucial for enterprises and governments to regularly evaluate and strengthen their security position to stay ahead of the ever-evolving threat landscape. The on-going arms race between cybersecurity experts and hackers is likely to last forever.
> Providers across the entire security spectrum could potentially continue to benefit from corresponding investment. This should allow those companies to further develop vital, cutting edge solutions and likely propel them to further growth.
>
> We believe that cybersecurity is a megatrend which is here to stay.
>
> (FIRST TRUST 2023)

References

First Trust (2023) *Another day, another threat vector. The key trends defining the future of cybersecurity.* Available at: https://info.ftgportfolios.com/Cyber-Security-Outlook-Download-2023.html# (Accessed 24 March 2023).

First Trust

IMPORTANT INFORMATION

This financial promotion is issued by First Trust Global Portfolios Management Limited ("FTGPM") of Fitzwilliam Hall, Fitzwilliam Place, Dublin 2, D02 T292. FTGPM is authorised and regulated by the Central Bank of Ireland ("CBI") (C185737). This report was produced in conjunction with Brian Comiskey of the Consumer Technology Association and Efram Slen of Nasdaq.

Nothing contained herein constitutes investment, legal, tax or other advice and it is not to be solely relied on in making an investment or other decision, nor does the document implicitly or explicitly recommend or suggest an investment strategy, reach conclusions in relation to an investment strategy for the reader, or provide any opinions as to the present or future value or price of any fund. It is not an invitation, offer, or solicitation to engage in any investment activity, including making an investment in a Fund, nor does the information, recommendations or opinions expressed herein constitute an offer for sale of a Fund.