Experience the commitment®

C*

*CYBERSECURITY 18
Ratkaisu Magazine Issue Excerpt

SAVING energy and lives

An interruption of the water, electricity or heating supply would directly affect almost all areas of life.

BY VESA KAARTINEN AND ESA LUOTO PHOTOS SHUTTERSTOCK AND KRISTIINA KONTONIEMI

A successful attack on the energy supply would quickly bring society to a halt. It would make life very cold, dark, and difficult. Literally!

So it is no wonder that cyber and information security risks have become key talking points in the energy sector.

"It is becoming increasingly important to detect information security threats at the earliest possible stage. This would enable rapid response to minimize damage," explains Marko Metiäinen, IT Service Manager at Jyväskylä Energy.

Companies face several cyber attacks month on average. Most such attacks remain undetected or are only heard of when they make the headlines. In general, cyber attacks are only noticed months or even years after they begin.

According to Marko Metiäinen, the basic challenges are the same for energy companies are the same as any other sector, but the scope of responsibility is much broader and more inclusive.

> "The key issue is to ensure the uninterrupted continuity of local energy production.
>
> MARKO METIÄINEN
> IT Service Manager,
> Jyväskylä Energy

"The key issue is to ensure the uninterrupted continuity of local energy production and our own business operations. At any rate, it is ultimately about ensuring the daily security of every customer and organization that we cover. Our tasks require constant emergency preparedness," Metiäinen summarizes.

Digitalization is an expertise renaissance

As digitalization and IoT progress, the discussion has moved from physical devices to overall infrastructure, and the related production, distribution and automation systems. Cyber risks are increasing due to by the easy blurring of risk responsibility in fragmented supply chains.

"Traditional antivirus software and network firewalls are no longer enough to keep information systems, networks and the data in them under companies' own control.

> **In contrast to the previous one-off audits, this enables us to anticipate the information and cybersecurity situation more comprehensively than before.**

grow, new tools and experts who understand the big picture are continuously needed to combat them," comments Metiäinen.

Jyväskylä Energy's solution is to outsource information security monitoring and management services to the experts of CGI's Security Operations Center (SOC). The agreement will provide Jyväskylä Energy with access to CGI's global threat information and service network.

When CGI's SOC experts spot abnormal activity in Jyväskylä Energy's networks or systems, they analyze the findings that triggered the alarm and, based on the criticality of such findings, propose further measures.

"This service generates a real-time snapshot of our network and information systems. In contrast to the previous one-off audits, this enables us to anticipate the information and cybersecurity situation more comprehensively than before. It also helps us to improve our preparedness for any incidents," Metiäinen explains.

According to the Finnish Government's Cyber Security Report, not all vital activities and maintenance-critical companies in society have adequate protection against cyber threats. There are also deficiencies in crisis tolerance.

Metiäinen compares support for the SOC service to insurance coverage. "Our priority is the security of supply and operations in the Jyväskylä region. We cannot risk relying on technology alone." ✱

QUESTION ABOUT THIS ARTICLE?
Mika Heino
+358 40 777 0370
mika.heino@cgi.com

CGI SECURITY OPERATIONS CENTER (SOC) – SHARED CYBER SERVICES

CGI'S SECURITY OPERATIONS CENTER, located in Helsinki Finland, provides Northern European clients with a full range of cybersecurity services, Organizations can select different services from risk management and threat modelling to continuous monitoring services.

SOC services are based on scalable. shared resourcing and processes. This enables clients to receive services that would typically require ten different resources to produce, at the cost of one resource. With efficient processes to manage multiple clients CGI still relies on named resources: "We always ensure that we have a named analyst focusing on the individual client, to ensure contextual knowledge and added value from the service", states Mika Heino, Director of the CGI SOC in Helsinki.