Jacobs Douwe Egberts: Effectively mitigating risks with OT cybersecurity insights

A complete overview of potential cybersecurity risks across its factories worldwide helped Jacobs Douwe Egberts implement adequate mitigation measures to decrease risks, improve its cybersecurity posture and operate with confidence.

Jacobs Douwe Egberts (JDE) is a global coffee and tea company formed following the merger of the coffee division of Mondelez International with Douwe Egberts. In 2017, a malware incident caused a computer outage across Mondelez's global operations. The incident disrupted shipping and invoicing for several days, resulting in losses of €100M. This breach served as a catalyst for JDE to implement a cybersecurity program to address its operational technology (OT), including the industrial control system (ICS) environment across its factories worldwide.

The challenge

Industry 4.0 is driving unparalleled interconnectivity in manufacturing environments. Moreover, due to the criticality of operations, the manufacturing industry is highly targeted for cyberattacks. Traditional IT security is not enough to protect manufacturing organizations anymore. However, manufacturers often lack the expert knowledge and capacity needed to address the growing specter of cybersecurity threats in an effective way.

JDE needed a partner with the expertise to provide a comprehensive overview of all cybersecurity risks and vulnerabilities across its factories. This included all operational technology computing systems used to manage the entire industrial operation.

A reliable partner in OT / ICS security

JDE selected us for our comprehensive and integrated IT and OT cybersecurity solutions and services, supported by the capacity to assess all of JDE's factories worldwide, with a uniform approach and within the time frame set out.

To assess the OT / ICS environments across JDE factories, we provided a team of specialists with deep knowledge of process control. Our experts used CGI's proven OT security assessment methodology to provide insights into the maturity of the OT security

Our OT / ICS cybersecurity assessment includes:

- Maturity assessment
- IEC62443 / NIST800 assessment
- In-factory validation phase
- In-factory discovery phase, examining both the physical and logical OT / ICS security and documented findings
- OT / ICS network scan and analysis, including asset discovery, anti-malware landscape, identity & access mgt., firewalls and remote access

policy in place and review its implementation. The assessment included site visits, structured interviews with key employees, examination of the factory against the IEC62443 standard and an OT / ICS network topology scan.

Assessing risks to people, machines, processes and technology

Our experts connected specialized equipment to the OT / ICS network to run an automated asset discovery and generate a topology map that displayed all relevant assets in the client's OT / ICS environment and how they are interconnected. Data from the plant supervisory, direct control and field level systems were evaluated to identify areas particularly vulnerable to cybercrime.

Our OT security assessments are based on relevant worldwide ICS compliance standards like NIST and ISO/ISA/IEC. We executed the assessments with multiple on-site assessor teams (each consisting of two assessors) specialized in OT security, using a uniform approach for consistent reporting. The assessment preparation, firewall and network analysis, and OT / ICS architecture evaluation were performed centrally from our OT Security Centre of Excellence.

The assessment report included a risk inventory with a heat map, mitigation advice and budget indication for every specific mitigation. It covered the risks, their likelihood and impact and prioritized advised mitigations, helping JDE define its OT / ICS cybersecurity priorities moving forward.

Mitigating risks and raising awareness

Following the assessments and report, we also were tasked with implementing relevant mitigation measures. In addition, an OT / ICS cybersecurity awareness video was created, based on the findings, to improve cognizance of cyber risks among employees. This video is now distributed to JDE factory workers worldwide to train them on OT / ICS cybersecurity best practices and lower the risk of internal breaches.

Cybersecurity is part of everything we do

CGI has a 45-year heritage of helping clients reinvent and secure their businesses for the future by delivering innovative and advanced cybersecurity services in complex environments across the globe, including defense and intelligence sectors. We have invested heavily in establishing our credentials, working closely with international security associations and standards bodies.

While cyber threats are global, we know that requirements vary locally, and challenges are unique to each organization. Through our expert talent, deep technical and business knowledge, best practices and accelerator frameworks, we provide strategic advisory services, engineering of secure outcomes and managed security services. We work closely with you to ensure security controls are baked in, not bolted on.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit cgi.com/manufacturing
Email us at manufacturing@cgi.com