HOW STRONG CYBERSECURITY DRIVES SUSTAINABLE OUTCOMES

Explore opportunities to improve your organization's cybersecurity to achieve corporate sustainability goals

Capgemini

Cybersecurity and sustainability have more in common than initial impressions. The strength of an organization's cybersecurity relies on its technology as well as its tools and processes. Equally important to protection of assets is the optimization of those assets for efficiency. That optimization can help organization's lower CO2 emissions and achieve their corporate sustainability goals. In this piece we will explore how strong cybersecurity practices support sustainability and define actionable ways to improve sustainability outcomes by implementing the right security measures.

How an organization's cybersecurity impacts sustainability

The design of an organization's business architecture is the starting point for a sustainable cybersecurity journey, as architecture directly influences the carbon footprint, including energy, water, and other finite resources. The sustainability tenets of reduce & re-use apply directly to cybersecurity decisions to optimize both security posture and sustainability goals.

The design of an organization's business architecture is the starting point for a sustainable cybersecurity journey, as architecture directly influences the carbon footprint.

Let's start with a **common struggle that organizations of every size grapple with: logs.** Many factors go into log architecture and cost, for example determining what data to log, the length of data retention for compliance and incident response, and storage tiers for optimized performance and cost. Today, we need to begin incorporating the sustainability impact into these decisions.

Data storage requires the use of finite resources such as rare earth minerals, which depletes the earth's natural resources and contributes to CO2 emissions through mining. Organizations can build more sustainable security by taking these steps into consideration, including:

- Reduce long-term raw log storage by focusing on critical metadata to decrease processing and storage needs. The right cyber strategy categorizes and tags logs and ensures only the most meaningful are used and stored.
- Choose solutions that excel in compression of data that must be retained, further reducing storage requirements.
- Lower network traffic by consolidating network ingress and egress points to lower power consumption.
- Consider a shift from private data centers to the cloud. Data centers require a tremendous amount of energy to operate, accounting for around 1.8% of electricity use in the U.S. and 0.5% of total U.S. greenhouse gas emissions.[1] Large amounts of water are also required to operate data centers, both directly for liquid cooling and indirectly to produce electricity. The per workload water and power requirements in data centers is estimated to be almost 5x higher than the cloud.[2]

Consider a shift from private data centers to the cloud. Data centers require a tremendous amount of energy to operate, accounting for around 1.8% of electricity use in the U.S. and 0.5% of total U.S. greenhouse gas emissions.

1 Environmental Research Letters, "The environmental footprint of data centers in the United States," May 21, 2021.
2 Ibid.

In addition to the above-mentioned impacts, **managed security service providers** and cloud-service provider tools reduce local data storage and energy consumption, providing more native security insights and sustainable cybersecurity. When organizations use their own security systems, the costs, both physical and environmental, are high. With managed security services, organizations can leverage the cloud either directly or through third parties, to benefit from mutualized resources. This also takes advantage of existing log sources without the need for duplicate storage, as is the case with AWS GuardDuty. A few examples of managed services that can deliver high value to organizations while also reducing their overall carbon footprint and cost include vulnerability management, Security Operations Centers (SOC), and managed detection and response.

Managed security service providers and cloud-service provider tools reduce local data storage and energy consumption, providing more native security insights and sustainable cybersecurity.

In the case of a managed SOC, organizations that choose to run their own SOC often find themselves dedicating real estate space in multiple geographies, purchasing dozens if not hundreds of screens and monitors, and requiring multiple SOC analysts onsite five days a week. Additionally, they struggle to implement the full range of desired automation, leaving many processes time and compute intensive. For some organizations, this is necessary due to requirements and specialization around their business or processes. But for others, leveraging a managed SOC service immediately allows for the use of mutualized compute resources and a reduction in the geographic footprint. Engaging a modern cloud-native SOC, provides the benefits of an automation-first mentality and in many cases, SOC personnel that can work effectively offsite. All of this directly leads to a lower carbon footprint while achieving better security results.

The above demonstrates how the careful consideration of the environmental impact of the systems architecture results in the reduced use of rare earth minerals, energy, and water, which supports publicly committed sustainability goals.

The careful consideration of the environmental impact of the systems architecture results in the reduced use of rare earth minerals, energy, and water, which supports publicly committed sustainability goals.

An additional sustainable cybersecurity consideration is system maintenance. Maintaining systems at optimal performance levels helps with resource management. Organizations leveraging Intelligent Industry using Operational Technology (OT) and the Internet of Things (IoT) benefit from waste reduction, improved visibility, and predictive analytics to improve their operations while reducing their environmental impact. Building controls to protect these systems is where cybersecurity can be a partner to the organization. For example, the infamous Mirai botnet at one point was comprised of over 600,000 IoT devices generating over 1Tbps of traffic.[3] The amount of wasted energy consumed by these devices and the network transmissions they created could have been avoided by improving default password practices on various IoT devices. If we ensure the security of this technology by default, we achieve a sustainable and secure outcome not only for manufacturing organizations, but for customers globally.

3 Cloudflare, "Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis," December 14, 2007.

How a cybersecurity event impacts sustainability

Cybersecurity attacks are both costly and carbon intensive. By one estimate the average cost of a cybersecurity event is $4.4 million.[4] The carbon impact of a cyberattack has both a direct and indirect influence.

A cybersecurity attack has a direct impact on an organization's carbon footprint.

While it is nearly impossible to calculate the number of events that *didn't* occur because of upgrades to cybersecurity, a cybersecurity attack has a direct impact on an organization's carbon footprint. An organization must quickly assemble a response team, often flying skilled people from around the globe to work together. **Travel is carbon intensive**, in addition to the cost of diverting so many people from their main job to a cybersecurity event.

A more overlooked yet significant indirect influence of cybersecurity attacks is the **carbon intensity of compute** for analysis of log entries and log aggregation. Millions of log entries can be created during a security event, and this requires processing power and storage. It takes time to process, analyze, and derive data, and that additional energy usage increases an organization's carbon footprint. According to IBM, the average time to fully contain a breach is 70 days,[5] and while not all that time is spent with the incident response team huddled in a room pouring over logs, the number is indicative of the amount of data and compute power for processing required to resolve the event.

A more overlooked yet significant indirect influence of a cybersecurity attack is the carbon intensity of compute for analysis of log entries and log aggregation.

Even events where the risk to sensitive data is low can result in serious environmental consequences. For example, a cloud-based cryptocurrency-mining attack on an organization can heavily impact resource consumption. Google found that 86% of compromised GCP instances (n=50) were being used for mining cryptocurrency in 2021.[6] Trend Micro estimates that miners can create a 600% increase in energy usage for compromised hosts.[7] While we don't have data on the number of cloud-based crypto-mining attacks, the impact of such events is far from negligible. Given 65%-70% of cloud security challenges are due to misconfiguration,[8] choosing the right cybersecurity tools and practices to protect and optimize systems is key to achieve corporate sustainability goals.

4 Security, "$4.35 million — The average cost of a data breach," October 17, 2022.

5 IBM, "Cost of a Data Breach 2022."

6 Google, "Threat Horizons, Cloud Threat Intelligence November 2021. Issue 1."

7 Trend Micro, "Probing the Activities of Cloud-Based Cryptocurrency-Mining Groups," March 29, 2022.

8 Trend Micro, "The Most Common Cloud Misconfigurations That Could Lead to Security Breaches," October 25, 2021.

Calls to action: Opportunities to transform your cybersecurity to be sustainable

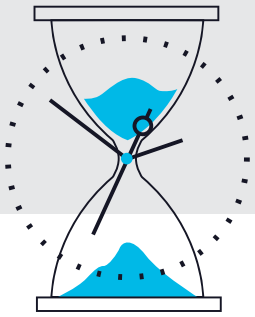
1. Sustainable cybersecurity is a new field and as a result, the very first step is to **grow your awareness** of the carbon intensity of your organization's IT and security decisions. To help grow awareness and determine your baseline for cost and energy savings, Capgemini offers a Greenhouse Gas (GHG) Impact Methodology that provides a five-step approach for calculating the carbon impact of projects. In addition, with sustainability as part of our DNA — we were listed by the global environmental non-profit CDP on their prestigious 'A list' for our climate leadership — Capgemini cloud security specialists are ready to work with you on your architecture and tooling approaches to enable the optimal security and sustainability decisions.

2. The second step is to **examine your business architecture.** Survey the security tools used. If you are not already leveraging cloud native tools that don't require additional storage, processing, and data paths, consider how they could replace existing services. In addition, investigate if managed security services can help reduce costs and also achieve sustainability goals. In the event you need third party tools, determine how you can architect data intensive actions — log sources, log storage, metadata architecture or processing — to ensure efficiency. Capgemini's expertise can help determine the right tech stack and provide managed security services if needed. We offer an automation-first approach to cloud security, leading to more sustainable and secure outcomes.

3. The third step is to **improve your business response to a cybersecurity event.** Review the incident response process and determine the ways to be effective remotely to eliminate the need for travel. This will require a change in behavior and expectations, not just technology. Capgemini can help with implementing new technologies, organizational processes, and people resources to enable your cybersecurity and sustainability goals. For example, see how we supported Nordic financial institutions to create an international financial CERT to pool resources across international borders to respond more effectively to cyber threats and online fraud.

There are many opportunities to improve your organization's cybersecurity to impact corporate sustainability goals and achieve net zero. By including sustainability in architectural and security decisions, you can ensure that strong cybersecurity practices lead to sustainable outcomes.

QUESTIONS FOR ORGANIZATIONS TO ASK IN THEIR SUSTAINABLE CYBERSECURITY JOURNEY



- **How can we share resources and use existing tools to have more sustainable outcomes?**
- **How can we architect data intensive actions — log sources, log storage, metadata architecture or processing — as well as third party tools — to optimize efficiency?**
- **How can we be effective remotely in the event of a cybersecurity event?**
- **Can a shift to managed security services help reduce costs and achieve sustainability goals?**

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of nearly 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com

Copyright © 2023 Capgemini. All rights reserved.