Going safely into the brave new world of 4IR

Put cyber security at the heart of industrial digitisation on the journey to 4IR, warns GECI

The Fourth Industrial Revolution (4IR) is changing the world as we knew it, and South Africa is pinning its growth ambitions on a 4IR-enabled economy. But 4IR adoption without putting cyber safety first could undermine growth efforts and expand the risks to manufacturing, heavy industry and key infrastructure, warns GECI.

GECI, a specialist in industrial cyber security, says key infrastructure, manufacturing and heavy industry is potentially at greater cyber risk than knowledge-based enterprises.

"Industries such as finance, telecoms, healthcare and retail are typically mature in terms of the digitisation journey, and usually have advanced and comprehensive cyber security measures in place," says Mike Bergen, Director of GECI International: Middle East and Africa. "In contrast, industrial and key infrastructure facilities are often running older operations technologies (OT) in siloes and not connected to the organisations' IT systems. For years, they have been at limited risk of cyberattack. However, as they digitise and start moving into a 4IR environment, these OTs will become connected to the internet and integrated into the enterprise IT environment, quickly expanding their risk exposure."

This risk is compounded by the fact that industrial sites tend to neglect basic information security measures in their existing environments. International OT cyber security solutions developer CyberX's 2019 Global ICS & IIoT Risk Report found vulnerabilities and flaws in basic cyber security at industrial sites around the world: 53% of industrial sites used outdated Windows systems, 57% were not running anti-virus software that updated signatures automatically, 69% had passwords traversing the network in plain-text, and the 'air gap' is a myth, as 40% of industrial sites had at least one direct connection to the internet, 84% had at least one remotely accessible device, and 16% of sites had at least one wireless access point.

Cybercriminals are already exploiting these vulnerabilities, costing companies millions in ransoms and other damages, Bergen says. "Research has found that virtually all industrial organisations have come under some form of cyberattack in the past few years. These attacks range from malware and ransomware attacks to targeted attacks designed to sabotage operations or steal sensitive data. The losses caused by successful attacks extend from actual theft and ransoms, through to production down time, safety risks, reputational damage and potential fines in the event of a failure to deliver critical services or due to sensitive information breaches," he says. The more connected these organisations become, the greater their risk footprint.

However, this does not mean the industrial sector should not advance into the 4IR. Bergen says: "Digitisation and technological progress helps overcome several common challenges in the industrial and manufacturing sectors – it improves throughput, efficiency and profitability, by achieving performance enhancement and resource efficiency through data acquisition and real-time analytics. Improved efficiencies help free up investment funds to support modern manufacturing innovation, rapid product iteration and customisation. Importantly, industrial safety can be enhanced by technologies such as better analytics and automation of dangerous tasks through robotics, cobotics and the digital workforce." He cites a McKinsey September 2018 white paper, which found 'manufacturing digitisation could boost heavy industry profit margins by three to five points'.

Says Bergen: "Nobody can afford to ignore 4IR progress. But companies wishing to move into the 4IR have to build cyber security into their strategies and systems from the ground up in both IT and OT environments, to counter the growing cyber risks facing them."

GECI International offers highly innovative and unique cybersecurity solutions for both administrative (IT) & industrial (OT) environments. GECI has provided global solutions to manufacturers and *consumers in the fields of aerospace, transportation, energy, petrochemicals, infrastructure, IT & Telecommunications for over 40 years. The Group has evolved to focus on digital technologies and has branched into IT/OT cyber security on the back of several acquisitions and partnerships.*

GECI provides CyberX in South Africa. The CyberX solution delivers the only industrial cyber security platform built by blue-team military cyber-experts with nation-state expertise defending critical infrastructure. CyberX delivers advanced OT asset discovery and visualisation, detects vulnerabilities and advanced known and unknown threats within seconds, prioritise and recommend actions to be taken to rectify vulnerabilities and threats, monitor continuously, providing alerts in real time, protecting critical IT and OT infrastructure against cyber-attacks, and automating Security Operations Centre (SOC) workflows.