THREE TIPS FOR CYBER SECURITY

Cyber security is a growing concern amongst manufacturers, with new strains of ransomware and other system viruses created every week.

Any company can be the subject of a cyber attack. The best way to prevent it is to plan ahead and prepare for the unexpected.

1

CONNECTED DEVICES

The benefits of mobile devices can be reaped in condition monitoring, predictive maintenance and analytics. For manufacturers using connected devices, regular security updates and software audits should be a priority if they wish to identify and resolve system faults.

2

LEGACY SYSTEMS

Generally, industrial computer systems are not updated or replaced as often as consumer technology, which can leave manufacturers open to older attacks such as Heartbleed or Shellshock.

Older systems may have an original OpenSSL software installed. Vulnerabilities in this software can open the system to attackers, who can eavesdrop or steal data.

Many software companies have released free critical updates to tackle vulnerabilities. All manufacturers need to do is simply update their software.

3

AUTOMATED PRODUCTION SYSTEMS

Networks and corporate systems are not the only things at risk. Industrial control systems can also be targeted by ransomware. If an attack locks down manufacturing computers, this can lead to expensive downtime. Manufacturers should safeguard automated production systems through cell protection, an effective form of defence against man-in-the-middle attacks.

In the age of Industry 4.0, connected devices and automated systems can be subject to additional threat. The best way to prevent an attack is to plan ahead and prepare for the unexpected.