STRIKING A BALANCE - DATA CENTRE SECURITY AND GOING GREEN

Data centers are notorious for their substantial energy consumption, particularly for cooling and maintaining servers. It is estimated that these facilities collectively account for nearly 2% of the world's total electricity usage, contributing significantly to global greenhouse gas emissions.

Consequently, the carbon footprint associated with data centers requires immediate attention. More and more data centres are being regulated for their energy consumption and impact on the environment and are currently under a microscope.

Many of them have embraced new regulations by implementing green policies such as renewable energy.

However, what is the impact of physical security on sustainability and vice versa?

The quest for Enhanced Physical Security

Given the increasing threats to data security, organizations continuously invest in advanced physical security measures. These include multiple operation platforms, cutting-edge surveillance systems, biometric access controls, fortified perimeter security, and the employment of dedicated security personnel.

As these become increasingly sophisticated and able to foresee future threats, they pose an additional burden on data centres energy consumption.

One answer might lie with renewable energy, however that requires renewable energy of a large scale which is questionable if smaller data centre operators will be able to accommodate this.

Environmental Damage Affecting Physical Security

The other side to consider in this debate is the impact environmental damage has on physical security. Suddenly, security threats are not limited to intrusions but also the effects of extreme weather patterns.

Floods, fires, power outages directly impact the effectiveness of security systems, leaving data centers vulnerable to physical security breaches. Risk assessments now have to account for things that historically were not perceived a security risk – but how far ahead to you plan?

Are physical security the new keepers of sustainability? Expected to warn of potential extreme weather patterns and fortify data centres accordingly?

If so, how does this change physical security?

It is likely to come in the form of additional training for staff, and technology solutions but one thing is certain, sustainability needs to become an integral part of security, at its very core.

Physical security operational technology will have to adapt to encompass sustainability and staff will have to understand the impact of evolving threats emanating from extreme weather patterns.

AI to the rescue?

As the use of AI further expands, it is likely to have all-encompassing operational systems which address all of a data centres' needs. This would include traditional security concerns but also environmental concerns - such as forecasts, monitoring consumption and raising alerts.

However, AI is energy-intensive. As per the Vrije University Amsterdam's studies, by 2027 will consume annually the electricity of a small country. While the relevant study looked at AI at much larger scale than simply a data centre, it is important to remember that there are approximately 8000 data centres worldwide.

Data Centres already consume massive amounts of energy and with a potential increasing reliance on AI, their will consume even more. Can sustainable resources cover this usage, considering that data centres operate 24/7. As per Vrije University, data centre energy costs will increase by 50% only in terms of cooling.

As per our previous article, physical security will likely become more reliant on AI to address unexpected threats. Unexpected threats now include environmental issues, and energy consumption suddenly sky-rockets.

Physical security is not a mere bystander in sustainability anymore.

Striking a Balance

Striking a balance between security enhancements and environmental sustainability is an ongoing challenge, however the 2 must co-exist.

The first step is a change of mindset - security organisations must be prepared to support clients in their green policies and goals. They need to embrace sustainability in their own plans, monitor their impact and train staff accordingly.

The second step is to determine exactly how to expect the unexpected. As per our previous article, the data centre security of the future will have to expect the unexpected where the line between fiction and reality will be blurred. Expecting the unexpected here comes in a different form - environmental damage and its impact.

Some answers lie with technology but the impact of AI itself on sustainability cannot be overlooked.

The ICTS Europe Group has been a trusted security partner to numerous data centres for over a decade. Our security teams operate in over 80 data centre sites across 7 countries. Our emerging technologies and strategy shape the global security landscape and make a difference in the environments in which we operate.

Contact us to find out more about our ever-expanding solutions and to find out how we can redefine your security.

mail@ictseurope.com

www.ictseurope.com
www.ictseurope-viridian.com

In conclusion, the data centre security of the future will once again have to expect the unexpected. In this case, the unexpected will come from the environment. We need to talk about sustainability in the security sector and find a balance between teams, technology and their impact.

By doing this, security teams can not only minimize their own environmental impact but also ensure that data centers stay safe. Remember, what's bad for the environment is likely to also mess with your security.