The role of cyber security in the manufacturing environment

Johannesburg 30 June 2016 – Cyber security has become an integral component of any organisational strategy. With intellectual property becoming even more essential in a highly competitive world, no company can afford not to ensure that this critical asset is protected. For manufacturers, with complex supply chains, the need to prioritise security is even more important, says Tiaan van Schalkwyk at Deloitte South Africa.

"The world is becoming increasingly connected. As new mobile devices are released and more bandwidth becomes available, employees are more reliant than ever on accessing sensitive corporate data irrespective of their physical location. Business is well and truly real-time but what impact does this have on security, especially in such a dynamic environment as manufacturing?"

One of the biggest challenges is to ensure that security of information technologies is included in all operations. The complexity of this cannot be underestimated. Systems and networks used in manufacturing environments have significantly more stringent requirements than those used in a general office.

"Manufacturers need to have the peace of mind that the safety, availability, and reliability of all aspects of their systems are nigh on guaranteed. Furthermore, the temptation exists to compromise on the security of some part of the chain in favour of usability. This does place the entire system at risk. But even if this is not the case, it is only a matter of when and not if a manufacturer will be compromised."

Preventative measures are good, but does the organisation have the capability in place to alert the right people when an attack occurs? Even better, proactively warn of an impending attack. The frightening thing is that companies, manufacturers included, too frequently only discover that the network has been breached months, and in some instances years, after the fact. The financial and reputational impact this will have can be significant for the organisation and its directors.

“But even before OT (operational technology) security systems are put in place or upgraded, decision-makers need to conduct a cyber-security assessment. This enables them to better understand the threats and also gain insight into what the capabilities of the organisation are when it comes to cyber security.”

Adding to the pressure is the fact that an OT security breach in a manufacturing environment could potentially impact safety. Imagine the consequences of a malicious person impacting the behaviour of a machine or any part of the supply chain process. This means no manufacturer can leave OT security as something that only happens in the virtual realm. The threat to physical operations is also very real.

In this environment, preventative measures are no longer good enough. Manufacturers need to get ahead of the cyber security challenge and look at ways of being more pro-active.
“Developing more advanced monitoring and risk intelligent response capabilities provides some of the steps required to be more agile when it comes to security in a manufacturing environment. When it comes to cyber risk, it is essential to be vigilant and remain as secure as possible. This aids the manufacturer in becoming more resilient to any potential attacks both from a pro-active and a reactive basis.”