Mining automation, IIoT, raise cyber risk

Next-generation automation is a double-edged sword for the mining sector, increasing the risk of cyber-attacks jeopardising safety and revenues, warns GECI

South African mining operations are set to embrace next-generation automation and Industrial Internet of Things (IIoT) systems to slash costs and increase production, but they risk crippling shutdowns and threats to human safety if they fail to adequately protect their infrastructures against cyber-attack, says cyber security specialist GECI.

GECI, a tactical cyber security specialist with a portfolio of cyber security innovations developed by former Israeli cyber defence unit experts, is now active in South Africa, focusing on local utilities, mines, manufacturers and other industrial sites in conjunction with local partner Sinac Group's Nokuthula Mgwebile.

South African GECI representative Mike Bergen says: "Mines are starting to adopt IIoT and intelligent automation across the entire pit-to-port chain, from autonomous vehicles to robotic drilling, and all of these new technologies are connected," says Bergen. "Unless this new smart mine environment is built on a foundation of industry-specific cyber security, mines risk financial losses, threats to human health and safety and even complete shutdown. With margins as tight as they are, no mine can afford this risk."

"Cyber-crime is a sophisticated and lucrative business, but mines have tended to lag in terms of cyber security," he says. Bergen cites EY Global Mining & Metals Cyber Security Leader Michael Rundus as saying 54% of mining companies had experienced a significant cyber incident in the past 12 months.

"Cyber risk has become such a major threat to the sector that EY lists cyber risk among the top five business risks facing mining and metals industry. And attacks on industrial facilities are taking place all the time, costing industries billions." For example, Bergen notes the attack on Swiss/Belgian mining and metals processor Nyrstar early this year, which shut down parts of its IT systems across its operations. The losses were not disclosed. "This is typical of many such attacks, the losses not being disclosed or purposefully trivialised as "insignificant" by the embarrassed victims," he says.

Norsk Hydro, an international aluminium, hydro and solar power firm, fell victim to a cyber-attack that crippled its computer networks in March this year. "Norsk Hydro operations in some 50 countries were forced to revert to manual operations and clip boards to conduct their business for weeks leading to serious operational inefficiencies and sales losses. This attack was launched through an employee clicking on a phishing email triggering a relatively new strain of ransomware called LockerGoga, and spread throughout all their international operations centres, causing losses so far estimated at €40million. Such attacks are occurring and increasing weekly," says Bergen.

"As mining operations embrace digitisation and IIoT to optimise their processes, they are increasingly opening themselves up to the risk of attack by cyber criminals, activists, and even possibly competitors or national enemies. So, automation is a double-edged sword, and mines need to make cyber security a top priority," he says.

GECI International offers highly innovative and unique cybersecurity solutions for both administrative (IT) & industrial (OT) environments. GECI industrial and mining cyber security solutions deliver advanced OT asset discovery and visualization, detect vulnerabilities and advanced known and unknown threats within seconds , prioritise and recommend actions to be taken to rectify vulnerabilities and threats, monitor continuously and provides alerts in real time, protect critical IT and OT infrastructure against cyber-attacks, and automate Security Operations Centre (SOC) workflows.