BIZCOMMUNITY

Addressing cybersecurity and climate change for a sustainable society

By Barbara Maigret

27 May 2022

Our society faces significant challenges that must be addressed quickly to prevent disruptions that can threaten lives. The first is climate change which poses a risk to our planet. According to the *2022 Global Risks Report*, the current climate crisis remains humanity's most significant long-term challenge. The second is cybersecurity, which has become a broad sustainability issue, threatening our evolving connected society and the digital economy on which individuals, organisations, and nations now rely.

Source: www.pixabay.com

These are both top concerns for governments, businesses, and individuals worldwide. And while these issues may seem starkly different, according to the “Declaration for the Future of the Internet” (recently issued by the US Department of State and more than 60 signatory countries and partners), technology plays a critical role in “the fight against global climate change” which, in turn, makes securing technology even more urgent.

Fortunately, the approaches to addressing these challenges are remarkably similar. They include changing behaviours, funding innovation, establishing strict and enforceable regulations, and encouraging collaboration across industries and interests.

Motivating behaviour change through awareness

One of the most significant barriers to addressing these challenges is human nature. So, the first step to addressing these issues is to change behaviours, and that is done through awareness. Of course, not everyone will change, but we can tip the scales if enough people understand the issues and then adapt their behaviours.

Climate change

Awareness is an essential factor in the global fight against climate change. Knowledge helps people understand the causes and consequences of global warming and encourages them to change their behaviour so we can adapt how we live to the realities of what is already a global emergency. A recent survey queried more than 3,000 people in eight countries about their awareness of climate change. Even during the pandemic, 76% of respondents reported that environmental issues were the same or more concerning than health issues. And 70% said they were more aware now than before Covid-19 that human activity threatens the climate and that the degradation of the environment threatens humans. They also expressed a commitment to changing their behaviour to support a sustainability strategy.

AI tech to predict climate change - possible solution for future floods

Junaid Kleinschmidt 10 May 2022

Cybersecurity

Awareness also plays a crucial role in improving cybersecurity. The most vital step in the fight against cyberattacks is improving our first line of defence. While security technology continues to improve, the biggest challenge — and opportunity — is the human element. According to the *2021 Verizon Data Breach Investigations Report*, 85% of data breaches involve human error. Opening a malicious email attachment, forgetting to change the password on a server, misconfiguring a device, or failing to patch or update a device are still the most common ways for attackers to breach a network.

Educating individuals on the risks they should avoid through cybersecurity awareness training is the most effective way to prevent most threats. Providing a workforce with the latest information about specific threats to the company and clearly explaining their essential role in protecting against them – both at work and at home – are vital for securing corporate networks and systems and keeping users safe online. This same effort needs to be added to school curriculum so children who grow up in an immersive digital society are also cyber aware. Effective cybersecurity awareness motivates lasting behaviour change, both professionally and personally.

Fighting climate change and cybersecurity risk through innovation

Innovation is another area where these critical issues intersect. Technology plays a crucial role in helping society retool the systems and infrastructure needed to achieve and maintain a sustainable society.

Climate change

Green technology innovation in all sectors is essential to addressing the global challenge of climate change. Renewable energy sources (solar, wind, wave, tidal, and geothermal power), sustainable transportation (electric vehicles, smart energy grids to reduce waste and improve efficiency), clean manufacturing processes, green buildings, and more energy-efficient devices all play a critical role in delivering considerably improved environmental performance.

According to the Global e-Sustainability Initiative, technology has the potential to contribute to all 17 of the UN's Sustainable Development Goals (SDGs). Technology and innovation have the power to implement climate transformation and address the critical challenges of climate change. For example, emerging technologies, like extracting carbon from the atmosphere, can aid in slowing down global warming and help heal the planet. Similarly, new internet of things (IoT) technologies are being distributed globally to improve data-driven decision-making to increase energy efficiency, amplify the effectiveness of "green" technologies such as wind power and bioenergy, and further reduce our dependence on coal-based electricity generation.

Egypt wants to shift focus to developing countries in climate talks - official

Aidan Lewis 25 May 2022

Cybersecurity

As our society accelerates its dependence on technology to ensure a sustainable future, cybersecurity becomes mission-critical. To enable and secure digital acceleration and innovation across every sector of the modern digital economy, cybersecurity vendors must develop solutions that can keep up with technological advances and address how today's businesses, governments, and individuals use technology. For example, to scale and adapt to today’s rapidly evolving digital world, cybersecurity is learning to apply advanced artificial intelligence and machine learning (AI and ML) to analyse massive volumes of data to detect sophisticated breaches and unusual network activity. It is also having to consolidate solutions so automation can be better leveraged to accelerate threat response time. Similarly, new security systems must be developed to protect emerging technologies, such as quantum computing, that hold so much promise.

Enforcing climate change and cybersecurity through regulations

While self-regulation is ideal, regulations and international standards are necessary to drive a change in behaviours, especially if we hope to affect that change in the limited timeframe available.

Climate change

Standards are essential to fighting climate change. They ensure trust, integrity, and consistent management in measuring and verifying greenhouse gas emissions and energy efficiency. To ensure progress is being made consistently, global frameworks are essential. The Taskforce on Climate-Related Financial Disclosures (TCFD) has become a worldwide standard for consistent climate-related financial risk disclosures. Companies, banks, and investors use it to provide sustainability information to stakeholders. The EU's Sustainable Finance Disclosure Regulation (SFDR) is designed to help stakeholders and clients understand, compare, and monitor the sustainability characteristics of investment funds, including their environmental impact.

The Corporate Sustainability Reporting Directive (CSRD), due to go live in 2023, requires all large companies to report on their social and environmental impact. And in the United States, the SEC draft rule, which requires public companies to disclose extensive climate-related information in their SEC filings starting in the fiscal year 2023, is another regulation that ensures that organisations are focused – and reporting on – efforts with environmental impact. These and similar measures put teeth in the more generic agreements governments have adopted, like the Paris Agreement.

SA corporates over budget on security, but cyber risks mount - report

3 May 2022

Cybersecurity

As with climate change, a unified set of practices and regulations serves as a shared map and reference point for organisations looking to secure digital infrastructures. They reduce risk by ensuring a baseline of quality and compliance for both technology and processes. Widely accepted guidelines for cybersecurity, such as NIST and ISO 27000 certification standards, help organisations implement best practices and technologies. On the other side, regulations like GDPR and HIPAA ensure data privacy, protect personally identifiable information (PII), and force organisations to report on breaches.

In addition, following the series of executive orders from the White House on the need for cybersecurity, the SEC has proposed new cybersecurity requirements for investment advisers and registered investment companies. They have also unveiled a proposed set of cybersecurity disclosure rules for public companies to standardise cybersecurity-related incident reporting, governance, and risk management.

Such standards are vital for ensuring that security requirements are consistently met using best practices and compliant solutions. Current and proposed regulations are designed to have the same effect as those targeting climate change.

Addressing climate change and cybersecurity through collaboration

If there is one lesson to be learned, it's that none of us can do this alone. In an age of specialisation, we must develop private-public partnerships to help us more effectively address climate change, cybersecurity, and other emerging challenges.

Climate change

As clearly highlighted during COP26 (the 2021 United Nations Climate Change Conference), saving the planet from climate change will not be possible without close partnerships between governments, NGOs, the private sector, and the public. A collective effort will be necessary if we are to meet global temperature and emissions reduction goals set by the Paris Agreement, new regulatory and compliance requirements, and the UN's 17 SGDs.

How the Russia-Ukraine conflict affects the local cyber threat landscape

Nithen Naidoo 14 Mar 2022

Cybersecurity

The arms race with cybercriminals also can't be won without global collaboration. Vendors, businesses, public agencies, and governments all have a role to play, whether through local coalitions, national organisations, or international forums. Disrupting cybercrime activities and dismantling the attack infrastructure is a joint responsibility that requires strong, trusted relationships between public and private organisations.

An example is FIRST, a consortium of incident response and security teams from every country that works together to ensure a safe internet. Other leading partnerships include the NATO Industry Cyber Partnership (NICP) on cyber threat intelligence sharing and the World Economic Forum's Partnership Against Cybercrime (PAC), which is currently mapping all major global cybercrime syndicates.

Conclusion

As leaders from around the world get together at Davos to discuss the critical issues that are impacting the sustainability of our planet and society, they must consider both climate change and cybersecurity as integral to enabling a better future for all. At their core, these are sustainability issues. And while each has its unique challenges, they also increasingly overlap as our digital and physical worlds continue to converge. Addressing one necessarily impacts the other.

At the end of the day, if enough people switch to renewable energy, enough businesses take the necessary precautions to protect their systems and data, and enough governments take efforts to level the digital playing field, I am confident we can make our world sustainable.

ABOUT THE AUTHOR

Barbara Maigret, global head of sustainability and CSR, and chair of the CSR Committee at Fortinet