SUSTAINABLE CYBERSECURITY

Sustainable Cybersecurity

by Changiz Sadr, P.Eng., FEC, CISSP

Published: August 2023

ONTARIO SOCIETY OF PROFESSIONAL ENGINEERS

www.ospe.on.ca

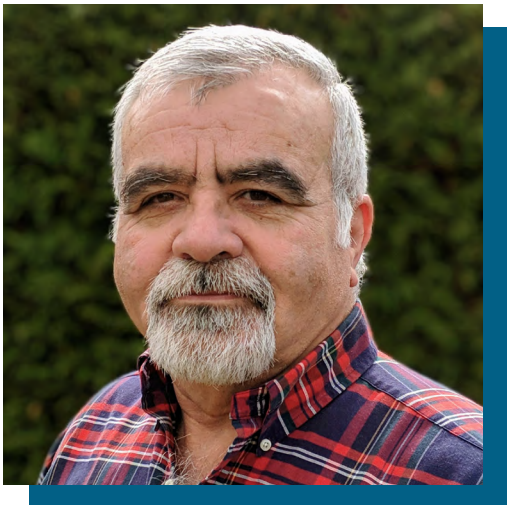
TABLE OF CONTENTS

FORWARD (OSPE STAFF)

Is Your Cybersecurity Provider Using Sustainable Practices?

In our digital world, cybersecurity is critical to the safe function of nearly everything. While its execution may seem virtual in our minds, the reality is that it is a significant industry, demanding significant real-world assets. As such, there is an opportunity for providers to comply with sustainability standards set across many industries. For those who retain information security service providers, consider looking for those who not only provide robust cybersecurity services but also those who do so in an energy efficient and climate-conscious manner as advocated by this author below.

ABOUT THE AUTHOR



Changiz Sadr, P.Eng., FEC, CISSP

Changiz Sadr is an accomplished telecommunications engineer, licensed professional engineer in Ontario, and a distinguished fellow of Engineers Canada. With a strong background in communications infrastructure engineering and cybersecurity, he has made significant contributions to the field throughout his career.

Changiz holds prominent positions within the industry, currently serving on the Board of Directors of the Cyber Security Global Alliance (CSGA) and as an Engineer-In-Residence (EIR) Advisory Board member for Engineers of Tomorrow. He has also been appointed to prestigious roles on the Canadian Engineering Qualifications Board and the board of Engineers Canada.

ABSTRACT

Sustainable cybersecurity refers to the concept of integrating sustainability principles into the field of cybersecurity. By collectively working towards sustainable cybersecurity, we can create a harmonious balance between environmental responsibility, social ethics, and technological resilience, ensuring a brighter and more sustainable digital future for generations to come. This paper outlines the benefits of sustainable cybersecurity, identifies challenges and best practices for implementing sustainable cybersecurity systems, and equips engineers to evaluate the sustainability of their cybersecurity infrastructure.

INTRODUCTION

Sustainable cybersecurity is an important approach to information security that combines environmental responsibility, social ethics, and technological resilience. In order to embrace sustainable cybersecurity and foster a greener and more secure digital landscape, it is imperative for organizations and individuals alike to take proactive steps. This includes promoting awareness about the importance of sustainable practices, advocating for the adoption of eco-friendly technologies, and supporting research and development in the field. By collectively working towards sustainable cybersecurity, we can create a harmonious balance between environmental responsibility, social ethics, and technological resilience, ensuring a brighter and more sustainable digital future for generations to come.

Definition of Cybersecurity: Cybersecurity encompasses the practices, technologies, and processes aimed at protecting computer systems, networks, and data from theft, damage, or unauthorized access. It is crucial in today's interconnected world, where various aspects of modern life depend on technology and the internet. Effective cybersecurity entails a comprehensive approach that includes technical and non-technical measures such as network security, access controls, encryption, incident response planning, and employee training. Its goal is to reduce the risk of cyber-attacks and minimize the impact of any breaches that occur.

Definition of Sustainability: Sustainability entails meeting present needs without compromising the ability of future generations to meet their own needs. It involves balancing economic, social, and environmental considerations to promote long-term well-being and resilience. In essence, sustainability requires utilizing resources in a manner that ensures their availability for future generations while minimizing negative impacts on the environment and society. It necessitates considering the long-term consequences of our actions and making choices that support a healthy and prosperous future for all.

Sustainable cybersecurity refers to the concept of integrating sustainability principles into the field of cybersecurity.

BENEFITS OF SUSTAINABLE CYBERSECURITY

- **Reduced Carbon Footprint:** Implementing sustainable cybersecurity practices can help organizations reduce their carbon footprint and environmental impact. For example, using renewable energy to power data centres significantly reduces greenhouse gas emissions, contributing to climate change mitigation.
- **Improved Resource Efficiency:** Sustainable cybersecurity practices enhance resource efficiency by reducing energy consumption and minimizing waste generation. This leads to cost savings and improved operational efficiency.
- **Increased Resilience:** Organizations adopting sustainable cybersecurity practices can be more resilient against cyber threats and disruptions. Implementing secure-by-default products and conducting regular security audits prevents cyber-attacks and minimizes their impact.
- **Enhanced Reputation:** Companies that prioritize sustainability in all of their practices enjoy a stronger reputation and greater trust from customers and stakeholders. This differentiation from competitors can drive business growth.
- **Regulatory Compliance:** Many countries and jurisdictions require organizations to report on their sustainability performance, including environmental impact and social sustainability.

Implementing sustainable cybersecurity practices ensures compliance with relevant laws and regulations.

CHALLENGES OF IMPLEMENTING SUSTAINABLE CYBERSECURITY

- **Cost:** Implementing sustainable cybersecurity practices may incur significant upfront costs, such as investing in renewable energy infrastructure or upgrading legacy IT systems.
- **Lack of Expertise:** Implementing sustainable cybersecurity practices requires specialized knowledge, particularly in the areas of renewable energy, green computing, and life cycle assessment. Many organizations may lack the in-house expertise needed for effective implementation.
- **Complexity:** Sustainable cybersecurity is a multifaceted field that necessitates coordination across departments and stakeholders. This complexity can make it challenging to implement comprehensive and integrated sustainable cybersecurity programs.
- **Regulatory Compliance:** Meeting regulatory requirements related to sustainability and cybersecurity can be a significant challenge due to rapidly evolving regulatory landscapes. Organizations need to dedicate resources to keep up and comply with relevant laws and regulations.
- **Resistance to Change:** Implementing sustainable cybersecurity practices may require significant changes to organizational culture, processes, and practices. Resistance from employees and stakeholders who are reluctant to change can pose challenges.

HOW TO ENGINEER BEST PRACTICES FOR SUSTAINABLE CYBERSECURITY

- **Implement Secure-by-Default Products:** Prioritize security and sustainability by using products and services designed to be secure from the outset, reducing the need for additional security measures.
- **Use Renewable Energy:** Reduce carbon footprint by utilizing renewable energy sources, such as wind and solar power, to power IT infrastructure. Options include installing solar panels, purchasing renewable energy credits, or using data centres powered by renewable energy.
- **Conduct Life Cycle Assessments:** Evaluate the environmental impact of cybersecurity solutions through life cycle assessments. Identify opportunities to reduce environmental impact throughout the product/service life cycle.
- **Minimize Waste:** Implement sustainable data centre practices, such as reducing energy consumption, recycling e-waste, and utilizing water-efficient cooling systems, to minimize waste generation and environmental impact.
- **Prioritize Privacy and Data Protection:** Emphasize user privacy and data protection through robust security measures and data protection policies. Ensure that sustainable cybersecurity practices align with ethical and social standards.

EXAMPLES OF SUSTAINABLE CYBERSECURITY BY SECTOR

- **Renewable Energy:** Numerous companies are utilizing renewable energy sources like wind and solar power to power their data centres and IT infrastructure. This approach not only reduces their carbon footprint but also ensures the long-term sustainability of their operations.
- **Life Cycle Assessment (LCA):** Implementing life cycle assessments helps evaluate the environmental impact of cybersecurity solutions throughout their entire life cycle. By identifying opportunities to reduce environmental impact and enhance sustainability, organizations can make informed decisions to improve their cybersecurity practices.
- **Ethical Considerations:** Sustainable cybersecurity also encompasses ethical considerations such as privacy, data protection, and human rights. Organizations can implement practices that prioritize user privacy and data protection, as well as avoid technologies that could be misused for unethical purposes.
- **Resource Efficiency:** Improving resource efficiency is another aspect of sustainable cybersecurity. This includes reducing energy and water consumption, minimizing waste generation, and optimizing material and resource usage throughout the IT supply chain.
- **Consider Green Computing:** Green computing involves designing, manufacturing, and using energy-efficient hardware, reducing e-waste, and implementing sustainable practices in data centres.

TECHNOLOGY COMPANIES LEADING THE SUSTAINABILITY MOVEMENT

If you commit to increased sustainability, you are definitely not alone.

- **Google's Renewable Energy Commitment:** Google promised to source 100% of its energy from renewable sources, powering its data centres and offices with wind and solar power.
- **IBM's Sustainable Data Centres:** IBM implemented sustainable data centre practices, including water-cooled servers, virtualization, and renewable energy usage. These practices led to a significant reduction in energy consumption and substantial cost savings.
- **Greenpeace's Click Clean Campaign:** Greenpeace's campaign urges companies to commit to using renewable energy for their data centres. Leading companies like Apple and Facebook (Meta) have responded by committing to sourcing 100 per cent renewable energy.
- **Microsoft's Circular Data Centre:** Microsoft developed a circular data centre that employs modular design, renewable energy, and recycled materials, showcasing their commitment to sustainability.

SUGGESTED POLICY ADJUSTMENTS AND REGULATIONS FOR PROMOTING SUSTAINABLE CYBERSECURITY

Reaching a more sustainable business environment will not be achieved in isolation. There are roles for government and industry.

- **Government Regulation:** Governments can enforce regulations and policies that mandate

organizations to adopt sustainable cybersecurity practices. For example, The European Union's General Data Protection Regulation (GDPR) requires organizations to implement appropriate security measures to protect personal data.

- **Certification Programs:** Certification programs provide organizations with frameworks for implementing best practices. Standards like ISO 27001 and ISO 14001 guide the implementation of sustainable cybersecurity management systems.
- **Financial Incentives:** Governments can offer financial incentives such as tax credits or subsidies to organizations adopting sustainable cybersecurity practices. For instance, the U.S. government provides tax credits for investments in renewable energy.
- **Collaborative Partnerships:** Governments can collaborate with industry stakeholders to promote sustainable cybersecurity. Initiatives like the Cybersecurity Tech Accord unite leading technology companies to promote cybersecurity and responsible technology use.
- **Public Awareness Campaigns:** Governments can launch public awareness campaigns to educate the public on the significance of sustainable cybersecurity. For example, the US Department of Homeland Security's "Stop. Think. Connect." campaign promotes cybersecurity awareness and encourages safe online behavior. A similar campaign for Sustainable Cybersecurity could be implemented with the InfoSec space.

CONSIDERATIONS FOR ORGANIZATIONS EVALUATING CYBERSECURITY PROVIDERS

To help organizations increase their sustainability practices, consider the following questions with your cybersecurity providers.

Does my cybersecurity provider...

- power their infrastructure with renewable energy sources?
- conduct life cycle assessments when selecting their infrastructure?
- use energy-efficient hardware?
- recycle their e-waste?
- comply with all government regulations concerning cybersecurity and sustainability?
- take advantage of applicable tax credits and other financial incentives?
- follow the best practices outlined in ISO 27001, ISO 14001, and other standards?

REFERENCES

Google's Renewable Energy Commitment:
https://cloud.google.com/blog/topics/sustainability/5-years-of-100-percent-renewable-energy

IBM's Sustainable Data Centers:
https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/it-sustainability

Greenpeace's Clean Click Campaign:
https://www.greenpeace.org/usa/fighting-climate-chaos/click-clean/#top

Microsoft's Circular Data Center:
https://customers.microsoft.com/en-us/story/1431789627332547010-microsoft-circular-centers

SUSTAINABLE CYBERSECURITY

CONTACT US

Ontario Society of Professional Engineers
4950 Yonge Street, Suite 502
Toronto, Ontario M2N 6K1
1-866-763-1654

www.ospe.on.ca

ONTARIO SOCIETY OF PROFESSIONAL ENGINEERS