Allianz Global Investors

APRIL 2024 | DOUBLE CLICK

A sustainable digital future

The digital age has revolutionized the way that we interact with each other, making it easier than ever to share and store information. Unfortunately, this digital world is becoming increasingly vulnerable to bad actors, from identity theft to malicious hacking. Cybersecurity has thus become a vital tool in protecting our computers, networks, programmes, and data from unauthorized access or attacks, helping safeguard individuals and businesses from these new challenges.

Cybersecurity is a pressing issue in the modern world. The FBI Internet Crime Complaint Center (IC3) reported a 300% rise in cybercrimes in the past two years.[1] Cybercriminals are continually devising new methods to exploit weaknesses in online commerce and vital infrastructure, including identity theft, ransomware, and targeted cyberterrorism attacks on key infrastructure across sectors. Identity theft and phishing, ransomware, and targeted cyberterrorism attacks on critical infrastructure in the energy, healthcare, financial, and manufacturing industries are all examples of malicious actors finding new ways to exploit vulnerabilities. The increasing prevalence of cybercrime has resulted in billions of dollars of losses for individuals and organizations globally and reputational damage. For instance, Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent annually over the next five years, reaching $10.5 trillion annually by 2025.[2]

Giles Money
CIO, Global Sustainable Equity

Alex Bibani
Senior Portfolio Manager

For instance, UnitedHealth Group's communication and PR strategy during the recent hack of its Change Healthcare unit show the difficulties of balancing regulatory obligations, informing customers, and handling sensitive information during a cyber

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
[2] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

incident. The day after the incident, UnitedHealth filed a regulatory disclosure with the U.S. Securities and Exchange Commission blaming a nation-state actor and pointing to a technical support website which provided few updates regarding missing services and the security of data. Less than a week later, the company followed up with a second filing, this time blaming the ALPHV ransomware gang. The result was a situation where my clients and partners felt ignored and Change Healthcare was left dealing with both a public relations crisis on top of the original hack.

A changing world

Cybercrime is growing increasingly sophisticated, prompting organizations to implement advanced security technologies to protect their data and assets. Compared to several years ago, cybersecurity has drastically changed. This is due to two compounding trends: the ongoing transition to the cloud and the emergence of AI. Where security in traditional on-premise deployments was relatively straightforward, with perimeters keeping untrusted entities out, cloud-native environments require more complex solutions due to the nature of their application architecture and the connectivity between users, data, and the internet. Hybrid infrastructure environments increase the complexity even further, as organisations need solutions that cover a broader scope.

AI is rapidly becoming an integral part of cybersecurity. This technology presents both opportunities and dangers to the field. It can be used to automate threat detection and response and improve the accuracy and speed of security operations. However, malicious actors can also use AI to quickly identify and exploit system weaknesses, automate activities such as phishing, social engineering, and hacking, as well as creating and distributing fake content.

Cybersecurity and sustainable development

In today's digital age, businesses are heavily reliant on technology to store and manage valuable data. Hackers and cybercriminals are constantly looking for ways to exploit vulnerabilities in these systems, which is why cybersecurity has become a top priority for organizations of all sizes. At the same time, more and more companies are embracing sustainable investing, which prioritizes environmental and social responsibility. While these two concepts may seem unrelated, they can work together to create a more secure and sustainable future.

Cybersecurity is essential for protecting businesses, organizations, and infrastructure worldwide, especially as more of our lives become digitized. As such, it is crucial to achieving sustainable development goals (SDGs), particularly Sustainable Development Goal 16: peace, justice, and strong institutions. This SDG focuses on promoting peaceful and inclusive societies, providing access to justice for all, and significantly reducing illicit financial and arms flows. Additionally, it emphasizes the need to combat cybercrime and strengthen the recovery and return of stolen assets.

A broad approach to sustainable development

Of course, while efficient and effective cybersecurity can contribute to sustainable development goals in this way, the cybersecurity industry faces the same broader sustainability concerns that affect all sectors. For instance, being a tech-based industry, cybersecurity is power intensive and may rely on data centres, raising questions surrounding sustainable energy usage. Furthermore, there may be issues about the types of clients that cyber security providers work with – if services are provided to, for example, oppressive state actors or arms manufacturers, then that may itself raise ethical and sustainability issues. These questions, and more, are all ones that sustainable investors will need to consider when addressing this sector.

As digital technologies become ever-more integral to our lives, a robust approach to protecting data, infrastructure, and digital assets is thus needed to mitigate cybercrime and ensure trust and safety in our digital society. And as sustainable investors, we can play a key role in this effort by considering the broader role of cybersecurity in sustainable development, while also addressing the type of issues – described above – that may affect providers in this area. Indeed, investing in companies prioritizing cybersecurity and sustainable development goals can drive systemic change and create a secure and sustainable world for all.

Furthermore, by investing in companies that are taking action to protect data, infrastructure, and digital assets, we can incentivize organizations to prioritize cybersecurity and create a safe and secure digital society. As sustainable investors, we can make a real and lasting difference in the world that will ensure a safe and sustainable future for all.

April 2024

ADM-3636492