Navigating cybersecurity challenges within the African transport and logistics space

The African transport and logistics sector is a rapid adopter of industrial automation, embracing technologies such as the internet of things (IoT) and operational technologies (OT) to enhance efficiency. However, cautions Ben de Klerk, Eastern Cape Branch Manager at Datacentrix, a leading hybrid ICT systems integrator and managed services provider, with these advancements comes a well-documented history of cybersecurity vulnerabilities that still demand attention.

The rapid development and deployment of new technologies are also often associated with limited protocols governing their use, which poses its own set of risks, he explains.

The complex landscape of cybersecurity risk

“The local transport and logistics industry relies heavily on the smooth flow of goods across a complex network of multiple entities; from suppliers and manufacturers to distributors and retailers,” De Klerk explains. “This intricate supply chain structure is highly vulnerable to cyberthreats, as attackers can exploit any particular point in the supply chain.

“Moreover, the industry's reliance on IoT and OT devices – such as sensors, GPS trackers and automated control systems – introduces new potential vulnerabilities.”

> In order to mitigate these risks and bolster cybersecurity, organisations within the transport and logistics sector should look at adopting a comprehensive approach that combines technical, personnel and policy-based measures.

In fact, De Klerk maintains that this is a serious security challenge within the sector, as these sensors often lack robust built-in security features. This vulnerability opens the door to cyberattacks that can disrupt operations, compromise data, and lead to costly downtime, he says.

“Another area of great concern to OT security leaders within the transport and logistics industries is the risk of either unwitting, unaware, or malicious insider threats.”

> As the African transport and logistics sector continues its digital transformation, securing OT and industrial control systems (ICS) is of paramount importance.

Ben de Klerk, Eastern Cape Branch Manager at Datacentrix

Addressing security challenges

In order to mitigate these risks and bolster cybersecurity, organisations within the transport and logistics sector should look at adopting a comprehensive approach that combines technical, personnel and policy-based measures, De Klerk advises.

Ideally, this should include:

- Identifying and prioritising assets: Start by identifying and categorising OT assets based on their importance to the business. This prioritisation helps focus security efforts on critical assets first.
- Safeguarding devices: Secure all IoT and OT devices by implementing encryption, firewalls, access controls and regular patch management to prevent attacks and the associated costly downtime.
- Securing supply chain and remote access: Establish secure supply chain access protocols to ensure that only authorised personnel have access to critical systems. Implement robust authentication mechanisms for remote access.
- Undertaking regular security assessments: Conduct routine security assessments to identify vulnerabilities and take corrective action before they occur, assess the effectiveness of security measures, and proactively address potential weaknesses.
- Establishing employee training: Employees can be a significant source of vulnerability in any organisation, so it is essential that employees are educated on cybersecurity best practices to enhance their awareness of potential threats and empower them to respond effectively.
- Putting in place robust cybersecurity policies: Develop and implement strong OT cybersecurity policies and processes, with continuous monitoring and a disaster recovery plan to ensure business continuity.

“As the African transport and logistics sector continues its digital transformation, securing OT and industrial control systems (ICS) is of paramount importance. By adopting a multifaceted cybersecurity strategy, including risk assessment, device security, employee training, and policy development, organisations within this space can navigate these challenges and safeguard their operations in this dynamic industry,” De Klerk concludes.

For more information on Datacentrix's cybersecurity services, please visit www.datacentrix.co.za/security-services.html