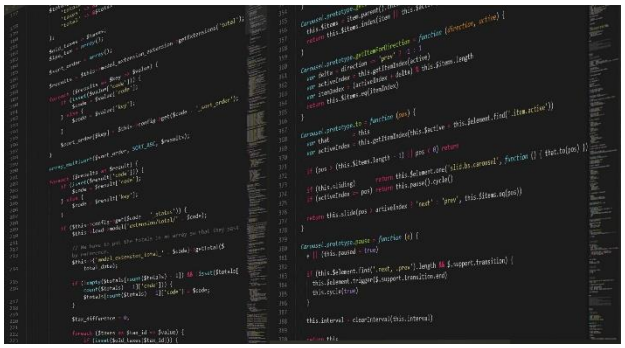
Why it's time to think again about energy software security

This month marks European Cyber Security Month – a time when organisations are encouraged to brush up on their everyday information security practices.

With a theme of 'Shared Responsibility,' the campaign aims to raise awareness of cyber security threats and help organisations protect themselves through education and sharing of good practices.

With cyber security under the spotlight, at Optima Energy we're particularly keen to highlight the importance of having secure and robust energy data systems, particularly as more organisations are now using software systems to monitor their energy usage.

It may seem surprising that the energy data generated by an organisation presents a risk, but all data has a value. Energy is a commodity which is required by everybody. It provides power to our homes but also critical functions such as hospitals, military and public services for example, where an outage is much more significant.



By its very nature data protection will always be a moving target. With the ever-growing demand for digitalisation, organisations of all sizes are open to the possible onslaught of cyber-attacks.

In the world of cyber-crime, it is often the more innocuous parts of the supply chain where weak links can be found. A vulnerability in a system that is monitoring energy data may be the route for building a profile of the target and may expose areas where some real damage can be done. In the energy industry, this is more likely to be through espionage or groups applying Advanced Persistent Threats (APT) to assist in their attempts to damage national security. Hacktivists may also have an interest in attempting to exploit high profile organisations in an attempt to gain attention to a cause, such as climate change.

Energy security matters

The reliance on IT-based systems for energy data management is now more prevalent than ever and as technology advances so does the level of vulnerability. As hackers finesse evermore ingenious methods of infiltrating systems, reviewing and maintaining the integrity of IT infrastructures and databases is crucial. Put simply, organisations have a responsibility to themselves and their customers to implement software and security controls which reduce exposure to cyber threats.

It's fundamental to be proactive when it comes to energy data security as a reactive approach could simply be too late to prevent a major breach. As a result, more companies are investing in advanced software to keep such sensitive data safe and are choosing to work alongside partners who have a track-record of ensuring data security is at the heart of its operation.

As a leading energy management software provider, our products are used across the public and private sector so it's absolutely essential that our products are secure and safe for use. At Optima, cyber security is considered in everything we do – from the development processes and the systems we use, to the way we store and manage data

and staff awareness. These are all key parts of our information security strategy. Using a 'defence in depth' approach, we have multiple layers of security controls to protect customers and eliminate a single point of failure. And we are constantly seeking new ways to enhance the security of our products.

One of the most common things we get asked about are our security certifications and accreditations. We are compliant with several ongoing security initiatives, including full accreditation for the Information Security Management Standard ISO 27001:2013 and Cyber Essentials Plus, which is a Government-backed scheme to help organisations protect themselves against common online threats. Now that we have taken steps to minimise risk with respect to information security, we are also actively working towards the Business Continuity Management Standard ISO 22301 and Quality Management System Standard ISO 9001.

When it comes to working with our customers, we take a 'shared responsibility approach'. We are committed to ensuring the confidentiality, integrity and availability of data. Protecting such important data is a critical responsibility we have to our customers, and we continue to invest and work hard to maintain that trust, with our robust systems outlined in our recent security whitepaper.

Whilst European Cyber Security Month raises awareness about the importance of having good information security practices, it is important to remember that it should be a year-round priority. It's certainly an area where companies will have to maintain vigilance, but an investment in robust energy management software can provide reassurance in at least one major area of company operations.

T: 01756 702488
E: info@optimaenergy.net
W: www.optimaenergy.net